SaferJourno

DIGITAL SECURITY RESOURCES FOR MEDIA TRAINERS

Internews
Local voices. Global change.

Acknowledgements

We are, first and foremost, indebted to **Manisha Aryal** and **Dylan Jones** for creating, writing and organizing these learning materials into a coherent, hands-on set for busy trainers and learners. Their development and design is also reflected in their commitment to media's safety and a deep collaboration with others.

We would also like to give special thanks to those in the digital security, journalism and advocacy communities who contributed critical review and invaluable feedback: **Jesse Friedman** (Google), **Dr. Richard R. Brooks** (Clemson University, South Carolina), **Jillian C. York** (Electronic Frontier Foundation), **Chris Doten** (National Democratic Institute) **Shahzad Ahmad** and team (Bytes4All) **Carol Waters** (LevelUp/Internews) and **Brian J. Conley** (Small World News).

The *SaferJourno* toolkit was field-tested in a *Training of Trainers* workshop in December 2013 in Nairobi, Kenya. Thank you, **Ida Jooste**, Internews Country Director in Nairobi for your support to *SaferJourno*; to **Sandra Ndonye** and **Eva Constantaras** for your help with planning of the training event; and to **Samuel Musila** for meeting – and exceeding – every one of our requests before, during and after the training. We thank all the journalism trainers at the Kenya workshop who, through their participation and recommendations, made the toolkit so much better.

During the course of research, the writers consulted with Internews media trainers and partner organizations who work on media safety and training in Afghanistan, Bosnia, Dadaab, Jordan, Kazakhstan, Lebanon, Pakistan, Palestine, South Sudan, and Tunisia. We wish to thank each of you for generously contributing your time and knowledge.

Internews is grateful to **Gary Garriott** for his leadership on the project. To the Internewsers who gave so much extra to help us get this right – **Anthony Bouch, Jon Camfield, Mark Jardina, Nicolas Ebnother, Oleg Gant, Sam de Silva, Thomas Chanussot** – we thank you all for your review and contributions. And finally a special thank you to **Megan DeBlois, Tere Hicks** and all the Internet Initiatives crew at Internews for their support and backup throughout.

This toolkit was made possible with the financial support from the US Department of State – Bureau of Democracy, Human Rights and Labor, the John D. and Catherine T. MacArthur Foundation, and Google Inc.

Created, Written and Produced by: **Manisha Aryal** and **Dylan Jones**
Copy Editing: **Charlotte Stichter**
Graphics: **Ashley Low**
Design and Layout: **Kirsten Ankers**

Internews, 2014

Foreword

At Internews, we are incredibly fortunate to work with, and for, many of the finest journalists, technologists, media and development professionals around the world. Some of our biggest achievements together are in education and direct support to new generations of storytellers.

However, as the opportunities to research and report via new technologies increase, so too do the challenges. Never before have the risks been as severe, complex or fast-changing. A commitment to ongoing learning is essential now to understand, and safely harness the power of technology to be better-equipped and more secure as journalists.

Two of the most talented journalists and media development professionals have designed and developed this curriculum with us, bringing their deep knowledge and experience, including with Internews in countries spanning from Afghanistan to Zimbabwe. We are deeply grateful to Manisha Aryal and Dylan Jones for their extraordinary work and leadership on this initiative. Together, they have responded to fervent requests from our friends and colleagues around the world to create this curriculum in response to the urgent need for more help.

Its our honor, then, to present this for trainers, teachers and journalists who take on the challenges of learning – and teaching others – how to be safer and more secure online in an era of changing conditions and threats to journalists.

Kathleen Reen, Vice President for ICT Policy and Programs

March 2014

Trainers should always check that the information in any safety guide is current. There are developments in technology every day, as well as new threats. This guide, introduced in March 2014, is intended as a supplement for media trainers, most of whom do not have access to, or are not aware of, security resources. The lessons do not replace the value of a dedicated security training from a qualified instructor.

Table of Contents

USING THIS GUIDE FOR TRAINERS 3

1. ASSESSING RISKS 15

2. MALWARE AND BASIC PROTECTION 36

3. KEEPING DATA SAFE 54

4. RESEARCHING SECURELY 68

5. PROTECTING EMAIL 84

6. MOBILE PHONE SAFETY 108

QUICK START: Tips for securing your smartphone 124

QUICK START: Tips for securing your PC and online accounts 125

SaferJourno: Digital Security Resources for Media Trainers

NAVIGATING THE GUIDE FOR TRAINERS

The six modules in SaferJourno: Digital Security Resources for Media Trainers are designed to help trainers integrate digital safety and online security topics into their media training. The modules do not assume that the trainer has special knowledge of the subject.

While we wrote the toolkit with journalism trainers in mind, we believe that the modules can also be used when training a wide range of media content producers (i.e., bloggers, citizen reporters, human rights activists who work with information, etc.) who use smartphones and the Internet to communicate. In addition, it often takes a team to produce media content, including fixers, editors, videographers, and photographers, who can also benefit from trainings that integrate this toolkit's resources.

More specifically, trainers can use the toolkit in four ways:

- As source material to integrate into trainings on journalism topics (e.g., an interview skills training can integrate the module on communicating safely, research skills training can integrate the module on circumvention and use of anonymizers, etc.).
- As the basis of a three-day digital safety training, using all of the materials provided.
- As curricula in an emergency training (used in response to specific requests or incidents in the local environment).
- As a component of a longer and more comprehensive journalism training program.

The modules are designed to run roughly three hours each and should be flexible enough to be used in each of the contexts described above. However, we recommend that trainers start with the Assessing Risks module, regardless of whether it is run as a three-day training or module-by-module over multiple weeks. Assessing Risks will help trainers and the journalists they train understand the digital and physical risks present in the environment in which they work, and provide context for the remaining modules.

While we do not expect trainers to be digital security experts, we do expect them to have a deep understanding of the media and the Internet in their countries/regions, and to maintain a healthy interest in device hygiene, mobile safety and online security.

The toolkit is written to train adult participants, who we expect will be selected for trainings in two ways – through open competition (where the training is advertised and an open selection process is practiced) or through a closed process (where organizers pick the participants in consultation with media organizations). In either case, once the participants are selected, and before they arrive at the training venue, the trainer(s) will need to start preparing for the training, keeping the needs of these adult learners in mind.

1. TRAINING PLAN

Malcolm S. Knowles, whose research helped shape modern approaches to adult learning, says in his book "The Modern Practice of Adult Education: From Pedagogy to Andragogy" that adults learn best when they take responsibility for their own learning. Andragogy, which comes from the Greek word andr (relating to "man" or an adult) and gogy meaning "led," is distinct from the more common pedagogy (pedo meaning "child"). Andragogy, as a learning model, then, means adult-led, adult-focused, and adult-driven learning. Five statements summarize Knowles' theory:

1. Adults need to understand and accept the reason for learning a specific skill.
2. Experience (including error) provides the basis for learning activities.
3. Adults need to be involved in both the planning and evaluation of their learning.
4. Adult learning is problem-centered rather than content-oriented.
5. Most adults are interested in learning what has immediate relevance to their professional and social lives.

The SaferJourno: Digital Security Resources for Media Trainers uses Activity-Discussion-Inputs-Deepening-Synthesis, or the ADIDS approach to learning. This andragogical approach has been used effectively in advocacy and skills training on human rights issues and we have found this to be useful in helping participants with minimal technical knowledge understand concepts as complex as digital security and online safety. For trainers, it may also provide a useful framework when creating lesson plans.

The operating principle behind the ADIDS approach is that adult learners benefit most from information presented in stages, and in a variety of formats – i.e., group activities, case studies, slide and audiovisual presentations, facilitated discussions, group work, hands-on practice, and reflection. This approach creates a comprehensive learning environment by taking into consideration the needs of kinesthetic learners (who need to do something physically to understand), as well as visual learners (who rely on pictures, diagrams and video) and auditory learners (who learn through hearing material such as lectures).

The ADIDS Approach

Activity (easing into the topic): We have organized each module to begin with an Activity that illustrates the material that is to follow. We recommend that trainers start with a group activity, as these act as "icebreakers" for new participants and will ease them into thinking about a topic that may be new to them.

Discussion (providing context): Discussion sessions follow each of the Activity sessions. These sessions are designed to help trainers engage participants in a conversation about the topic (and the preceding session). We have included a list of questions/talking points to help facilitate these discussions. We encourage trainers to adapt as necessary.

Input (interacting): While many trainers start their sessions with lectures or presentations, we recommend that trainers go through the two previous steps (Activity and Discussion) before launching their PowerPoints. Complex topics benefit from preparation and participants will have been prepared by the prior sessions. An effective Input session is one in which participants are engaged with a range of materials, including case studies, and there is a give-and-take in knowledge sharing among trainer(s) and participants.

Deepening (hands-on activities): In journalism and online safety trainings, this session usually includes the installation of software and learning to use it. This is possibly the most important session in training, as this is where participants learn new skills by doing them. However, it needs to follow the previous three segments so that the participants understand why they are learning a particular skill.

Synthesis (reflection): Lessons benefit from practice and review, and learning is reinforced by reflecting on the knowledge acquired. Trainers can summarize the knowledge and skills that have just been addressed in this session. We recommend that this session be used to clarify and wrap up. Participants should be encouraged to ask questions, seek clarification and understand the next steps.

We believe that all of these steps are necessary if we are to help participants turn learning into habits. The questions below should help the trainers plan for their event:

- What basic skills will the participants arrive with?
- Where are the gaps in their learning?
- What skills will the participants pick up during the training?
- What are the learning goals for each session? (What will each session cover?)
- Do the sessions build on participants' skills? Do they relate to their environment?
- Do the topics and subtopics flow well together?
- What activities may be effective in introducing the topics or subtopics to participants?
- What collaborative/interactive exercises can illustrate the main points of the sessions?
- What questions may facilitate a constructive discussion?
- How will the participants connect the activities with main topics of the session?
- How can the participants' understanding of the topic be deepened?
- Are there real-life examples that can be used to illustrate the need for these skills?
- What resources will be used? Lectures? PowerPoints? Videos?
- What are the steps in the hands-on exercise? How will time be set aside for this flow?
- What is the best way to find out what the participants have learned? Will quizzes work?
- How can the lessons learned from one session be used to improve other sessions?
- What skills will participants leave with?
- Will their behavior change as a result of the training?
- How do participants build on the skills they have picked up after the training?

2. ABOUT THE MODULES

For the purpose of this toolkit, we've chosen to call the collection of materials that relate to one subject a module. We have created six modules to cover the situations that most affect journalists. More may follow, and we hope that trainers will share their own materials and lesson agendas in community-driven projects like LevelUp.

When running a full training, we recommend that the trainers make participants go through each of the modules in the order that they are listed, with Assessing Risks at the beginning. This will help participants prioritize and apply information they learn in later modules. As mentioned earlier, each module has five sections (Activity, Discussion, Input, Deepening and Synthesis). We recommend that trainers follow them in this order to get the most from this approach.

Modules start with a group activity (Activity) that will introduce a key concept or illustrate a security vulnerability to participants. The second section of the module (Discussion) gets them talking about the module concept or vulnerability and how it affects their work. These two steps are

necessary to get the participants primed to learn during the next section (Input), which provides an interactive lecture or audiovisual presentation. Once the participants have a fair understanding of the risks involved, and some knowledge of risk mitigation strategies, they should be ready to learn the skills that will protect them (Deepening). Finally, the closing discussion session (Synthesis) summarizes what has been covered in the module through various sessions. Though extremely important, this last session tends to get cut due to time constraints. We encourage trainers to end with this because it is the last opportunity for participants to confirm and reflect upon what they have learned with the trainers in the room while providing a sense of closure for each module.

Each module comes with supporting materials trainers can hand out, including:

- Class Notes (salient points discussed in class).
- Glossary (vocabulary and technical words used during the sessions).
- Additional Reading (materials that will help the participants further their learning).

NOTE: *For lesson material that covers Mac OS X and iOS devices, we have provided a separate section in each module that includes appropriate applications and exercises. These "Mac OS X" sections appear at the end of each ADIDS session, modules 2 through 6.*

We have also included two Quick Start Guides – "cheat sheets" on mobile security and PC security which operate as:

- Quick Start Guide: Securing Your Smartphone
- Quick Start Guide: Securing Your PC and Communications

As these Quick Start Guides will be useful for all the modules, we suggest that they be used as handouts for students to examine after class.

3. TRAINING TIPS

Some of the material below is drawn from the LevelUp program supporting security trainers, a community-driven initiative led by Internews. Journalism trainers using this curriculum will also find these recommendations useful when planning and conducting their training events.

Managing Expectations

As a trainer, it important to make sure that the organizers (management, contracting organizations) are clear about their expectations for the training. Can the requested outcomes be met? Are the resources made available for the training adequate? Is the number of participants manageable? Is the number of days enough to cover the skills that need to be taught? It is important to understand these before the training begins. We have provided a sample Pretraining Questionnaire for Organizers (which can be modified and adapted) for trainers to use.

For a training to run smoothly, the journalism trainers should ideally have access to a technical staff member (IT manager, technical coordinator, or others who are comfortable with devices and software).

Often, participants come in with unrealistic expectations of what they will learn in three days. As soon as the participant list is final, we recommend that the trainers contact the participants with:

- A Welcome Note that sets the framework of the training.
- A questionnaire that they will fill out and send back before the training begins so trainers can gauge participants' skill levels and expectations.

  (We have provided a sample Pretraining Questionnaire for Participants, which trainers can adapt and use.)
- Reading Materials (no more than a page) on two or three topics that are going to be covered in the training. These should not be long papers; rather, they should be quick reading materials that get participants interested in the training.

  (At the time of this writing, we recommend two online articles from Wired magazine, "How Apple and Amazon Security Flaws Led to My Epic Hacking" and "How I Resurrected My Digital Life After an Epic Hacking," and a CNN Video.)

We encourage trainers, participants and organizations to remember that understanding and addressing digital safety issues is a continuing process and that these materials are not the last word on security:

- There are no such things as final or permanent Internet security solutions. The programs/services available on the Internet can change their security settings and privacy policies without notice, possibly putting users at risk.
- New security updates, as well as viruses and malware, are launched every day and what was secure yesterday may be vulnerable to attack today. There is no alternative to staying aware, informed and engaged.
- A trainer can only help participants take the crucial first step towards educating themselves; the rest is up to the participants. We encourage trainers to drill down the message that while the three days they spend in training will open their eyes to digital and online dangers and introduce some current mitigation measures, they will ultimately need to start taking responsibility for their own safety and security.

Planning the Training

Class size: We recommend no more than 12 participants per training and, when possible, at least one co-trainer or assistant trainer to help participants during exercises, drills and software installation (allowing for one trainer or co-trainer per six students). If all six modules are to be taught at one time, we recommend that two full-time trainers take turns at leading trainer/co-trainer duties to maintain their energy levels, and go through the material to be covered over a three-day period. Anything more will zap both the trainers' and the participants' energy, and limit the effectiveness of the training.

Space: Digital security trainings need be run in a safe and secure space. While organizers are in the best position to pick an appropriate venue, digital and online security trainings have a requirement that trainers need to be cognizant of, namely Internet connectivity. The list below will be useful in planning the space:

- **Equipment:** Is the equipment necessary for your training available? Equipment includes computer hardware, audiovisual equipment, projection and multimedia devices, etc. If they are not available at the training venue, can they be brought in? Are there adequate equipment hookups or electrical outlets available to bring in laptops?
- **Room:** Do the rooms lend themselves to lectures, group work and hands-on demonstrations? What kind of seating is available? Are the seating arrangements flexible? Can the seats be moved around? Can tables be added or taken away when needed?
- **Connectivity:** Does the building have secure Wi-Fi? Can a VPN be set up if needed? Is the wireless router industrial grade (to support 12 to 15 people online)? Is the bandwidth at least 6MB/1.5MB so larger groups can access the Web and do email with a robust router? Will there be an IT person, fully permissioned (with administrator access) to troubleshoot hardware, software and connectivity issues that come up during the training?
- **Finally, intuition counts!** If a trainer feels uncomfortable in a training venue, and if there are choices available, we recommend that other venue options be explored.

Common training materials:

For most training events, organizers should be asked to provide:

- LCD projector and screen.
- Markers, flip charts and butcher paper or chart paper.
- White board, nonpermanent markers, white board cleaner.
- Notebooks and pens.
- Laptop or desktop computers.
- Internet connectivity with sufficient bandwidth for the number of participants.

If participants will be using rented equipment, these need to be done before the training:

- Ensure computers have genuine and updated software.

- Sweep computers for viruses and other malware.
- Ensure that the Wi-Fi access point is secure with WPA2 encryption and a strong password, and that the default password for the access point has been changed. (This is important and either the trainer or the organizers' IT support personnel need to do this.)

The trainers (and the organizers) need to prepare:

- Online folders containing a training schedule; course outline; course methodology; reading materials and handouts; exercise sheets; feedback and course evaluation forms; short biographies of trainers and participants; and a sheet containing contact numbers for the organizers, trainers and participants. The last two are optional as some participants may have security concerns and do not want to leave a paper trail. Dropbox and Google Drive seem to be in most common use.
- Printed versions of more recent guides on digital security. We suggest:
  - "Journalist Security Guide" from the Committee to Protect Journalists.
  - "SpeakSafe" from Internews.
  - "Threatsaurus" from Sophos" with: "Security in-a-box" from Tactical Technology Collective and Front Line Defenders. (link = https://securityinabox.org).
- Flash drives (memory sticks) — one per participant — with software, programs and reading materials, and a short handout explaining the contents of the flash drive. (If trainers wish to distribute software through a single device or media that will be passed around, from participant to participant, they should use a CD for this purpose as it cannot become infected with a virus.)

The participants can bring:

- Personal laptops (optional).
- Mobile phones or tablets that they use for their work.

Participant Security

Trainers need to do their own risk assessment when they are training participants who live in high-risk environments where journalists and other media producers are constantly monitored. In these situations, it is important to establish communication protocols with organizers and participants before, during and after the training. This may involve agreeing to some or all of the steps below:

- Designating one contact from the organization to communicate with the participants.
- Not divulging the list of participants and names of trainers/training organizations online.
- Keeping details of the participants (passport number, addresses) offline and secure.
- Not connecting the participants to each other without their express consent.
- Avoiding the use of organizational email addresses.

Creating a Contract

In the context of adult learning in general, and this training in particular, the trainer-participant relationship needs to be a partnership. Mutual respect and trust is the key to this partnership. Both are adults with a variety of experiences, skills, expertise and motivations. Digital security training addresses topics and issues that are sensitive and may put people (participants, organizers, trainers and donors) at risk.

The training also needs to establish some guidelines for acceptable behavior. Once they are agreed to, they can be posted in the room, and distributed to the participants to be included in their folders. The guidelines should cover, but need not be limited to the following:

- **Training times:** Agreement on the start, end and length of sessions. This includes breaks and lunchtimes. Times can be flexible, and may change each day, but once agreed to, need to be adhered to.
- **Presence:** Participants need to be physically and mentally present for all sessions. This means that they cannot be surfing the net, checking email or posting to social networks during sessions. Participants can have their mobile phones on silent mode during the training, so they can capture calls and messages and respond later.

- **Posting:** Digital security trainings for media workers and activists generally are off the record. However, if the training does not pose a risk to the organizers, participants and trainers, the Chatham House Rule can be applied. The Chatham House Rule states: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." When applied to social media, the Rule dictates that only what was said at an event, without identifying the speaker or another participant, can be tweeted or posted.
- **Security:** The security of everyone involved, including that of participants, trainers, organizers and donors, is important. The participants need to agree that they will refrain from practices that will put fellow participants, organizers, trainers and donors at risk or exposure.
- **Downloads:** Participants cannot monopolize the bandwidth of the class. This means turning off any torrent-related software and – unless it is the subject of a lesson – applications like Dropbox, Google Drive or OneDrive that generate background traffic, and closing social networking applications like Facebook, Twitter and Skype, as these inevitably result in a constant stream of alerts and other disruptions.
- **Respectful participation:** Showing respect (for each other) and taking responsibility (for their own learning) are two non-negotiable rules before the training begins. The particulars will need to be discussed as negotiating acceptable behavior is important. This will also invite participants to have a stake in the training and in their own learning.

The set of guidelines agreed to by the participants and trainers will be a contract that participants and trainers will use before, during and after the training.

Schedule

The modules we present in the following pages are designed to be three to three and a half hours long, with a 15-20 minute stretch/bathroom/snack break in between. We recommend that trainers remind participants that they can use the time to check their emails as well, so that this will not interfere with class time.

As described above, the modules use the ADIDS approach and roughly use the following format and timeline:

Session 0: Welcome, Housekeeping and Training Rules

00:00 to 00:30	Introduction and Expectations
00:30 to 01:30	Training Rules (discussion and agreement)

Sessions 1 through 6: ADIDS Approach to Digital Security Topics

00:00 to 00:15	Activity (15 minutes)
00:15 to 00:30	Discussion (15 minutes)
00:30 to 01:00	Input, Interactive Presentation with Questions/Answers (30 minutes)
01:00 to 01:15	Break (15 minutes)
01:15 to 02:45	Deepening (90 minutes)
02:45 to 03:00	Synthesis (15minutes)

Session 7: Wrap-up

00:00 to 00:30	Open-ended, Closed-circle Feedback Session
00:30 to 01:30	Training Evaluation, Next Steps Discussion

4. BEST PRACTICES

Below are some principles in training that we hope will make these sessions more effective. Feedback, tips and other trainers' suggestions on digital security topics can be read at the security-community website LevelUp, from which some of the material is drawn.

Commitment to Learning

Technology tools change constantly! This toolkit builds on Internews' SpeakSafe and LevelUp initiatives and is current as of December 2013.

As new tools and technology are invariably followed by new threats and vulnerabilities, trainers need to look beyond this resource and keep themselves updated on new developments. A number of groups, including the Tactical Technology Collective, Committee to Protect Journalists, Reporters Without Borders and Medill School of Journalism at Northwestern University, have produced digital security guides for journalists. These self-study resources are worth bookmarking and consulting regularly.

Unlike media trainers of the last century, who approached print media trainings with a set of notes and a few well-known examples, today's trainers have to understand their participants' media and technical environment, and commit to updating their knowledge of emerging tools and innovations that may be appropriate. Below are excellent resources for staying current on the state of media freedom for your participants:

- Freedom House's two reports (updated annually): "Freedom on the Net" and "Freedom of the Press."
- Reporters Without Borders' Press Freedom Index.
- Committee to Protect Journalists' Impunity Index.

We recommend keeping up with news, trends and developments by reading specific blogs; following thought/industry leaders on Twitter; and joining online discussion forums, Facebook groups, etc. The Liberationtech Listserv hosted by the Center on Democracy, Development, and the Rule of Law at Stanford University is a smart way to keep current on trends and topics. The Listserv is a discussion forum for individuals and institutions that work on open Internet initiatives, and it hosts discussions on the strengths and vulnerabilities of digital tools. The items generated by the Listserv are collected at the Liberationtech Archives.

Other resources we recommend that trainers refer to regularly include:

- ArsTechnica Security.
- The SANS Institute's news summary page.
- The Krebs on Security website from former Washington Post reporter Brian Krebs.

Last, but not least, we recommend that trainers set aside time on a regular basis to increase their own knowledge. Staying up-to-date requires commitment.

Using Open Source

This SaferJourno toolkit also encourages the use of "open-source" tools/software/programs, as much as possible. Open-source tools are easily available for download and their source codes are available to anyone who wants to view the codes, copy them, alter them and share them. They are also usually free. Open-source applications are open to public review and allow users and other developers to test, spot and correct errors, and address vulnerabilities.

In terms of online and digital security resources, open-source tools have become especially important as they are developed by individuals and institutions that are willing to have their codes tested by a community of users in a range of security settings. Enough developers out there are committed to open source, and the resulting efforts have made it possible to have open-source alternatives for almost every proprietary/closed-source tool, ranging from operating systems to applications to online platforms.

This open, community-driven and user-led development process is an important reason for using open-source tools. While most of the coding may still be done by a relatively small number of people, the collective intelligence of a large group of people contributing their personal experience and

time to improve open-source tools by working on patches, testing in various environments, tweaking small features, and removing bugs, makes open source an exciting development for the media industry. For more, watch "What is Open Source?" or read "Benefits of Open Source Software." Those interested in the security strengths and weaknesses of open source software may find the Wikipedia (open-source encyclopedia) entry titled "Open-source Software Security" an interesting read.

Mitigating Risks

Conveying the dangers of the online world can be challenging because the risks are virtual and therefore not tangible for most participants until they have been the victim of an attack. That is why a lot of security trainers start their sessions by hacking into someone's system (or social network) account. This gets the participants thinking of risks and dangers in ways that a lecture never could. Another effective way to get participants' attention is to tell stories or provide case studies of reporters or activists put at risk because of their insecure Internet communications and practices.

However, a responsible trainer also needs to know when to stop; fearmongering often fosters a feeling of disempowerment among the participants. If the issue is "too big" for them, it may paralyze them when it comes to solutions. The point of digital security trainings is to make participants aware of risks so they can be conscious and conscientious in their Internet communications and practices. A good rule of thumb is for trainers to remember that for every fear, at least one technical solution and/or strategy will need to be presented to the participants. Even if the risk being discussed does not have a technical solution, there will be strategies and tactics that the participants can employ to mitigate their risks.

Simplifying Jargon

Jargon is a "secret language" shared by people who are experts in a particular field – a shorthand in which complicated concepts get abbreviated into a single word or phrase. Technical training will have technical terms and concepts participants have not come across before. A trainer's job is to use the jargon (not avoid it), but demystify the concepts for the participants, using metaphors and stories.

When explaining the use of PGP or other kinds of encryption used to protect the contents of email, for example, it may be helpful to describe the process in terms of ordinary objects, such as putting a letter into a locked box, before describing the technology behind it.

Make it Participatory

To a certain extent, lectures cannot be avoided in trainings – this is typically a one-way communication where trainers will speak on a specific topic that they are knowledgeable about and open the floor for questions. Trainers need to watch out that they don't just talk to the participants in monologue. Here are a few things a trainer can do to make sure that the lecture does not become a monologue:

- **Prepare to stop before starting.** Outlining the lecture with breaks (points to stop and ask questions from the participants) will help break this monologue.
- **Try to "read" the energy level of participants.** Some indicators of low energy are:
  - **Lots of nodding heads.** This may not be an indicator of the participants agreeing with everything a trainer is saying but rather that they have stopped paying attention, and are only nodding because they don't want to appear to be not paying attention. (To check, the "nodding heads" can be asked a question. If they look confused, chances are they are not "there.")
  - **Distracted behavior.** Tapping feet, tapping pens, fixing hair, checking nails. This behavior means that people have lost interest.
- **Low-energy indicators are cues for a trainer to stop and ask questions.** If the energy level in the room feels low, and the participants are not paying attention, a quick break or an energizer may be helpful.

Preparing Presentations

Many trainers use presentations for workshops as part of the standard trainers' routine. And there is undeniable value in using PowerPoint, Prezi or another presentation program in a training context – a prepared visual presentation can address language differences and focus participants' attention. However, presentations can also become an ineffective one-way training tool. In cases when a presentation needs to be used, it needs to build in space for "open forums" so that the participants can ask their questions:

- The presentation should be no longer than 10 minutes in a 90-minute session and the number of slides should not exceed seven.
- Presentations are not meant to be read by participants; they are meant to support what trainers are saying. A glob of text on the presentation slide is not a good idea.
- Design the slides to end with a question (or a set of questions), so that the trainer is reminded to stop speaking. PowerPoint presentations need to facilitate a discussion.

Value of Hands-on Learning

Hands-on activities are the staples of any technical training. Participants learn best when they are able to learn by doing – in this case installing and using new software that will enhance their safety. Not all participants may be as used to handling a computer as their peers. In these instances, trainers need to be careful they do not take over the mouse to show the participant what to do. When participants are not allowed to learn by doing, the hands-on activity becomes a learning barrier. The best way to help these participants is for the trainer to physically stand behind a participant during the hands-on activity, guiding them rather than taking control of the mouse.

- **The best hands-on exercise happens when trainers are able to work in training teams.** The best-case scenario is when one trainer stands in front, demonstrating the steps in the exercise (his or her computer can be projected onto a second screen), and one or more trainers (or assistant trainers) walk among the participants, providing supportive guidance as they follow the steps.
- **Show, don't tell.** Trainers first need to demonstrate, then get participants to install/uninstall and then check their work. Use a projector at the front of the room with additional instructors to help walk through each step and ask the participants if they are following. Questions like "Is this what you can see on your screen?" or "Is this what happens when you clicked this box?" is a good way to know who is following the demonstration and who is falling behind.

Have Fun!

Ultimately, the goal of sharing knowledge is to help others. People learn in a variety of styles and formats, but they share a universal love of fun. If they feel they have attended a fun-filled event, where they have learned new things, then your work as a trainer has been successful.

Manisha Aryal and Dylan Jones

PRETRAINING QUESTIONNAIRE FOR ORGANIZERS

To be sent by the trainer to ORGANIZERS.

Trainers are encouraged to adapt the following questions to suit their training goals. Not all questions may be relevant or necessary for some trainings; other trainings may require additional questions.

NOTE: *It is advised that you distribute the questionnaire in person to avoid using less secure methods.*

1. Have the participants attended a digital security training before?
2. Do participants have access to a technical specialist who can help them with digital safety tools and practices outside of class?
3. Has anyone in your organization had a device stolen or confiscated? Has anyone lost a device with sensitive information on it?
4. Has your organization ever been a victim of a cyberattack (virus, loss of data, communication interception, email/social network hacking, website shutdown)? Please provide a brief description of the event(s).
5. As far as you know, has your organization been under surveillance?
6. Are you able to supply laptops for each participant in the training?
7. If yes, will the laptops be examined for viruses or other malware prior to the start of training?
8. What operating systems will the participants be using? (And are the operating systems genuine?)
9. Will an Internet connection be supplied during the training?
10. If so, will the connection be shared with your organization's staff?
11. Is the connection sufficient to support a video stream from YouTube that might be used for demonstration purposes?
12. Is the Wi-Fi connection secured with a password?
13. If so, does the Wi-Fi access point use WPA2 encryption to protect the activities of participants?
14. Will each participant have a smartphone?
15. What mobile phone brands/networks will the participants be using?
16. Is the use of encryption legally permitted? (Is there a ban on the use of VPNs or the use of software that encrypts data that is stored on a PC)?

PRETRAINING QUESTIONNAIRE FOR PARTICIPANTS

To be sent by the trainer to PARTICIPANTS.

Trainers are encouraged to adapt the following questions to suit their training goals. Not all questions may be relevant or necessary for some trainings; other trainings may require additional questions.

NOTE: *It is advised that you distribute the questionnaire in person to avoid using less secure methods.*

1. Do you use PCs (or Macs) or mobile devices when you are reporting?
2. If your phone or tablet is your primary reporting tool, what make and model is it and what operating system does it run? (iOS? Android?)
3. What operating system does your computer use? (Windows? Mac OS?)
4. How do you usually connect to the Internet? (Wi-Fi at the office? At home? Internet cafe?)
5. What web browser do you usually use?
6. What search engine do you usually use when researching information online?
7. Do you use voice, video or text chat programs to contact/interview your sources? (If so, list those you use most, e.g., Skype, Google Chat, etc.)
8. Do you know about SSL connections? Do you know the difference between HTTP and HTTPS?
9. Have you used privacy tools such as a VPN or Tor?
10. Is your computer's hard drive password protected?
11. Do you ever use personal email accounts for work?
12. Do you use Facebook, Twitter and other social networks? If so, which ones?
13. Have you ever had a device stolen or confiscated?
14. Do you have access to a technical specialist when you have questions about digital safety tools and practices?
15. Have you ever attended a privacy training? If yes, what topics were covered?
16. What topics would you like this training to cover?
17. Will you bring your own laptop to the training?
18. Will you bring your own smartphone to the training?

1. ASSESSING RISKS

WHY THE TOPIC MATTERS

Journalists handle sensitive information and the devices that contain them on a daily basis. Few have considered the risks to these assets and the potential consequences of losing control of them during a theft, confiscation or natural disaster.

Risk assessment is a systematic process of taking stock of physical and digital assets, identifying layers of risks and vulnerabilities, and coming up with a plan to address them. This module will include some tools for assessing digital and physical threats and will encourage participants to consider:

- The value of their work and the information they depend on for their work (e.g., contacts).
- Personal habits that may put their work at risk.
- A practical level of safety and privacy in an office.

WHAT PARTICIPANTS WILL LEARN

Concepts: Risk assessments, safety plans.

Skills: Basic methods for assessing common digital and physical risks to data in the work environment.

NOTE TO TRAINERS:
Solutions to digital safety challenges usually start with becoming aware of the risks. For this reason, we recommend that trainers consider starting with this module before moving on to the remaining topics. Although journalists face different kinds of risks in their daily lives, this module is limited to risks to devices and digital connections.

OBJECTIVES:
Learning to identify and prioritize risks.

PRACTICAL USES:
Identifying and protecting sensitive data and equipment.

PREREQUISITE SKILLS:
This module does not require prior technical knowledge.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- Guide: "How to Protect Your Information from Physical Threats" (Security in-a-box).
- Guide: "Threat Assessment & the Security Circle" (Equalit.ie).
- The SSD Project: "Risk Management" (EFF.org).

REMINDER:
If this module is the first in a larger course, we recommend trainers spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Handouts

- Class Notes.
- Glossary.
- Assessment Worksheet: Physical Environment.
- Assessment Worksheet: Digital Security.
- Instructions: "How to Protect Your Information From Physical Threats" (Security in-a-box).

Personnel

- We recommend that trainers alert the IT support staff of the media organizations participating in the training to be present (to answer questions) when this module is taught, particularly during the Activity and Deepening sessions.

RELATED MODULES

- As mentioned above, we recommend that this module precede other modules in this toolkit so that the participants understand the full range of risks journalists face.
- Some trainers will want to pair this module with the module on Malware and Basic Protection as, together, they address a broad range of common risks and solutions.
- Other digital safety modules may contain useful suggestions for mitigating or eliminating the digital threats that participants identify in this module.

LESSON PLAN

1. ACTIVITY (20 MINUTES)

Risk Hunting

This activity invites participants to explore a mock room or a "risky space" (a place that has been set aside in the training venue, or a separate room) to identify potential risks to equipment and data. In this activity, the space is prepared in advance and the trainer will keep a list of risks that have been intentionally left for participants to find.

Preparation

Prior to the start of the class, the trainer prepares the "risky space" with several risks left intentionally visible. These might include:

- Open windows.
- Door with key hanging from the lock.
- Laptop(s) without a locking cable on a desk.
- Wires or cables for devices that have been strewn on the floor where someone would need to step over them.
- Power plugs dangling loosely from a power strip near paper.
- Open desk drawers, with an external hard drive sticking out.
- Passwords written on a "sticky note" or other paper taped to a monitor or onto the surface of a desk.
- An open bag with a smartphone, camera or other valuable device exposed in it.
- A flash drive, left in a computer's USB socket.
- Computer left unattended with active Outlook, Gmail, Skype or other communication application open and visible.
- Laptop(s) without a locking cable on a desk.

NOTE: *This is only a list of a suggestions. This can be modified to fit the requirements of the participants and a risky habit practiced by participants that trainers want to draw attention to.*

Conducting the Activity

At the start of the exercise, the trainer explains that the purpose of the module is to learn ways to identify risks to journalists and their electronic devices. Since journalists often have to be good investigators, this activity should be perfect for them. The trainer then:

- Invites participants to walk up to or around the prepared space (or view a prepared photograph) for five minutes and take notes of risks they see.
- Organizes participants into groups of two or three and asks them to work together to share their findings with each other, and to then take five minutes to write their observations on a sheet of chart paper.
- Reminds participants that some "risks" will be obvious while others may not be obvious to all members in the group, and encourages discussion among participants to explore their views.
- When 10 minutes are left in the activity, asks teams to take turns presenting their "risks list" and to explain why individual items on the list might create a risk.
- Takes some time to point out any prepared risks that the group has not identified.

ADDITIONAL MATERIALS:

- Chart paper.
- Marker pens.
- A dedicated space that can serve as the "risky space."
- Equipment and furniture that can be used in the "risky space."

NOTE: It is not essential that furniture match the work spaces of participants, but the closer to an authentic work space, the more effective the activity is likely to be.

Alternatives

1. In cases where there is insufficient time or room to create the "risky space," the trainer may wish to substitute this activity with the "Day in the Life," described at the LevelUp website.
2. In cases in which participants belong to the same media organization and the event takes place at their office, trainers may prefer to divide the class into teams and ask participants to assess their normal work surroundings. This encourages participants to look at familiar territory in new ways and provides an immediate, practical benefit to the organizers of the event.

2. DISCUSSION (10 MINUTES)

Frequently, the Risk Hunting activity (above) leads to an extended discussion on its own when teams take turns presenting their findings. However, if time remains, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion. Trainers are welcome to add to this list or improvise as they see fit.

Trainers are welcome to add to this list or improvise as they see fit.

As always, trainers should encourage each person to speak up. It is likely that some have thought carefully about the issues; others may not have thought too much. This exercise will likely reveal some interesting practices, which makes for a rich discussion.

- Did anything in the exercise remind you of your office or your workspace? Did it look similar? Very different? In what ways?
- Why do you think risks like these are common in newsrooms or workspaces?
- Do you think these risks only affect the person using the workspace or would other people in the office be affected by these risks? How?
- What kinds of risks are present in public spaces? Do you see similar issues in IT cafes, for instance?
- Do you know of examples where:
  - A journalist's personal safety was compromised? Do you know what happened?
  - A journalist's property or data was compromised? How did that happen?
- What kinds of precautions do you take to protect your physical safety or the safety of your work?
- Has anyone in this group conducted a risk assessment? If someone has, ask the person to explain how he or she went about in the exercise.

3. INPUT / LECTURE (30 MINUTES)

This section includes recommended case studies, key messages and some materials to help get the point across.

Trainers are welcome to add or improvise as they see fit.

Case Studies

The following case studies examine digital safety risks that would not have been included in the opening activity (Risk Hunting) and are included to raise awareness about a broader set of challenges.

A. Sharing Files Can Put Lives at Risk

Introduction: As journalists, we're constantly researching and sharing information. Even as we take steps to ensure the protection of our data, this case reminds us that it is just as important, internally within the media organization, to pay attention to who has access to that information. This is especially important to remember when reporters rely on the Cloud to share files.

Story: A newsroom in Afghanistan was using Dropbox for file sharing. It was a collaborative news project and everyone working on each of the investigative stories had access to all the files and folders, including sensitive information. No one was keeping track of what was in the shared folder, who had access to specific files, and which of the many members could share or had shared which folders with other individuals not connected to the project.

During the course of investigating the story, one of the team members was asked to leave the news organization. As he left, he returned all the hardware (including laptop, camera, and flash drives) that he had in his possession. However, no one remembered to revoke his permission to the Dropbox folder.

The outgoing team member joined another news organization and published an article that used all the information that his former colleagues had so painstakingly collected. In the process, he also revealed the identity of a source that wished to remain anonymous and sensitive information that could be traced to the source.

The source had to be spirited out of the country.

B. Loose Lips and Open Devices

Introduction: The first case study was an example of one sort of risk – losing control of data stored online. The one below looks at the loss of control of data in a physical environment.

Story: An international media training organization was conducting a digital security training for Libyan activists and bloggers in Turkey. The organizers openly discussed where the training was being held, how many were to be involved, the names of participants, the equipment participants were carrying, and the equipment they were to be given upon arrival, etc.

When the training was completed and the participants were crossing the border to return home, they found that a new checkpoint had been established with the specific purpose of searching them. The reporters were carrying laptops, cameras and flash drives with encryption programs, and circumvention and anonymizing tools. Their vehicles were searched, their laptops confiscated, and three of the training participants were taken into custody by the border security forces.

One reporter was eventually set free, but the other two died in custody.

Interaction with the Participants

In each of these cases, the trainer asks participants what they think the journalists and their organizations could have done differently.

- **For Case Study A:** What could the Afghan news organization have done to ensure that they did not lose control of their information and to reduce the chances of damage? Could a policy of updating the list of people with access to shared folders have helped? What would you do in a similar situation?
- **For Case Study B:** In your opinion, where were the vulnerabilities? Should the people who were affected not have trusted their own colleagues? What would your suggestion be to the organization when running a similar training in the future?

Using the case studies, the trainers can make the following points:

Specific to Case Study A:

- Depending on the security environment, any file can be considered sensitive.
- Control where information is shared and sent. Information should not be shared with anyone outside of a need-to-know basis, and controls should be in place to ensure that people receiving information do not share it repeatedly.
- Reviewing access and changing passwords at regular intervals is a good idea.

Specific to Case Study B:

- In some places, just having these ICTs can be cause for arrest.
- Sensitive information on devices can be a target and a reason for profiling and arrest.
- Consider two sayings: "Even walls have ears" and "Loose lips sink ships."

Talking Points for the Trainer

With the case studies concluded, the trainer now directs participants to follow their Class Notes.

In this session, we recommend that trainers begin by explaining that the opening Activity and the subsequent Case Studies were intended to give a sense of the variety of challenges that journalists face. The remaining material in the lesson is intended to show how a risk assessment can help identify solutions to those challenges and jump-start the creation of a safety plan.

1. Risk assessment is a process that involves:

- Identifying valuable assets (e.g., contact lists, research data, interview notes or audiovisual files).
- Determining what threatens those assets.
- Assessing when and where the threats are likely to hit.
- Weighing the potential consequences.
  - ✔ Answering these questions not only provides a full picture of what hardware and information is at risk; it also helps a journalist prioritize what's most important. No reporter wants to lose the work they've completed on their current article, for example, but they also cannot do their work without their contacts list!

2. When conducting a risk assessment, it may help to think of your environment in layers:

- **Neighborhood.**
  - ✔ Do your neighbors share your concerns about safety? Are there ways you can help one another to make your homes or offices more secure?
- **Outside the office.**
  - ✔ Can anyone walk into the office? Can people reach your Internet or phone equipment from a window? Is your office Internet access point visible to people immediately outside?

TRAINER'S NOTE:

Text with a ✔ does not appear in the student version of the Class Notes.

- **From the front door.**
  - ✔ From the front door of your home or office, can you see potential vulnerabilities? Are you sharing your project details or your ideas with visitors or people walking by the window? Could someone walking by have physical access to your network cables or to a PC?
- **At your desk.**
  - ✔ Is your PC locked down with a cable or padlock, or can anyone walk off with it? Is it protected with a password? Have you taken steps to prevent dust, excessive heat or power surges from impacting the PC? Keeping your work area clean, making sure the PC is ventilated and employing an uninterruptible power supply (UPS) may help.
- **Your digital "space".**
  - ✔ Are your devices protected with passwords? Do you have any policies or guidelines that you follow when sharing materials or communicating with others?
- **Your "human network".**
  - ✔ Who do you know? Who do you trust? Who should have access and who shouldn't?

3. A safety plan identifies actions you can take to address the threats. Questions that may help formulate your plan include:

- What risks can be eliminated entirely and how?
- Which ones can be mitigated and how?
- Based on their likelihood and significance, which risks should be addressed first?

✔ It is assumed that journalists and their bosses won't be able to address all threats at once. They should be prepared to schedule work on this project, just as they would on any other.

4. Things to keep in mind:

- **Be inclusive in your planning.**
  - ✔ Your own risks may depend on other peoples' habits. Having group discussions about safety policies is important.
- **Be judicious with permissions and access.**
  - ✔ Does everyone in the office have access to all the data or devices in that office? Should they?

TRAINER'S NOTE:
This module is intended as a primer on the subject of risk assessments. However, if trainers wish to learn more about prioritizing risks and the formulas that are sometimes used to generate detailed risk scores, the following material from Equalit.ie provides a more thorough explanation and guidelines: "Threat Assessment & the Security Circle."

4. DEEPENING (90 MINUTES)

This section is divided into risk assessment and safety plan exercises. We recommend the **trainer set aside approximately 60 minutes for the first exercise and 30 minutes for the second.** Participants should be told at the outset that the purpose of the exercises is to help them start a practical risk assessment and action plan.

Exercise #1: Identifying Risks (60 minutes)

The trainer distributes the assessment worksheets at the start of this session:

- Assessment Worksheet: Physical Environment
- Assessment Worksheet: Digital Security

The goal of this exercise is to provide participants with a team-based approach and some tools to begin a risk assessment for their workplace. The trainer guides the participants through the following steps:

- Divides participants into two teams, one of which will focus on physical safety and the other on digital safety.
- Explains that 30 minutes will be spent on identifying risks and prioritizing them. Everyone should return to the training room at that point and be prepared to contribute to a group list of identified risks.

  NOTE: *In the event the training takes place in a single office, this exercise greatly benefits from the presence of one IT support staffer. However, if training is at a remote location such as a hotel and includes participants from several organizations, trainers may wish to divide participants by organization or job type to create personalized checklists.*
- At the end of 30 minutes, collects the participants and facilitates a discussion in which he or she writes on chart paper a collective list of risks spotted by participants.
- Asks the class to prioritize the risks based on the likelihood of each threat and what level of impact the threat could have. For example, earthquakes are potentially devastating no matter where they occur (high impact), but they may be rare in some regions (low likelihood).

Exercise #2: Starting a Safety Plan (30 minutes total, with 10 minutes to present findings)

This exercise builds on the previous exercise. The trainer guides the participants through the following steps:

- Divides participants into two teams and alerts the teams they will have 20 minutes to build on the work they just concluded.
- Asks Team A to brainstorm ways to avoid or mitigate the risks that were identified in Exercise 1. Participants should list these on a single list of chart paper. Team A should take the following into consideration:
  - Assuming they may not have all the answers, who are the key people they could ask for help and recommendations?
- Asks Team B to create guidelines that their office (or any office) might follow when trying to conduct a comprehensive risk assessment and the safety plan (or action plan) to implement recommended solutions. Team B should take the following into consideration:
  - Who are the key colleagues who would have to be involved in any comprehensive risk assessment? (Generic titles are fine: e.g., "managing editor.")
  - Who will have to make key decisions in order for safety-related changes, such as new policies, to be implemented?
  - What would a reasonable schedule look like?
  - What tools could be used in the office to educate colleagues about changes in security policies when they are rolled out?
- When **10 minutes** are left, asks teams to present their findings.

ALTERNATIVES:
In cases where participants do not have immediate access to their offices or to IT support staff, trainers may wish to split up the Deepening exercises and assign Exercise #1 (Starting a Risk Assessment) as homework before conducting Exercise #2 on the following day.

For additional ideas and related activities, visit the **LevelUp** website.

5. SYNTHESIS / CONCLUSION (15 MINUTES)

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

- Outside the work environment, do you think risk assessments have a practical use for you personally?
- Based on some of the topics we've discussed, is there anything that you know you do, or that you see in your office, that you would change immediately?
- What do you think will be the biggest challenge in trying to conduct a risk assessment and create a Safety Plan for yourself or the organization that you work with?
- What challenges do you foresee in implementing the safety plan?
- Some people have said that physical security, personal (data) security and network security are not separate things, and instead are dependent on one another. Would you agree?

NOTES

- Assessing risks is a process of:
  - Identifying valuable assets (e.g., contact lists, research data, interview notes or audiovisual files).
  - Determining what threatens those assets.
  - Assessing when and where the threats are likely to hit.
  - Weighing the potential consequences.
- Questions commonly used in the process:
  - What is valuable that needs to be protected? (E.g., phones, laptops, important articles and photographs.)
  - How likely is it that specific information or a device is in danger?
  - What are the most likely sources of threat to that material? What are the human threats (such as thieves or someone who could confiscate equipment), infrastructure threats (such as pirated software or poor power supplies), and environmental threats (such as natural disasters)?
  - What is the potential impact of an individual device or type of information being lost, stolen or destroyed? Would the impact be big or small?
  - What can we do to mitigate the risks?
- When assessing risks, it may help to think of your environment in layers:
  - Neighborhood.
  - Outside the office.
  - From the front door.
  - At your desk.
  - Your digital "space."
  - Your human network.
- A safety plan is your response to the threats you have identified. Questions that may help formulate your plan include:
  - What risks can be eliminated entirely and how?
  - Which ones can be mitigated and how?
  - Based on their likelihood and significance, which risks should be addressed first?
- Things to keep in mind:
  - Be inclusive in your planning.
  - Be judicious with permissions and access.

For Further Learning:

- Guide: "How to Protect Your Information from Physical Threats" (Security in-a-box).
- Guide: "Threat Assessment & the Security Circle" (Equalit.ie).
- The SSD Project: "Risk Management" (EFF.org).

ASSESSMENT WORKSHEET: DIGITAL SECURITY

TRAINING:

DATE:

GROUP:

MEMBERS:

1. WIRELESS ROUTERS:			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Is the wireless connection you use protected with an encrypted connection? (In other words, does your router ask for a password before you can connect?)	Example: *Neighbors, hackers parked near the office*	Example: *High*	Example: *Turn on WPA2 encryption in the router's settings and protect it with a strong password.*
Are you using strong passwords for your wireless connections? *(For tips, see the handout, "Creating and Maintaining Strong Passwords.")*			
Does your router use WPA2 encryption? *(WPA2 encryption is generally the strongest.)*			
Are routers located away from public areas where someone can intentionally or accidentally tamper with them? *(Reception areas, waiting rooms, and kitchens tend to be accessible to members of the public and not safe.)*			
Has the administrator password on the router been changed from its default setting so that only someone with authority or permission can change the device's settings? *(If not, the router's user manual will provide instructions for doing so.)*			
In your router's settings, have you disabled Web access – sometimes called WAN administration – so that people outside the office cannot change your router's configuration? *(If not, the router's user manual will provide instructions for doing so.)*			
Additional notes/discussion points about wireless routers:			

2. INFRASTRUCTURE AND MAINTENANCE			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Is someone on staff responsible for technical matters and able to look after emergencies right away (e.g., set up the office network or recover lost data)?			
If not, is there an outside contractor or company you hire for IT tasks in your office and is their contact information available to key personnel?			
Does the office maintain its own server(s)? If Yes, go to the questions below:			
Is online access to the server protected? 1. Is the firewall enabled? 2. Is access restricted to administrators? 3. Are accounts protected with strong passwords?			
Is physical access to the server(s) protected? *(Is each server locked and kept away from water, direct sunlight and public areas?)*			
If your office runs its own server(s), are precautions being taken to protect against malware and is the operating system kept up-to-date?			
Additional notes/discussion points about infrastructure and maintenance:			

3. STAFF MEMBERS AND HABITS:			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Do all staff members have anti-virus software installed on their PCs at the office? If so, is the anti-virus software updated automatically or on a regular schedule?			
Are all PCs in the office set to automatically accept updates to the operating system? Outdated operating systems are frequently used by hackers to gain remote control of PCs.			
Is encryption software being used to protect files or PCs at the office (e.g., BitLocker or TrueCrypt)?			
Are all staff members required to use strong passwords on their work accounts? *(For tips, see the handout, "Creating and Maintaining Strong Passwords.")*			
Do staff members use the same password for more than one online account? *(This is not recommended because that password can then open access to more than one account.)*			
How do staff members keep their passwords safe? Do they use an encrypting application like KeePass?			
Do staff members use unlicensed software? If so, list at right in the Source of Risk column so that you can more easily search for free, genuine alternatives at a site like osalt.com. In addition to breaking copyright law, unlicensed software often comes with malware (viruses).			
Are staff members allowed to use personal email accounts for work? If so and if these accounts have received phishing attacks (fake emails) or have been hijacked by hackers, has that presented a problem for the office network, other PCs or work documents?			
Do staff members use personal laptops at the office? If so, do you have minimum requirements for these laptops before they can use the office network?			
Additional notes/discussion points about staff members and habits:			

4. SHARED SERVICES AND ACCESS POINTS

Vulnerability	Source of Risk	Risk Level (low, medium, high)	Possible Solution
Do staff members use file-sharing services that are not controlled by the office (e.g., Dropbox)? Are the files encrypted or protected in some way? If so, please list them in the Source of Risk column and explain the protection.			
Do you or your colleagues ever use public access points, such as those at coffee shops?			
If so, you may wish to establish guidelines for using work laptops at public access points. *(Tips for connecting to sites securely can be found in the "Safer Surfing" chapter of SpeakSafe.)*			
Does the office provide a public access point for visitors? If so, is this kept separate from the staff's network?			

Additional notes/discussion points about shared services and access points:

5. BACKUP PLANS AND SCHEDULES			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Does your office have a backup plan or policy that applies to all PCs at the office?			
Do you have a **uniform** method for backing up data on your PCs? If not, do you think backup tasks would be more reliable if you adopted one?			
Does your office keep one copy of its backups on the same site as the original data so that backups can be accessed in emergencies?			
Does your office keep a copy of its backups at another location outside the office, to avoid destruction of both originals and backups in the case of natural disaster or theft?			
Does the entire office staff have physical access to all backups or is access limited to key personnel?			
Are backups encrypted to protect them from people who do not have permission to use them?			
Additional notes/discussion points about backup plans and schedules:			

6. MOBILE PHONE SAFETY			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Do staff members have sensitive information related to work stored on mobile phones (photos, audio interviews, essential contact information, etc.)?			
Would staff members benefit from reviewing online materials about mobile phone security? (*Security in-a-box has an excellent "Mobile Security" guide.*)			
Do staff members use a long password to prevent access to phones? (*A long password is safer than a PIN number.*)			
Are staff members protecting the data on their phones with an encryption feature? (*Android, iPhone and Blackberry devices allow users to enable encryption in Settings.*)			
Do staff members use text messages to share information related to work? (*Text messages are visible to the phone service provider and to whomever has access to that provider's records.*)			
Do staff members use an application like ChatSecure (for Android) to send instant messages to one another? (*Developer's website has excellent information about ChatSecure.*)			
Do you or your colleagues make backups of "crucial" phone data, such as contact lists, and keep these backups encrypted?			
Additional notes/discussion points about mobile phone safety:			

ASSESSMENT WORKSHEET: PHYSICAL ENVIRONMENT

TRAINING:

DATE:

GROUP:

MEMBERS:

1. AWAY FROM THE OFFICE			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Do you or your colleagues travel with laptops and phones and have a way to make these devices physically secure where you stay? (Do you keep your devices with you at all times or have a lock to physically secure them?)	Example: *Loss (forgotten)* *Theft from other travelers or pickpockets* *Confiscation by authorities*	Example: *Medium*	Example: *Bring cable and lock on trips* *Keep laptop in carry-on luggage and keep carry-on nearby* *Keep phone hidden inside pocket*
Do staff members take office laptops and work information home? What precautions are taken to reduce the risk of theft?			
Additional notes/discussion points about security away from the office:			

2. YOUR BUILDING

Vulnerability	Source of Risk	Risk Level (low, medium, high)	Possible Solution
Are points of entry to the office (doors and windows) protected with locks?			
Do you or your colleagues stand outside the office with the doors open (to smoke, to make personal cell phone calls)?			
Are windows at ground level normally open during the day and left unattended?			
Is your office Internet and telephone connection easily accessible from a circuit box on the outside of your building?			
As far as you know, is your office currently under surveillance from a neighboring building?			
How does your office monitor office visitors prior to giving them entry into the office? (Does it have a glass door, peephole, video cameras and/or other means to monitor visitors?)			
Does the office have security protocols for allowing visitors that may not be known to all staff members (ID check, cell phone deposit, metal detector, body scan, etc.)?			
Additional notes/discussion points about building security:			

3. IN THE OFFICE			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Can guests who walk into the office immediately see your computer screen(s), white boards or other places where business information is visible?			
Are story meetings and team meetings held in open spaces where visitors who are not involved may hear?			
Are network devices like your routers, hubs or modems kept in secure rooms or cabinets so that intruders won't have direct access to them?			
Are your desktop computers and laptops attached to a security cable with a lock to prevent theft?			
Additional notes/discussion points about risks in the office:			

4. COMMON ELECTRICAL RISKS			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Do power strips or wall sockets consistently spark when you plug a device into them, indicating a fire hazard?			
Are computers and other sensitive equipment kept in direct sunlight, which could potentially lead to overheating?			
Do computers kept inside cabinets have adequate ventilation to avoid overheating?			
Do you use an uninterruptible power supply (UPS) in your office? *(A UPS stabilizes the power reaching your PC and can provide temporary power in the event of a blackout.)*			
Are your PCs and cables kept clear from hallways, reception areas and other places where people walk frequently?			
Are your network cables away from windows where rain might damage them and cause an electrical short?			
Additional notes/discussion points about common electrical risks:			

5. MOBILE PHONES			
Vulnerability	**Source of Risk**	**Risk Level (low, medium, high)**	**Possible Solution**
Do staff members leave phones in plain view when meeting in public places (e.g., on the table at a cafe)?			
Do staff members keep phones with them at all times? *(This is advised during the work day, unless reporters wish to avoid broadcasting their physical location.)*			
Additional notes/discussion points about mobile phones:			

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

access point – Any point at which a device connects to the Internet, usually a wireless access point (Wi-Fi).

Bluetooth – A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions.

encryption – A way of using mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

firewall – A tool that protects your computer from untrusted connections to or from local networks and the Internet.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

Internet Protocol address (IP address) – A unique identifier assigned to your computer when it is connected to the Internet.

Internet service provider (ISP) – The company or organization that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.

malware – A general term for all malicious software, including viruses, spyware, Trojans, and other such threats.

phishing – Creating fake websites or email that appear genuine in order to lure Internet users to interact with the content. Frequently used to capture passwords and financial data.

physical threat – In this context, any threat to your sensitive information that results from other people having direct physical access to your computer hardware or from other physical risks, such as breakage, accidents or natural disasters.

router – A piece of networking equipment through which computers connect to their local networks and through which various local networks access the Internet. Switches, gateways and hubs perform similar tasks, as do wireless access points for computers that are properly equipped to use them.

security policy – A written document that describes how your organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place.

security cable – A locking cable that can be used to secure a laptop or other piece of hardware, including external hard drives and some desktop computers, to a wall or a desk in order to prevent it from being physically removed.

server – A computer that remains on and connected to the Internet in order to provide some service, such as hosting a Web page or sending and receiving email, to other computers.

service provider – A company, either private or public, that provides mobile phone service or Internet service to customers.

2. MALWARE AND BASIC PROTECTION

WHY THE TOPIC MATTERS

When a PC becomes infected with a virus or other malware, journalists can lose control of their equipment, email accounts and other data that's essential to their work. A nasty "worm" infection can spread itself across an entire office network. The consequences can be significant for others, as well: An infected PC can provide a hacker with access to sensitive communications, research and other files.

WHAT PARTICIPANTS WILL LEARN

Concepts: Computer viruses related to our behavior (and software).

Skills: Using the Avast! anti-virus application and keeping operating systems and software up to date.

OBJECTIVES:
Learning about common methods of attack and anti-virus applications.

PRACTICAL USES:
Preventing infections on a PC, detecting fake emails.

PREREQUISITE SKILLS:
The module assumes that the participants are able to:

- Identify operating systems.
- Install applications.
- Save and locate files on their computer.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- "Malware FAQ" (SANS Institute).
- "A List of Computer Viruses" (Wikipedia).
- "How to Protect Your Computer from Malware and Hackers" (Security in-a-box).

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Software & Installation

- Avast!.
  - Guide.
- ClamWin.
  - Guide.

Handouts

- Class Notes.
- Glossary.
- "How to Protect Your Computer from Malware and Hackers" (Security in-a-box).

NOTE: *Trainers requiring information related to Apple devices should consult the "Mac OS X" training notes found immediately afterthe Synthesis section of this module.*

RELATED MODULES

While learning to protect one's PC from malware relates to every module in this course, the following modules are closely related, as they involve sending and receiving email as well as visiting websites that may be unfamiliar to the user:

- Researching Securely.
- Protecting Email.

LESSON PLAN

1. ACTIVITY (20 MINUTES)

Virus Busters

This activity is intended to highlight a common way that PCs get infected with computer viruses: through fake emails (called "phishing") and viruses in attachments. The goal is to show participants that they may be able to avoid many potential infections just by paying attention to what is in their Inbox.

Preparation

Prior to class, trainers should review the following article at the Electronic Frontier Foundation (EFF) website: Vietnamese Malware Gets Very Personal. We also recommend that trainers bookmark pages with screenshots or download them prior to class so that they can be easily projected onto a wall or printed as handouts.

Conducting the Activity

The trainer asks participants if they have heard of computer viruses and then asks if they know of some of the most common ways that PCs become infected. If participants offers the suggestion "email", the trainer can move directly onto the next step of the activity. If not, the trainer may wish to explain that email is one of the most common tools that hackers use to infect PCs. They may do this in a variety of ways, as the class will now discover.

The trainer then projects the first screenshot from the EFF article, which shows the email that was received by that organization and a journalist at the Associated Press.

The trainer announces, "Something doesn't feel right about this email, but I don't know what it is. Can you help me figure it out?"

At this point, the trainer starts at the top and works his or her way down. Participants should be allowed to spot the problems first, but if they need some help, this list identifies some of the problems:

- What about the sentences in this email? The text in the email has several typos in it. For instance, there are no periods at the end of sentences and the sentences may seem awkward to native English speakers.
- How about the email address of the person who sent this email? It appears to be andrew.oxfam@gmail.com. Is there anything strange about that? Would Oxfam be more likely to have its own email, such as "oxfam.org"?
- This email asks the recipient to click on links to get some information about an invitation. Those links are the very long (blue) strings of letters and numbers near the bottom of the email. Does anything seem odd about them? The links appear to point to "www.oxfam.org" (notice that there is a difference between the website address and the email address of the person who sent this email). However, when the details of the links are examined, it's possible to see that the links actually point to a different location, a shared file in someone's Google Drive folder.

The trainer asks participants what they think might happen if someone clicked on one of the links or one of the attachments in the email. Answer: The EFF determined that the links would cause the PC to install a virus.

REMINDER:
If this module is the first in a larger course, we recommend you spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

The trainer writes two words on the flipchart:

- "Malware"
- "Phishing"

The trainer writes the words "Malware" and "Phishing" on a flipchart and explains their definition:

- "Malware" is what infects your PC. The word is a combination of "malicious" and "software," and it refers to viruses of all kinds.
- "Phishing" is the electronic equivalent of fraud. It is the tricking of a user into clicking a malicious link or exposing private information, such as a password, by presenting him or her with a fake email, instant message or website that appears genuine. This is a common way in which PCs become infected.

NOTE: *Trainers who wish to create more ambitious versions of this activity should review, "Analysing a Potentially Harmful Email", described at the LevelUp website.*

2. DISCUSSION (15 MINUTES)

With the activity completed, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion:

- Has anyone in the group had their PC infected? What happened as a result?
- How can our PCs get infected by a virus?
  - From infected hardware (such as USB sticks).
  - From unlicensed or cracked software (e.g., fake download sites).
  - By clicking malicious links to download viruses (e.g., fake advertisements).
  - By downloading them through malicious email attachments.
  - Through social engineering attacks (i.e., impersonation).
  - By downloading them through scams on social networking sites.
- How do we get phished?
  - Through e-mails that ask you to log in to your online banking account.
  - Through e-mails that ask you to log in to your social network accounts (e.g., "tvvitter.com" instead of "twitter.com").
  - Through private messages on Twitter with shortened links that bring you to a fake login screen.
  - Through Facebook wall posts and links that bring you to a fake login screen.
- What would you do if you received the email we looked at? (What would you tell a friend to do?)

  We recommend:
  - Deleting the email, or
  - If someone on staff or a friend is very advanced with technical issues, show it to them to see if they can determine where it came from. Was it from another country or did it come from your city, indicating you were the target?
- Are there any applications or browser add-ons that you know of that could help?
- How many people in the group have an antivirus application installed on their PC? What antivirus applications are you using? How did you choose the antivirus application you are using?
- How many people here update their operating system? Can you tell us why you do that?
- If you do not update your operating system, can you tell us why? (Are you concerned the piracy police will come visit you?)
- Does anyone here have an antivirus application installed on their smartphone?
- Let's review the words we put on the flipchart ("phishing" and "malware"). What are the meanings of these words?

Trainers are welcome to add to this list or improvise as they see fit.

3. INPUT / LECTURE (30 MINUTES)

This section includes a recommended case study, key messages and some materials to help get the point across.

Trainers are welcome to add or improvise as they see fit.

Case Study

FinFisher in Bahrain

Introduction: Most malware in the world is connected to criminal organizations trying to steal money. As journalists, we have no money. But we have something else of value to another group of people: information.

Story: In July 2012, the Citizen Lab, and an interdisciplinary research lab based at the Munk School of Global Affairs, University of Toronto, examined malicious software e-mailed to Bahraini activists from an account associated with Al Jazeera reporter Melissa Chang. Researchers examined the emails sent to pro-democracy activists and identified them to be infected with FinFisher (also known as FinSpy), a surveillance software sold by U.K.-based Gamma Group.

Bahrain has been tense since the 2011 government crackdown on mass protests involving those opposed to minority Sunni Muslim rule over the Shiite majority. Tests carried out at the Citizen Lab showed that if a recipient clicked on attachments – generally photos and documentation about human rights abuses in Bahrain – the spyware would secretly install itself. The malicious software then went through an elaborate process of hiding itself, checking and evading anti-virus programs, and establishing a connection with the server in Manama to which it would send its data.

Spyware like FinFisher is intrusive. It attaches to peoples' digital devices and carries out covert surveillance. Spyware and other malware can penetrate the most private spaces, secretly taking over control of a computer remotely, copying files, intercepting Skype calls, turning on Web cameras, and logging keystrokes.

Although a Gamma Group executive reportedly said in a 2012 email that "FinFisher is a tool for monitoring criminals, and that to reduce the risk of abuse of its products the company only sells FinFisher to governments," the targets were pro-democracy activists who had never been charged criminally.

The researchers watched how the malware behaved; they concluded that it acted as a Trojan, malicious software named after the wooden horse Greek warriors used to sneak into Troy before destroying the ancient city. The Citizen Lab researchers found that the compromised machines were reporting to a computer based in Bahrain. However, when Bloomberg reached out to the Bahrain government, Luma Bashmi, spokeswoman for the government's Information Affairs Authority, said in an emailed statement that the Bahrain government does not target political activists through surveillance technology.

FinFisher is only one of many surveillance tools available in the market. FinFisher was developed in the West and is being sold to governments worldwide that are willing to pay for its use. While traditional hacking techniques involved phone tapping, email and text message monitoring, which governments carried out by tapping into national communications networks, FinFisher allows them to go further and reach across political borders. It also allows governments who may not be able to develop their own cyberweapons to purchase sophisticated surveillance software.

"When FinSpy [FinFisher] is installed on a computer system it can be remotely controlled and accessed as soon as it is connected to the Internet/network, no matter where in the world the Target System is based," a Gamma Group brochure published by WikiLeaks says.

Sources:

- **Citizen Lab:** "From Bahrain With Love: FinFisher's Spy Kit Exposed?"
- **Bloomberg:** "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma."

Useful Materials:

- **Video:** "FinFisher Products and Services."
- **Video:** "FinSpy Surveillance Tool Takes Over Computers" (Bloomberg).

Interaction with the Participants

Using the examples above, trainers can help participants reflect on their own practices that may be putting their sources at risk. Some questions that may help:

- Do you click on all attachments that arrive in your Inbox?
  - If so, why? And has that led to your computer slowing down, crashing, losing data, etc.?
  - If not, why have you stopped before clicking?
- Have you worried about malware infection? Why? Do you have information that would make you vulnerable to such infections?
- If you have experience with malware, in what form has it arrived? As an attachment? Software update? Please share.
- If a source you are interviewing is being particularly difficult, would you be tempted to use spyware or malware to hack into their computer?
  - Why?
  - Why not?
- Do you think you can protect yourself? How? Please share.

Talking Points for the Trainer

With the case study concluded, the trainer now directs participants to their Class Notes.

✔ Antivirus application developers report that most PCs become infected with Trojan viruses – viruses that masquerade as something innocuous or even desirable. (Have you ever had a window pop-up that you didn't expect, from a company you never heard of, telling you that your PC was infected and that, just by clicking on a simple link, they can clean it for you?) Pandasecurity.com says three out of every four infections occur this way. This was the point of the Activity.

1. Viruses are a BIG problem:

- Tens of thousands of computer viruses have been recorded.

  Unprotected PCs have a very short "survival time" of only about six minutes!

  ✔ **"Unprotected PC" means:**
  - ✔ A Windows PC.
  - ✔ Without a firewall turned on.
  - ✔ With no anti-virus application installed.
  - ✔ That is connected to the Internet.

✔ The good news is that, since Microsoft released Windows 7, they have turned on a built-in firewall by default. But this figure of six minutes still tells us how aggressive some malware (a type that is called "worms") have become.

2. Who makes viruses?

- **Some hackers do it for money:** Conficker.
  - ✔ Conficker is a famous computer "worm" – a kind of virus that replicates itself onto any other device on a network. Conficker, which has been found on millions of PCs, was

TRAINER'S NOTE:

Text with a ✔ does not appear in the student version of the Class Notes.

intended to give hackers control of infected PCs for a variety of purposes. When many PCs (sometimes in the hundreds of thousands) come under the control of hackers, that array is usually called a "botnet" (see Glossary).

- **Some are developed as a service for intelligence:** Ghostnet.
  - ✔ Discovered in 2009, this spyware application gave remote control of PCs (including microphone and camera) to unknown hackers; some of the targeted PCs were used by the entourage of the Dalai Lama, and some by finance ministries in the ASEAN economic block.
- **Some … just because:** ILoveYou.
  - ✔ This virus required users to click on an attachment that appeared to be a simple text file. It resulted in "I Love You" appearing on the screen and image files on the PC being deleted or corrupted.

3. Common Myths:

- **Only Windows gets viruses.**
  - ✔ Mac and Linux also have viruses, though Windows has the most, probably because it remains the most popular operating system, estimated to be on more than 80% of PCs around the world. People who use these non-Windows operating systems should have an anti-virus application, in any case, to help stop the spread of viruses that they may otherwise unknowingly send to other people.
- **Smartphones don't get viruses:**
  - ✔ iPhone and Android platforms have viruses. This is probably because, more and more, people are using smartphones for things that they used to reserve for PCs, including chatting, emailing and purchasing.
- **An anti-virus will always clean an infected PC.**
  - ✔ Anti-virus applications are usually better suited to prevent infection than clean them up after they have occurred. Security experts generally advise that users reinstall their operating system and applications after they confirm they have been infected because it is increasingly hard for anti-virus applications to protect themselves once the operating system has been compromised.

4. Four helpers:

- **Anti-virus:** Blocks infection before it can take hold.
  - ✔ Examples of free anti-virus applications: Avast!, Avira, AVG.
- **Anti-spyware:** Blocks applications that send your information to someone else.
  - ✔ Spyware includes things like keyloggers (see Glossary) that record whatever you type and send that information to someone else so that they don't need to see your monitor to figure out your password on an account, etc. Examples of free anti-spyware applications: Spybot, SUPERAntiSpyware.
- **Malware scanner:** Locates and removes a virus or spyware application.
  - ✔ Examples of free malware scanners: Malwarebytes Anti-Malware.
- **Firewall:** Blocks Internet traffic you did not request. Can prevent unintended installation of software.
  - ✔ Sometimes, an infected device or an infected website may attempt to install malware onto your PC. A firewall can alert you to this and give you a chance to prevent the installation. We include additional information about Windows Firewall in the Deepening section.

5. Update everything:

- Anti-virus applications.
- Operating system (e.g., Windows).
- All other applications.

- ✔ For tracking your "other applications," some applications make this easier so you don't have to visit every website to check. Avast! anti-virus has a software version-checker built into it. Also, Secunia PSI looks for updates to the applications you have installed.

6. Protect your data with two backups:

- One nearby, one off-site.
  - ✔ An example of "off-site" might be the Cloud or a friend's house. This is to protect against a natural disaster or the seizure of equipment at an office.
- On a regular basis (e.g., weekly).
  - ✔ To limit loss, you may not be able to get back everything but at least you will have lost only a few days' work.
- Password-protected.
  - ✔ So that the backup is as secure as the original.

7. Block unintended installations:

- In Windows, make sure UAC (User Account Control) is running.
  - ✔ You can do this just by clicking Start and typing "UAC." The slider should never indicate "Never notify."

8. On a mobile device:

- Locate free anti-virus software for your platform at the official app store for your device.
  - ✔ The major brands all make one, including Avast!
- Don't install applications, wallpapers or ringtones you don't need.
  - ✔ They may contain harmful code, or may have access to sensitive information that they should not need (e.g., an alarm clock application that requests access to your phone records).
- Always update.

9. When all else fails and you are infected:

- Copy essential files that were not included in your most recent backup to some external media.
  - ✔ This could be a DVD or external device.
- Write down any license or purchase information related to paid applications (if you have any).
  - ✔ This is important because reinstalling the operating system will wipe away all the data on the device.
- Make sure you have your installation disk.
- Reinstall the operating system and applications.
  - ✔ This requires booting to the installation disk, and most people won't be comfortable with that. We recommend that people seek out desktop support personnel in their office for help.

Common Question:

- My copy of Windows is not genuine. Will Microsoft turn off my computer if I try to update it?

  No. Microsoft makes security updates available for copies of Windows, including pirated ones. However, pirated copies do not allow access to all Windows features. Users of pirated copies (software that is cracked and/or not registered) cannot use Microsoft's Security Essentials; Windows needs to recognize the software as genuine for users to be able to use the security feature.

4. DEEPENING (90 MINUTES)

This section is divided into anti-malware applications and updates. We recommend that the bulk of training time be spent on the anti-virus application Avast! and then on updates. The additional application ClamWin Portable can be addressed as time allows, but the crucial topics that will prevent the majority of infections are addressed in Parts I and II below.

SOFTWARE & INSTALLATION NEEDED:

- Avast!
  - Guide
- ClamWin Portable
  - Guide

PART I: Anti-virus Applications

NOTE: *As mentioned in the Talking Points, there are several free applications that can help protect PCs. Due to the limits of time, we have chosen specific applications for these exercises, but knowledgeable trainers may wish to explore other options.*

A. Installation and Walk-through of Avast!

Normally, we recommend that participants install software before entering the classroom. In this case, however, we recommend waiting until this section of the module because some participants will have an anti-virus application already installed.

If the trainer can determine that the participant's anti-virus application is pirated (and the only way to do this may be to ask), it is recommended that the participant uninstall that pirated anti-virus application and then install Avast!

Before walking participants through the installation process for an anti-virus, trainers need to know a few things:

- **Users do not need more than one anti-virus application.** Having more than one can cause instability. During the exercises (below), participants still need to be able to demonstrate that they know how to update their application.
- **All participants who install an anti-virus will be asked to reboot their PCs at the end of the installation process.** They should not choose to run a boot-time scan. Ask participants to bypass the option to run a boot-time scan when they restart their PC. A boot-time scan will scan the full contents of the PC and will not allow participants to access the Windows operating system while it is running. This will lead to lengthy delays in the class.
- **Avast! has a new design.** Like other applications, Avast! changes its design from time to time. In November 2013, the application had a significant update to the appearance of its free version. The materials we are providing, unfortunately, do not reflect the visual changes. We encourage trainers to keep a watchful eye on YouTube and other public resources for updated materials that may be available after the publication of this course.

Instructional Material that May Be Useful:

- Video tutorial (YouTube).
- Guide (Security in-a-box).
- Avast! technical support.

NOTE: *Trainers should note that Avast! has changed its design since the video and guide were produced. Some screenshots and images in the video may differ from the instructions.*

Trainers may want to stress the points below during the video presentation:

- An anti-virus application must be kept up-to-date to keep pace with new viruses on the Internet.
- The free version of Avast! will update automatically at least once a day but you can also trigger an update manually in the Settings tab of the application.
- After Avast! is installed and your PC is rebooted, you can scan an individual file on your PC by selecting the icon for that file, right-clicking once and then selecting Scan in the menu, next to the Avast! icon.

Exercise #1: Updating Avast!

Trainer shows participants how to update Avast! from two locations:

- With the application open, the trainer selects the Settings tab and then clicks the Update link to update the virus definitions and then the application itself.
- From the system tray, the trainer right-clicks the Avast! icon and selects Update→Engine and Virus Definitions.

This is just showing participants two ways to do the same thing.

We recommend that, as participants carry out this task, the trainer walk around the room to confirm that those with other anti-virus applications also know how to update their applications.

Exercise #2: Running a Quick Scan

The quick-scan application gives users a choice of a quick or full system scan. A full system scan will examine every file on every hard drive attached to the PC. For reasons of time, we recommend that the class conduct a quick scan, which limits its search to core system files in the operating system. To do so:

- Select the Scan tab.
- Quick Scan should already be selected by default in the drop-down menu.
- Click Start.

IMPORTANT: *To avoid time delays, trainers may wish to tell participants to cancel their scan (by clicking the Stop button) and, instead, assign a full system scan as homework. The trainer may wish to prepare his or her PC by keeping one infected file on the desktop to demonstrate what messages the participants would be likely to see if they had infected files.*

Exercise #3: Updating Other Applications With Avast!

The purpose of this exercise is to help participants understand that they can update the applications on their PC and that Avast! has a feature that can help:

- Open Avast! main window ("user interface").
- Select Tools and then Software Updater.
- Review the list of applications on display and see if any need updating.

Tips on Using Avast!:

- You will frequently see "up-sell" advertisements inviting you to turn on "automatic updates." This is Avast!'s way of trying to get people to buy the paid version of the application. You can ignore these invitations.
- If you have a graphics card on your PC, particularly an Nvidia graphics card, you may receive a warning at the end of a complete system scan that says "Some files could not be read." When you examine the details, you will usually find that it is the driver – a kind of application associated with the graphics card – that could not be read. This is normal and need not alarm the participants.
- It is recommended that you run a boot-time scan at least once for a higher level of confidence that your PC is clean. A boot-time scan examines files on the PC that would not be available if Windows was running.

NOTE: *Trainers can assign all participants to run a boot-time scan as homework instead of a full system scan.*

B. (OPTIONAL) Installation and Demonstration of ClamWin Portable

The purpose of this demonstration is to show participants that they can carry a portable anti-virus application on a USB memory stick. If the trainer feels this will not be a concern of the participants in their class, they can ignore this section and, instead, have participants conduct a full system scan. If participants discover viruses on their PCs, participants will need to return to the Class Notes to review recommended steps.

Video tutorial: "Clamwin Ver.portable and ClamWin Technical support." Distribute copies of ClamWin Portable (for Windows users) and ClamXav (for Mac Users), ideally with virus definitions already downloaded.

- Explain some of the peculiarities of ClamWin and ClamXav:
  - It is a FOSS anti-virus program.
  - It lacks certain features important to commercial anti-virus programs, such as Internet protection.
  - It has the advantage of being available in a portable version (for Windows), which allows you to run it from a USB stick on computers for which you don't have administrative rights.
  - It doesn't scan automatically, but rather only when executed by the user.
- Instruct participants to open the program and explore its options. By clicking on Tools and Preferences, they should instruct the program to quarantine infected files so that potentially important information isn't lost during the first scan.

Tips on Using ClamWin:

- ClamWin also comes in a MacOS version called ClamXav.
- One benefit of using an anti-virus from an external device is that it can help when the anti-virus that is installed on your PC becomes infected or compromised. Other "rescue" applications like AVG Rescue CD can also help.

Resources for ClamWin:

- Official homepage.
- ClamWin Portable.
- How to Use ClamWin.

Run and Update ClamWin

- Participants should launch ClamWin from an external device.
- In the main window of the application, participants should select the update tool to confirm that their virus definitions are up-to-date.

NOTE: *For this module, participants will not be asked to install Spybot or Comodo Firewall, although they may wish to do so after the module to increase their protection.*

(Source for ClamWin instructions and material: LevelUp.)

PART II: Your Operating System

This portion of the module is devoted to simple walk-throughs of two features in the Windows operating system that can help protect a PC:

- Automatic Updates.
- Windows Firewall.

A. Automatic Updates

We suggest that trainers use the instructions or video clip (provided below) to have participants locate their automatic updates settings, and to confirm that the feature is enabled.

Talking Points:

- Your operating system has to be updated to protect you from new exploits, just like your anti-virus application and other applications.
- Turning on automatic updates removes the danger that you will forget to update your operating system manually.
- Updating your operating system is supported by Microsoft even if your version of Windows is pirated. Having pirated software is not good, but it's also not a reason to avoid updating your operating system (failing to update may endanger your colleagues' computers).

Materials that May Be Useful:

- **Guide:** "How to Configure and Use Automatic Updates in Windows" (Microsoft).
- **Video:** "How to Enable or Disable Automatic Updates in Windows 7" (also appropriate for Windows 8) (YouTube: MiamiURSC).

B. Windows Firewall

We suggest that trainers use the instructions or video clip (provided below) to have participants locate their Windows Firewall settings, and to confirm that the feature is enabled.

Talking Points:

- A firewall protects your PC from network connections that you did not request.
- This specifically helps protect against becoming infected by worms – viruses that automatically try to replicate themselves onto any PC they can contact.
- A firewall does not protect your PC from connecting to a hacker's computer if your PC is already infected or you click on a link that connects you to that hacker's PC.
- Windows Firewall is considered a very basic firewall. If you are interested in installing a more robust firewall that has additional features (for instance, one that shows you which applications on your PC are sending data out to the Internet), you may be interested in investigating Comodo Firewall.

Materials that May Be Useful

- **Video:** "Turn On Windows Firewall Protection (On/Off)" (YouTube: TheMarketingMan).
- **Guide:** "Turn Windows Firewall On or Off" (Microsoft Support).

For additional ideas and related activities, visit the LevelUp website.

5. SYNTHESIS (10 MINUTES)

We recommend that trainers use this wrap-up session for informal questions, covering the material that has been covered in the module. The following questions may help participants think about using what they have learned:

- Does your office have a system for dealing with viruses? Do the PCs have anti-viruses installed?
- Did you learn anything that you think your colleagues should know? How could you tell them?
- If you use public PCs, such as at an Internet cafe, do you think they might have viruses?
- What words did we learn at the start of the module?
- What safer habits did you learn or are you now thinking about?
- Do you have a method for backing up "clean" copies (uninfected copies) of your files?

MAC OS X: MALWARE AND BASIC PROTECTION

The following material includes applications and exercises that may be useful to participants with Mac OS X and iOS devices. Trainers working in pairs may wish to divide their efforts during the Deepening exercises, with one trainer working with Windows/Android users and one trainer working with OS X/iOS users.

Software & Installation

- ClamXav anti-virus application.
  - Guide

Deepening

PART I: Antivirus Applications

Exercises #1 & #2: Installation and Walk-through of ClamXav

- Guide: Installation.
- Guide: Updating.
- Guide: Running your first scan.

Material That May Be Useful:

- Video: Overview.

Exercise #3: (Not applicable)

Exercise #4: Updating Applications

- Guide: Updating.

Material That May Be Useful:

- Video: "How to Turn On Mac Auto Software Updates."

PART II: Your Operating System

A. Automatic Updates
  - Guide: Updating

B. OS X Firewall

Talking Points:

- Apple sells their devices with the firewalls turned off by default, which is risky unless a user only uses it behind a router with a robust firewall and nowhere else.
- Go to System Preferences → Security & Privacy → Firewall to toggle your Firewall to "on" if it is off. You may have to click on the lock in the lower-left corner of the screen and enter your administrative password to do this.
- For trusted programs that need permission to make outgoing connections through the firewall (Instant Messaging, VoIP, etc.), users will have to either a) give each application permission manually as each is used after turning the firewall on, or b) click on "Firewall Options" in order to manually Allow or Block incoming connections for a given app. We strongly recommend that you block incoming connections for all apps except those that users actually utilize and trust – otherwise this can be a common entry point for malware.
- Also on the Firewall Options page is an option to "Enable Stealth Mode"; we recommend turning this on as it prevents your computer from responding to potentially hostile requests for information and data.

MATERIAL THAT MAY BE USEFUL:

- Guide: Mavericks Firewall Options.
- Guide: Prevent Unwanted Connections with a Firewall.
- Guide: Setting Firewall Options for Services and Apps.
- Video: "How to enable the built-in firewall in your Mac OS X."

NOTES

Viruses are a BIG problem:

- Tens of thousands of computer viruses have been recorded.
- Very short "survival time" for an unprotected PC.

Who makes viruses?

- Some hackers do it for money (e.g., Confickr).
- Some are developed as a service for intelligence (e.g., Ghostnet).
- Some … just because (e.g., ILoveYou).

Common myths:

- Only Windows gets viruses.
- Smartphones don't get viruses.
- An anti-virus will always clean an infected PC.

Three helpers:

- **Anti-virus:** Blocks infection before it can take hold.
- **Anti-spyware:** Blocks applications that send your information to someone else.
- **Malware scanner:** Locates and removes a virus or spyware application.
- **Firewall:** Blocks Internet traffic you did not request. Can prevent unintended installation of software.
- **Update everything:**
  - Anti-virus applications.
  - Operating system (e.g., Windows).
  - All other applications.
- **Make two backups:**
  - One nearby, one off-site.
  - On a regular basis (e.g., weekly).
- **Block unintended installations:**
  - In Windows, make sure UAC (User Account Control) is running.
- **On a mobile device:**
  - Locate free anti-virus for your platform at the official app store for your device.
  - Don't install applications, wallpapers or ringtones you don't need.
  - Always update.
- **When all else fails and you are infected:**
  - Copy essential files that were not included in your most recent back-up to some external media.
  - Write down any license or purchase information related to paid applications (if you have any).
  - Make sure you have your installation disk.
  - Re-install the operating system and applications.

For Further Learning:

- "Risk Assessment" (ArsTechnica.com). For journalists, this may be the most useful resource as it compiles news articles about recent viruses and other online threats.
- "Malware FAQ" (SANS Institute).
- "List of Computer Viruses" (Wikipedia).
- For those interested in getting a sense of malware at work in Moammar Gadhafi's Libya, read Matthieu Aikins' excellent Wired magazine article, "Jamming Tripoli: Inside Moammar Gadhafi's Secret Surveillance Network."
- "Threatsaurus" (sophos.com). An updated list of common PC security threats.

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

Avast! – A freeware anti-virus tool.

booting – The act of starting up a computer.

botnet – A vast array of computers, usually infected with malware, controlled by hackers for a variety of purposes including cyberattacks that can disable websites or the mass-mailing of spam.

CCleaner – A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself.

ClamAV – An open-source anti-virus program for desktop and laptop PCs.

ClamWin – A graphical user interface (GUI) for Windows that lets users access ClamAV anti-virus. A portable version called ClamWin Portable is able to run from a flash memory stick.

ClamXav – A graphical user interface (GUI) for Mac OS that lets users access ClamAV anti-virus.

Cobian Backup – A FOSS backup tool. The most recent version of Cobian is closed-source freeware, but prior versions are released as FOSS.

Comodo Firewall – A freeware firewall tool.

domain name – The address, in words, of a website or Internet service – for example, speaksafe.internews.org.

Firefox – A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer.

firewall – A tool that protects your computer from untrusted connections to or from local networks and the Internet.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

freeware – Free software. Includes software that is free of charge but subject to legal or technical restrictions that prevent users from accessing the source code used to create it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

keylogger – A type of spyware that records which keys you have typed on your computer's keyboard and sends this information to a third party. Keyloggers are frequently used to steal email and other passwords.

malware – A general term for all malicious software, including viruses, spyware, Trojans, and other such threats.

NoScript – A security add-on for the Firefox browser that protects you from malicious programs that might be present in unfamiliar webpages.

phishing – Creating fake websites or email that appear genuine in order to lure Internet users to interact with the content. Frequently used to capture passwords and financial data.

portable applications – Programs that run from a portable device, such as a flash memory stick or memory card, and do not require installation under the PC's operating system.

service provider – A company, either private or public, that provides mobile phone service or Internet service to customers.

spear phishing – The act of tailoring a fake website or email in order to make it appear authentic to a specific individual or a small group.

Spybot – A freeware anti-malware tool that scans for, removes and helps protect your computer from spyware.

spyware – An application that monitors a PC user's activities and data covertly and sends the information it logs to a remote computer.

3. KEEPING DATA SAFE

WHY THE TOPIC MATTERS

Journalists, especially those working in high-risk areas, handle sensitive information, including contact lists, research for articles, photographs and interviews. As journalists keep much of this information stored on mobile devices, computers, and in the Cloud (Dropbox, etc.), it is important for them to learn about these two helpful habits:

- **Backing up** – protecting against loss.
- **Encryption** – protecting against misuse/abuse.

Backups protect digital data from disappearing and encryption protects data from unauthorized access.

WHAT PARTICIPANTS WILL LEARN

Concepts: Encryption for PC and Cloud storage.

Skills: Use TrueCrypt to encrypt data.

NOTE TO TRAINERS: This module involves the distribution and demonstration of software that may not be legal to use in some countries. We recommend that trainers do basic research about local laws that govern Internet access in the country where they are training before using this module to train journalists. In some locations, for instance, the use of encryption (including VPNs, which are mentioned in our case study) is not legally permitted.

OBJECTIVES:

Learning about encryption and how to use it.

PRACTICAL USES:

Backing up sensitive data, protecting sensitive data, moving data safely.

PREREQUISITE SKILLS:

The module assumes that the participants are able to install applications, as well as locate and save files on their computer.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- Video: Art of the Problem.
- General Resource: "Journey Into Cryptography" (Khan Academy).
- Article: "The Spy Who Came in from the Code" (Columbia Journalism Review).

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Software & Installation

- TrueCrypt.
  - Guide.

Handouts

- Class Notes.
- Glossary.
- Article: "The Hackers of Damascus" (Business Week).
- Guide: "How to Install TrueCrypt and Create Standard Volumes" (Security in-a-box).
- Guide: "How to protect the sensitive files on your computer" (Security in-a-box).

NOTE: *Trainers requiring information related to Apple devices should consult the "Mac OS X" training notes found immediately afterthe Synthesis section of this module.*

RELATED MODULES

- Assessing Risks.
- Protecting Email.
- Mobile Phone Safety.

LESSON PLAN

1. ACTIVITY (15 MINUTES)

Spectrogram

This activity poses statements related to the session topic and asks participants if they "agree," "disagree" or are "in between." The purpose is to chart the "spectrum" of opinions in the room and also help participants explore a range of views.

Preparation:

- The trainer will need to create a list of statements (see below for suggestions) and these can be written on chart paper, with a vertical line drawn below each, with one side marked "Completely Disagree" and the other side marked "Completely Agree." If paper is not available, the questions can be read aloud.
- Collect materials:
  - Masking tape or colored chalk.
  - Chart paper and markers.
- Ensure that there is enough space for people to walk around freely (in some cases, a parking lot may be useful).

Statement Suggestions (need to be short, straightforward and easily understood):

- "The less information I share, the more secure I am."
- "My research for stories is not sensitive information."
- "If someone has agreed to be my source, his or her identity does not need to be protected."
- "It is likely that my computer or phone will be stolen or searched at some point."
- "My data is safe because my computer is password-protected."

Steps to Creating a Spectrogram Exercise:

1. Trainers ask participants to arrange themselves in a curved line (in the shape of the letter "C"). Colored chalk or masking tape on the floor are good for indoor spaces.
2. They then designate one end of the line to represent "Completely Agree" and the other "Completely Disagree."
3. Once participants understand this, trainers read out a statement from the list of statements and ask the participants to place themselves somewhere along the "spectrogram" of the room between "completely agree" and "completely disagree." Some participants may need to think about and try out several spots before making a final choice.
4. Trainers then randomly select participants and ask why they have placed themselves in a given position. Have they experienced something similar, or did a friend or colleague?
5. After one or two participants respond, others in the room may wish to change their location – the participants are allowed to change their position.
6. Once everyone has found their spot, trainers place large "+" and "-" signs immediately below the statement and write down the apparent "score" based on where people are standing.
7. Then trainers move to the next statement and repeat steps 3 through 6 for each statement.
8. At the end of the exercise, the trainer enlists the help of the participants to post the statements and the numbers on the wall.

(This activity, Spectrogram, was drawn from LevelUp as well as descriptions in the Aspiration Facilitation wiki and P2PU.)

REMINDER:
If this module is the first in a larger course, we recommend you spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

This exercise encourages trainers and participants to form opinions about topics, to recognize that one topic can be measured in different ways and that it is safe to change one's opinion.

2. DISCUSSION (15 MINUTES)

With the activity completed, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion.

- What kinds of confidential information do journalists normally keep on computers?
- On their smartphones?
- Among those items, what would be the most important? What might happen if someone confiscated it?
- Has anyone among the participants lost sensitive information? How did that happen?
- Does anyone know of any cases related to this topic?
- What do people in the room do now to protect the information on their PCs and phones?

  NOTE: *Encourage each person to contribute their "method." Ask them why they do what they do. The idea is to find out if they are taking these steps consciously.*

- Do participants back up their data?
- Do you use Dropbox or Cloud storage? Do you think there may be weaknesses?

Trainers are welcome to add to this list or improvise as they see fit.

3. INPUT / LECTURE (30 MINUTES)

This section includes a recommended case study, key messages and some materials to help get the point across.

Trainers are welcome to add or improvise as they see fit.

Case Study

"The Spy Who Came in from the Code"

Introduction: Even experienced journalists can lose their phones or computers to theft, natural disasters or – as we will see here – confiscation by authorities. When this happens, journalists don't just lose their important data, but also put their sources at risk.

Story: In the fall of 2011, Dlshad Othman, a young Kurdish Syrian activist and IT specialist living in Damascus, Syria was contacted by the British journalist and filmmaker Sean McAllister. McAllister was shooting a documentary for the UK's Channel 4 television about Syrian underground activists and enlisted Othman's help to make contacts.

McAllister is an award-winning filmmaker, with film credits from other conflict zones, including Yemen and Iraq, and had managed to get into the country undercover, even though the Syrian government had stopped issuing visas to international journalists.

Othman was helping reporters, human rights activists and the resistance with secure communications tools, and organizing VPN servers outside the country. Othman and his fellow activists were careful with their security and took measures such as encrypting their communications, using anonymizing tools, and encrypting their storage, etc.

As President Bashar al-Assad's regime had started to crack down on political activists, Othman felt McAllister would get the story to the outside world and agreed to be interviewed about his work. When he sat for an on-camera interview with McAllister, the filmmaker assured Othman that he would protect his identity and in the produced piece blur his face so he would not be identified. Othman also put McAllister in touch with other activists.

However, as Othman observed McAllister at work, he remembers feeling uneasy with McAllister's professional practices. Othman noticed McAllister was using his mobile and SMS without encryption and was leaving his unencrypted data, including raw footage of interviews with activists the Syrian regime was hunting, in his apartment. Othman also felt that McAllister did not appreciate how aggressive the Syrian regime's surveillance was, how much risk the activists were putting themselves into when they agreed to talk to him, and what the consequences of being "outed" would be for the activists.

A few days after McAllister's interview with Othman, Othman heard that Syrian security agents had raided McAllister's hotel, arrested him, and seized his laptop, mobile phone, camera, raw footage and research, including the names and contact details of his sources.

Othman turned off his mobile phone, took out the SIM card from his mobile, and left the country soon after. Other activists McAllister had contacted also fled. Several who did not leave, or were unable to, were arrested, including the activist Omar al-Baroudi, who had been interviewed on camera and whose number was on McAllister's phone. Baroudi disappeared the next day and has not been heard from since.

The Syrian regime also supports a pro-regime hacker organization called the Syrian Electronic Army (SEA). The hacktivists of SEA have attacked online platforms of the Washington Post, Al Jazeera, the Telegraph and the Independent, and flooded the Twitter accounts of BBC Weather and the Associated Press with pro-regime propaganda. Earlier this year, the SEA attacked the New York Times' website and rendered it offline for almost 20 hours.

Compiled From:

- "The Spy Who Came in from the Code" (Columbia Journalism Review).

Supporting Videos:

- "Syrian Uprising: 'The Internet has been Central to the Revolution' " (The Guardian).
- "Interview: Dlshad Othman" (Huffington Post video).
- "Sean McAllister: British Filmmaker Detained and Released from Syria" (CITIZENSYRIA's channel, YouTube).

Supporting Audio:

- "Reporters Unwittingly Exposing Sources" (http://www.onthemedia.org/story/204629-reporters-unwittingly-exposing-sources).

Interaction with the Participants

Using the Othman example, trainers can help participants reflect on their own practices that may be putting their sources at risk. Engage participants in a discussion on these questions:

- What could McAllister have done differently?
- Did Othman do the right thing in leaving the country? Was he too hasty?
- If the participants were to get arrested and their tools confiscated, would they or their sources be in danger?

Talking Points for the Trainer

With the case study concluded, the trainer now directs participants to their Class Notes.

1. Encryption transforms files from the format we normally see into a protected format

- You usually need a key (or password) to unlock the file again.
  - ✔ Without knowing the password or combination, we can't return the files to a format we recognize.

  Video demonstration: "What is a Caesar Cipher?" (Khan Academy).

2. Benefits:

- Protection: No access without permission (or key).
- Can help phones, PCs, Cloud.

3. But it ...

- Only works on the files or devices you choose to encrypt.
  - ✔ If you have a photo on your hard drive and a copy of that photo on Facebook, encrypting the one on your hard drive will not affect the one on Facebook.
- Does not always hide what is on your device.
  - ✔ If you open a Word document on your PC, edit it and then close it and encrypt it, the file is locked but someone who examines your PC may see signs that the document was recently opened. This might appear in your Recent Documents list in Word, for instance, or the file may appear in search results.

TRAINER'S NOTE:
Text with a ✔ does not appear in the student version of the Class Notes.

4. Most devices now come with encryption tools that allow you to encrypt your entire drive ("full-disk encryption") and/or smaller "containers" or drives, including USB drives:

- Windows = BitLocker.
- MacOS = FileVault.
- Android and iPhone (built into settings).
  - ✔ Note that it very important for anyone in the class who is considering using full-disk encryption to back up their data (and other essential files) before starting the task. Full-disk encryption can take several hours to complete and power outages during that time can ruin the data on the hard drive. Students interested in tips on backing up data should visit the LevelUp website.

5. Risks of using encryption:

- Encryption can be detected.
- In some countries, laws forbid the use of encryption.
- Not all encryption is strong.
- Just because a file is encrypted doesn't mean it will not show up in Recent Documents or Search results.
  - ✔ **One example:** "Steganography" – a way of hiding information in a file (for instance, saving a message inside what appears to be an ordinary photograph) – is susceptible to pattern recognition.
- Even "strong" encryption is only as strong as the password used to lock it.
  - ✔ "Password" and "passw0rd" remain among the most commonly used passwords in the world, according to the security software firm SplashData. But remember: Using a password does not always mean you are using encryption. Windows lets users protect their account on a PC with a password, for instance. This convenience, which lets users customize their experience (different wallpapers or applications) on the same computer, does not encrypt the data on the drive unless the user has specifically turned on BitLocker.

6. Encryption + "3-2-1" = good backups:

The 3-2-1 rule means that the best way to back up your data is to:

- Have three copies (original files + two other copies).
- Keep them at two locations.
- One of those locations needs to be off-site (away from the office).
  - ✔ The purpose of this system it to make sure that you have one copy handy in emergencies, but a second copy somewhere else in case of confiscation or a natural disaster at one location.
  - ✔ Encrypting those backups keeps the information safe on the backup, as well.

7. TrueCrypt (today's focus):

- Open source.
- Runs on PC, Mac OS, Linus.
- "Portable" (runs on USB flash drives)
  - ✔ TrueCrypt is widely used by human rights reporters and several security experts (like Bruce Schneier) and there is a project underway to confirm that the application has no hidden vulnerabilities. This is in contrast to "closed source" applications.

4. DEEPENING (90 MINUTES)

This section focuses on the use of TrueCrypt. We are also including an optional exercise related to passwords, in case the trainer has extra time. Trainers may wish to distribute the handouts related to TrueCrypt at this time.

Other resources that may help:

- Guide: "Installing and Using TrueCrypt" (Security in-a-box).
- Article: "TrueCrypt FAQs" and "Help" (www.truecrypt.org).
- Video: "TrueCrypt Full Disk Encryption on Windows 7" (CryptNode).

SOFTWARE & INSTALLATION:
- TrueCrypt
  - Guide

Exercise #1: Creating an Encrypted Volume

This exercise demonstrates TrueCrypt's most basic function: making an encrypted folder where files can be stored safely.

NOTE: *TrueCrypt calls folders "volumes." Some trainers prefer to use the term "secret device" to help participants understand. There will be an exercise immediately after the second exercise to help participants remember the term.*

- With TrueCrypt installed on a demonstration laptop, the trainer will need to create a standard volume. The best instructions for this are located in the handout "How to Install TrueCrypt and Create Standard Volumes" from the Security in-a-box website, though the following videos may help reinforce the steps:
  - "Using TrueCrypt to Create an Encrypted Volume".
  - "How to Encrypt a USB Drive Using TrueCrypt".
- Because TrueCrypt can be complicated, we strongly recommend that trainers repeat the demonstration before directing the class to create their own standard volumes. When it is time for participants to try, we recommend that they:
  - Keep the size of the volume small (1-2MB).
  - Remember where they create their volume (so they can find it).
  - Don't forget the password they used in the creation step.

NOTE: *The trainer needs to spend time with each participant to confirm that they have created their volume.*

Exercise #2: Opening an Encrypted Volume

This exercise shows participants how to use the volume they just created:

- With TrueCrypt open, the trainer should "mount" (open) his or her encrypted volume.
- Key point to make – the volume can be accessed in two ways:
  - By clicking on the name of the volume in TrueCrypt's interface, or
  - Through My Computer (Windows) or Computer (MacOS), both of which "see" the volume as a hard drive.
- The trainer now "dismounts" the volume.
- We recommend that trainers repeat this demonstration at least once before inviting participants to try.
- At this point, the trainer may wish to walk around the class to provide help and to confirm that participants are able to open (mount) and close (dismount) their volumes.

- Key points to make while participants are carrying out the exercise:
  - When the volume is mounted (open) it is not encrypted.
  - When it is dismounted (closed) it is locked/encrypted.
  - This is like locking a box: When you open the box with a key, it stays open until you lock it again.
- When all the participants have completed the task, the trainer can invite questions. Some that are frequently asked include:
  - **Can I make a copy of my volume?**

    Yes. It is just like a file on your computer – you can copy-and-paste and make perfect copies. This might be one way to use TrueCrypt when backing up data – keeping a volume on your PC at work and another on, for example, an external drive.
  - **Is there a limit to the size of a volume?**

    Not that we know of. It can be hundreds of gigabytes or it can be your entire PC. We point to instructions for this in the Class Notes.
  - **What is a "hidden volume"?**

    That is an advanced feature. It means that you can lock a volume with two passwords instead of one. Together the passwords can open 100% of the volume, but separately, they can only open part of the volume. So if someone opens a volume with Password 1, they will only see files that were associated with Password 1. You can learn more about this in the handouts, however we do not recommend training on this feature. It is easy to accidentally destroy data and should be unnecessary in all but the most extreme cases.
  - **What is a "key file"?**

    When you create a volume, TrueCrypt will ask if you want to associate it with a key file, in addition to your password. Using a key file is similar to using two-step verification in Gmail or Facebook (see our module on Protecting Email for more details). It means that you cannot open your volume without providing both a password and a file (any file, such as a .txt or photo) at the same time. This can be extra protection, but it also has a danger: If you lose your key file – maybe you delete it by accident – you will no longer be able to open the volume that was associated with it.
  - **What is a "Traveler Disk"?**

    This is the funny term that TrueCrypt gives to the portable version of TrueCrypt. You can install TrueCrypt onto a USB memory stick, for example, and run the application from that stick. The option for this is listed in Tools, but we ask that you investigate that after class.

Exercise #3: Making Volumes of Different Sizes

Before beginning, trainers should review with participants the unusual labels the TrueCrypt interface uses for otherwise familiar concepts or navigation buttons:

- Mount means open.
- Dismount means close.
- A volume is a secret folder or secret drive.

This exercise is designed to help participants feel more confident using TrueCrypt. It will not only give them more experience with the process of creating a TrueCrypt volume, but also help them become familiar with choosing volume sizes based on the size of material being stored:

- The trainer asks participants to choose on their PC a fun photograph, song or video clip that they would like to share.

- When participants are ready, they are asked to pick a "secret partner" – someone close by to whom they will send their file.
- Secret partners need to agree to a password that they both will use for this exercise.
- With the passwords chosen, participants can now create a volume of an appropriate size for the file they will share.

  NOTE: *Each participant is creating a small volume that they will exchange with their partner.The trainer may wish to warn participants that whatever they share cannot be bigger than the volume they create. Otherwise, they will get an error message.*
- When everyone has created a volume, they should mount (open) their volume and place their file inside.
- They should dismount (close) their volume.
- Now it's time for sharing: Secret partners should exchange their volumes.

  NOTE: *The trainer may wish to assign a variety of methods. For instance, by sending the volumes as attachments in email or exchanging USB memory sticks.*
- In the final step, partners will mount (open) the volumes that were sent to them, using the passwords that they agreed to at the start of the exercise.
- Repeat at least three times, or until all participants are comfortable with the creation process and the concept of sizing a volume.
- Some points to make while participants are carrying out the exercise:
  - This shows us a second use for TrueCrypt: It can protect files on our PC and can help us convey files to other people.
  - If you share a password for a file, should you send that password in an email with the file? (No.) How can you convey a password more securely? (There's no perfect answer. Agreeing to a password in person is best, but if that is not possible then journalists need to use any channel other than the one they use to share a volume.)
  - You can upload TrueCrypt volumes to Dropbox or other file-sharing services, too.

OPTIONAL Exercise

If time allows, trainers may wish to review with participants some recommendations for strong passwords. Why? If a password is weak (short, or easy to guess), encryption is not going to help. The importance of lengthy and strong passwords cannot be stressed enough!

For this exercise, we suggest that trainers use the Security in-a-box chapter "How to Create and Maintain Secure Passwords" or this summary from SpeakSafe as reference material.

For additional ideas and related activities, visit the LevelUp website.

5. SYNTHESIS (15 MINUTES)

We recommend that trainers use this wrap-up session for informal questions and discussion, reviewing the material that has been covered in the module. Because this module focused on TrueCrypt, however, trainers may wish to mention the following before the discussion begins:

- If you have an Android phone or an iPhone, you can enable encryption on it as well. To do this in Android, go to Settings →Security →Encrypt Phone.
- iPhone users can find instructions and a list of devices that support encryption at the Apple support site.

Some questions that may help participants think about using what they have learned:

- How do you think you might use encryption in your work?
- Do you think encryption is part of our commitment to protecting our sources? Why?
- Is encryption a guarantee that someone will not be able access your files? What could happen?

  A password could be guessed. Or you may be forced to give up a password.

Additional questions that may help participants review what was covered in the module:

- If your original copy of a file is secure and encrypted, but your backup is not, is your data secure?

  No.
- Do you think encryption protects against viruses?

  No.
- If your original copy on your PC is encrypted, but the version you have in Dropbox is not, is your data secure?

  No.
- When we store a photograph on a PC in an encrypted volume, are online copies of that photograph that are already uploaded automatically encrypted as well?

  No.

MAC OS X: KEEPING DATA SAFE

The following material includes applications and exercises that may be useful to participants with Mac OS X and iOS devices. Trainers working in pairs may wish to divide their efforts during Deepening exercises, with one trainer working with Windows/Android users and one trainer working with OS X/iOS users.

Input

Talking Points for The Trainer

Some journalists may want to use Mac OS X's built-in encryption tool called FileVault 2 for full-disk encryption and TrueCrypt to encrypt certain files or sections of their drive. This can be a powerful tactic if you are concerned about hiding specific files or documents in an environment where you may be forced to provide your login information for your computer to someone you do not trust.

Material That May Be Useful:

- Guide: "About FileVault 2" (Apple Support).

NOTES

- Encryption locks up our articles, photographs and other files so that people without permission can't access them (permission = password).
- Works on phones, PCs, the Cloud.
- But ...
  - Only works on the files or devices you choose to encrypt.
  - Does not always hide what is on your device.
- Most devices now come with encryption tools:
  - Windows = BitLocker.
  - MacOS = FileVault.
  - Android and iPhone (built into settings).
- Risks of using encryption:
  - Encryption can be detected.
  - In some countries, it is illegal to use encryption.
  - Not all encryption is strong.
  - Just because a file is encrypted doesn't mean it will not show up in Recent Documents or Search results.
  - Even "strong" encryption is only as strong as the password used to lock it.
- Encryption + "3-2-1" = good backups.
- TrueCrypt:
  - Open source.
  - Runs on PC, Mac OS, Linux.
  - "Portable" (runs on USB flash drives).

For Further Learning:

- **Video:** Art of the Problem.
- **General Resources:** "Journey Into Cryptography" (Khan Academy).
- **E-learning Application:** Cryptool.

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

BitLocker – An application in the Enterprise and Ultimate versions of Windows Vista, Windows 7 and Windows 8 that protects both PC hard drives and external drives.

booting – The act of starting up a computer.

encryption – A way of using mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

Firefox – A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

portable applications – Programs that run from a portable device, such as a flash memory stick or memory card, and do not require installation under the PC's operating system.

steganography – Any method of disguising sensitive information so that it appears to be something else, in order to avoid drawing unwanted attention to it.

TrueCrypt – A FOSS file encryption tool that allows you to store sensitive information securely.

4. RESEARCHING SECURELY

WHY THE TOPIC MATTERS

As recent reports have confirmed, there is not much we can do on the Internet that is completely private. Reporters who research their stories online, for example, may be leaving a record of their activities on their PCs and on the Web, which can potentially compromise their safety – and that of their sources – when investigating stories that others are trying to suppress. At the same time, journalists may find it frustrating that some of the resources crucial to their research are not available where they live.

WHAT PARTICIPANTS WILL LEARN

Concepts: Secure vs. insecure Internet connections, fingerprints.

Skills: Using a VPN, using Tor.

OBJECTIVES:

Learning how the Internet works and how to reduce our Internet footprint.

PRACTICAL USES:

Researching sensitive topics, avoiding content filters, publishing anonymously.

PREREQUISITE SKILLS:

The module assumes that the participants are able to:

- Identify operating systems.
- Install applications.
- Save and locate files on their computer.

NOTE TO TRAINERS: This module involves the distribution and demonstration of software that may not be legal to use in some countries. We recommend that trainers do basic research about local laws that govern Internet access in the country where they are training before using this module to train journalists. In some locations, for instance, the use of VPNs (discussed in this module) is not legally permitted.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- "Safer Surfing" (Internews: SpeakSafe).
- Guide: "How to Remain Anonymous and Bypass Censorship on the Internet" (Security in-a-box).
- Video: "The Internet Explained" (YouTube).
- Interactive graphic: "Tor and HTTPS" (EFF.org).
- Article: "How (and Why) to Surf the Web in Secret" (PC World).

This module will help journalists install and use software that can provide more privacy for their online research, as well as reach resources that would otherwise be unavailable.

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Software & Installation

- CCleaner.
  - Guide.
- BleachBit.
  - Guide.
- Psiphon 3.
  - Guide.
- Tor Browser Bundle.
- Firefox Web browser.

Handouts

- Class Notes.
- Glossary.
- "How to Remain Anonymous and Bypass Censorship on the Internet" (Security in-a-box).
- "Tor – Digital Anonymity and Circumvention" (Security in-a-box).

NOTE: *Trainers requiring information related to Apple devices should consult the "Mac OS X" training notes found immediately afterthe Synthesis section of this module.*

RELATED MODULES

- Protecting Email.
- Mobile Phone Safety.

LESSON PLAN

1. ACTIVITY (20 MINUTES)

We Are the Internet

The purpose of this activity it to illustrate how the Internet works and to show participants how much we expose about ourselves every time we go online.

Preparation

Prior to the class, the trainer needs to write the following words in big letters on index cards:

- Wi-Fi
- ISP
- Router
- ISP
- Gateway
- ISP
- Router
- ISP
- Website

Getting Started

- The trainer asks for three volunteers to represent "Journalists" and gets them to stand together on one side of the room. The volunteers could carry pens and notepads to represent that they are journalists.
- The trainer then asks for two volunteers to represent popular "Websites" (e.g., Google, Yahoo! or Wikipedia) and directs them to stand together at the opposite side of the room. Because they are popular, they could wear cool sunglasses (up to the trainer).
- The trainer then makes an announcement: "Our journalists need to conduct research. Our popular websites have the information. So let's help them get connected."
- The remaining participants will then be asked to form a line between the Journalists and the Websites.
- The trainer hands an index card with the word "Wi-Fi" to the person standing closest to the Journalists and announces that this person is now an "Access Point." (Of course, the trainer can use whatever he or she likes to identify this person, such as asking the person to wear antennae. The more humorous the activity, the better it will be!)
- Remaining participants play other parts of the Internet, with each person wearing or holding a card that identifies them:
    - Local ISP (ISP = Internet service provider)
    - National ISP
    - Router
    - International gateway
    - Router
    - National ISP
    - Local ISP
    - … and so on. (The trainer can decide how many cards to issue. The purpose is not for the participants to learn the terms but for them to understand that no one connects directly to websites; there are many links in the chain.)

Conducting the Activity:

The trainer explains that we have now formed the Internet in the room and guides the participants through the following steps:

- Asks the participants to take a couple index cards each and write a question on each card that they would like to ask the Websites – maybe questions for an article they are working on. So that everyone knows where each index card goes, they should start their questions with "Dear (Google, Yahoo!, Wikipedia, etc.)."
- Asks participants to pass their cards to the Wi-Fi person, the first link in the chain that is the Internet. At some point, the Wi-Fi person will have six index cards in his or her hand.
- Asks the participant holding the Wi-Fi card: "Okay Wi-Fi, how do you know where to send each card?" (Hopefully the participant sees "Dear (website name)" at the top of each card.)
- Says, when Wi-Fi responds: "Great! How will you know where each card came from?" Here, the trainer can suggest that Wi-Fi write the location of each person who handed him or her a card: "right," "left" and "center."
- Encourages Wi-Fi to hand the cards, one at a time, to an ISP person and say, "Please give this to Google" (or Wikipedia, etc.) and so on, down the line.
- At this point, the trainer stops the traffic and asks ISP: "Great! How will you know where each card came from?" The trainer can suggest that ISP write the word "Wi-Fi" on each card.

  NOTE: *To save time, other participants in this activity do not have to write where the cards came from – the goal is just to illustrate that a network does not function unless people (and machines) have addresses.*
- Then the ISP is asked to hand each card, one at a time, to the next person who calls out, "I got a card for (website)!" and hands that card to the next person. (This is usually a humorous moment as more than one person may be calling out at the same time.)
- When people representing various websites eventually receive their index cards, they should send a reply that begins: "Dear (person on the left, right or center), here is your answer ..." and then send them back.
- When Wi-Fi successfully delivers each index card with its answer to each participant, they should congratulate themselves with applause!

With participants still standing, the trainer can ask the participants:

- What did the Websites know about the index cards they received? What information was exposed?
- What did Wi-Fi know? What did the ISPs and other links in the chain know?
- Could the Websites have received the index cards that were intended for them if the cards didn't say "Dear (website)"?
- Could the Journalists have received a reply from the Websites if the Websites didn't know where they were?
- Did everyone in the chain see where the index cards were going and where they came from?

  The trainer explains, before moving onto the Discussion session, that this is a very simplified version of what happens on the Internet and the kinds of information we include every time we click on a link. Instead of index cards, we send out "packets" that contain lots of data/code that can identify us.

REMINDER:
If this module is the first in a larger course, we recommend you spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

ADDITIONAL MATERIALS:
- Markers.
- Pens.
- Notepads.
- Index cards.
- Envelopes.
- Tape (any kind).
- (Optional) Cheap plastic sunglasses.

Options:

- The number of people representing Journalists and Websites is not important, but there needs to be two or three of each to illustrate the need for identification.
- For a large class, more people can be assigned to play the roles of Journalists and Access Points. This will reinforce the concept that ISPs also need to distinguish Access Points, in the same way that Access Points need to distinguish Journalists.

2. DISCUSSION (15 MINUTES)

With the activity completed, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion.

Trainers are welcome to add to this list or improvise as they see fit.

- Did the activity you just participated in show you anything you didn't know about the Internet?
- In your work, what kinds/categories of information should be kept private when you use the Internet to visit websites?
- Would we ever care about someone knowing what search terms we type into a search engine, what websites we visit, what we post in a blog or on a social network?
- Do you know of examples here, in this country, where it was clear that the Internet was not private? (Trainers need to engage participants in a discussion about surveillance.)
- Have you heard of surveillance in other countries? Have you followed these stories? What lessons have you drawn from them?
- Have you ever changed your online habits because of what you heard about online monitoring and surveillance?
- Should we expect privacy when we surf the Web or should we assume that nothing is private, ever? (If participants think it is a mix, engage them in a discussion about what things they think should be private and what things are OK to be public.)

For additional ideas and related activities, visit the LevelUp website.

3. INPUT / LECTURE (30 MINUTES)

This section includes a recommended case study, key messages and some materials to help get the point across. Trainers are welcome to add or improvise as they see fit.

Case Study

Attacks on a Privacy Tool

Introduction: A software application called Tor (The Onion Router) has made it possible for journalists and activists to use the Web in relative anonymity. However, documents leaked by former National Security Agency (NSA) contractor Edward Snowden indicate that the NSA in the United States and its counterpart in the United Kingdom, the Government Communications Headquarters (GCHQ), have been attempting to defeat Tor's protections.

Story: The Guardian reported in October 2013 that the NSA and GCHQ have been working together to defeat the popular anonymity software, Tor.

Tor is a free application and network that helps users protect their identity and online habits. It bounces a user's Internet traffic around a network of computers, usually located in several countries, preventing others who are watching from learning what sites are being visited. It also prevents websites from seeing who is visiting.

NOTE: *The participants will learn to use Tor later in the lesson.*

The Guardian quoted a presentation leaked by former NSA contractor Snowden that said: "We will never be able to de-anonymize all Tor users all the time. With manual analysis, we can de-anonymize a very small fraction of Tor users." The Guardian story concluded that the NSA had not been able to "de-anonymizing a user in response" to a specific request. Another presentation called Tor "the king of high-secure, low-latency internet anonymity."

Although the NSA and the GCHQ had not succeeded in cracking Tor, the documents the Guardian story quoted show that the agencies have had limited success when they have been able to identify users and launch an attack through vulnerable software on users' computers. One involved the NSA targeting the Firefox browser used with the Tor Browser Bundle, giving the agency full control over users' computers, including files, keystrokes, browsing history and online activities.

Tor is used by reporters and activists around the world, including in Syria, Iran and China, to keep their communications private. The governments of China and Iran have attempted to limit Tor's use in their countries, with China attempting to block Tor, and Iran trying to create a "national internet" to prevent circumvention of governmental controls. The law enforcement agencies in the West, however, say that TOR is used by those involved in terrorism, trade of child pornography, and online human and drug trafficking, and needs to be watched.

While the NSA and GCHQ reportedly have not breached the Tor network yet, they have tried out models such as mass surveillance of the Tor network, tapping core Internet cables while simultaneously controlling a large number of Tor's "exit nodes" and "shaping" future Tor development to increase crackability, or actively disrupting Tor to drive users off the network.

The NSA infected browsers with a rogue code using a "honey pot" site, designed only to attack those who were using the Tor network. The vulnerability that the NSA was exploiting, according to the Guardian story, has since been addressed in Firefox 17.

"The good news is that they went for a browser exploit, meaning there's no indication they can break the Tor protocol or do traffic analysis on the Tor network," the Guardian quoted Tor President Roger Dingledine as saying. "Infecting the laptop, phone, or desktop is still the easiest way to learn about the human behind the keyboard."

Compiled from:

- Guardian article: "NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users."

Supporting Videos:

- Interview: BBC Newsnight interview of Glenn Greenwald.
- Explanatory item: "Snowden Leak: NSA Targeted Tor Users' Anonymity" (Newsy Tech).
- Edward Snowden Interviews with Glenn Greenwald: June 9, 2013, interview and July 9, 2013, interview (The Guardian).

Interaction with the Participants

The trainer may wish to engage participants with questions related to the case study:

- Do you agree or disagree that a government has the right to keep track of their citizens' online activities? Please explain the reasons.
- Should governments be monitoring their citizens? Are there special circumstances under which governments should be allowed to do so?

  Trainers may wish to point out that surveillance can be used for negative purposes such as keeping tabs on political opponents, human rights activists and journalists; however it may also be used to track terrorists, human traffickers, child pornographers, and people who sell drugs and weapons.
- Whether you think there should or should not be monitoring, would you change your surfing habits and use a tool like Tor if it was available?
- Should Snowden have released the information? Why? Why not?

Talking Points for the Trainer

With the case study concluded, the trainer now directs participants to their Class Notes.

- **These can be identified:**
  - IP addresses.
  - MAC addresses.
  - More ...
    - ✔ Like Caller ID on mobile phones, websites can see who is "calling" when a connection is made. One type of information they see is an IP address (Internet Protocol address) and this is what we illustrated in our Activity. Another kind of information is called a MAC address, which relates to the hardware on your PC and which we won't cover here … and there are other things, as we will see.
    - ✔ **Live Demonstration:**To illustrate an IP address, the trainer visits whatismyipaddress.com or whatismyip.com. The resulting Web pages will provide both the IP address and geographic location of the trainer's PC.
    - ✔ **Video Demonstration:** "The Internet Explained." For this lesson, only a few seconds of this clip needs to be shown. End at: 00:47.
- **Websites have identifiers, too.**
  - ✔ Every website has at least one IP address for the physical computer on which it resides. Some very popular websites are hosted on more than one computer (or server) and so they might have many IP addresses associated with their name. In any case, this is one way of monitoring which devices are contacting which websites. It is also one way authorities filter websites – they simply block an IP address.
- **Browsers have "fingerprints":**
  - Version
  - Plug-ins
  - History
  - More ....

TRAINER'S NOTE:
Text with a ✔ does not appear in the student version of the Class Notes.

- ✔ **Live Demonstration:** Panopticlick. This Web tool run by the Electronic Frontier Foundation (EFF.org) displays detailed information about the user's browser that websites and authorities can use to identify a specific computer or mobile device.
- ✔ **Alternative:** JonDonym IP Check. If Panopticlick is not available, this similar (though less detailed) site from the developers of JonDo (an anonymity application) may work.

- **Applications and settings can help. Start with the Web browser:**
  - Don't store passwords in the browser.
  - Don't save history or cookies.
  - Run CCleaner or BleachBit when done with session.
  - Install the add-ons called HTTPS Everywhere and NoScript (Firefox).
    - ✔ HTTPS Everywhere creates a secure tunnel between a PC and popular websites that support HTTPS connections. Trainers can learn more about HTTPS Everywhere from the EFF.org website and read about HTTPS in this Wikipedia article.
    - ✔ NoScript prevents malicious websites from running applications on your PC without your knowledge. NoScript behaves a bit like a firewall: Initially, it will prevent all "scripts" (short for Javascript, a popular coding language) from running in the user's browser and the page will display these blocked elements as broken. The user can then choose which elements he or she would like to give permission to run.

- **VPN = "Virtual Private Network." It provides a secure connection between a PC or mobile device and a server (another computer) on the Internet.**
  - ✔ This is a little different from Tor, which we just discussed. A VPN requires you to install software on your PC or mobile device. That software connects to another computer on the Internet called a VPN server. When that connection is made, the things that you upload to or download from the Internet are protected between your device and the VPN server (though they might not be protected between the VPN server and the website you are visiting).
  - ✔ **Video demonstration:** "VPN Tutorial" (Google Privacy). This video clip also explains the difference between a VPN connection and a standard HTTPS (SSL) connection.
  - ✔ **Live Demonstration:** The trainer launches Psiphon 3 and revisits whatismyipaddress.com or whatismyip.com, showing that his or her IP address has changed.

- **There are risks associate with VPNs:**
  - It is not private unless you visit a site with HTTPS.
  - It is not anonymous: Your VPN service knows what you do.
    - ✔ Going back to the Google Privacy video, one can see that a VPN's connection is only protected between a PC or phone and a VPN server. The connection is not protected between the VPN server and the website being visited, unless that website supports an HTTPS connection.

- **Tor adds some steps to make the connection more anonymous:**
  - Voluntary, global network.
  - Connection through three volunteers (or "proxies").
    - ✔ Tor is slower than a VPN but more secure because it uses three proxies instead of one – it's a bit like connecting to three VPNs in a row. Tor-type onion routing got its name because it provides three layers of encryption, which it "peels off" – like the layers of an onion.
    - ✔ Each VPN is connected to the next one in the chain with a protected connection that only they share. They do not share other information with one another, such as where the connection might be originating from or what website you want to visit (until the last step in the chain).

- ✔ **Live Demonstration**: The trainer opens two browsers – one (regular) Firefox and one through the Tor Browser Bundle. The trainer visits the following site in each and runs a test: JonDonym IP Check. The trainer compares the difference in what information can be captured by sites and authorities in each case (the Tor connection will be shown to be much less revealing about the user).
- ✔ **Interactive graphic:** This chart at EFF.org illustrates what information you expose when you use an HTTPS connection vs. a Tor connection.

- **Tor has risks:**
  - As always, malware can defeat our precautions and give away our location.
    - ✔ The example in our Case Study shows that no security technology can provide perfect protection if other parts of the PC are insecure.
  - Tor only protects your activity if you visit a site with HTTPS.
    - ✔ As with a VPN, your connection is encrypted only as long as you are within the Tor network itself. Once your connection leaves the last "node" and goes to the website, the content of what you post or read will be visible to the person who runs that last "node" unless the site is protected by HTTPS.

- **Because VPNs and Tor "mask" your IP and that of the website you are visiting, some journalists find they can access resources that were previously unavailable.**

4. DEEPENING (90 MINUTES)

This section introduces the following applications:

- CCleaner and BleachBit.
- Psiphon 3 and Tor Browser Bundle.

If participants have not preinstalled the software, the trainer may wish to take a break at this time and ask those who have not come prepared to use the time to catch-up.

SOFTWARE & INSTALLATION:

- CCleaner
  - Guide
- BleachBit
  - Guide
- Psiphon 3
  - Guide
- Tor Browser Bundle
- Firefox Web browser

PART I: Cleaning Up Traces and Browser Settings

Exercise # 1: Erasing Your Browser History with BleachBit (10 minutes)

The goal of this exercise is to ensure that participants know how to erase temporary files, including browser history. The trainer needs to confirm that participants have installed either BleachBit or CCleaner on their PCs before walking them through these exercises:

- Participants open Firefox (or the default browser) and navigate to their browser history. In Firefox, this is located under History → Show All History.
- After confirming that details of their recent browsing are visible, participants close their browser and open BleachBit (or CCleaner).
- To avoid unintentional loss of information, participants should deselect all and then check the boxes for Firefox for "URL history," "cache," "session restore" and "Download history." Then they click "Clean" to start erasing information associated with those items.
- Participants now need to open Firefox and navigate to their browser history again. They should see that the references to their browsing history and download history have been deleted.

Exercise #2 (Optional): Erasing Your Browser History with CCleaner (10 minutes)

This exercise is similar to the first one. However, the trainer needs to take additional time to point out the other features that CCleaner has, particularly Drive Wiper (located under the Tools tab). Drive Wiper lets the user destroy data on a drive so that someone else cannot recover it. How does this compare with BleachBit?

What is the difference between BleachBit and CCleaner? BleachBit is open source, which means that its code is available for someone to inspect. CCleaner is not. On the other hand, CCleaner has more tools that may be useful to participants. Both may be valuable.

Exercise #3: Making Your Browser Settings More Private (10 minutes)

The purpose of this demonstration is to show participants where privacy settings are located in Firefox. We recommend limiting this to a demonstration instead of an exercise in order to preserve time for the next exercises, which are crucial. Participants can visit their privacy settings after class:

- In Firefox, go to Tools → Options and select the Privacy tab.
- In the History section's pull-down menu, select "Never Remember History" or instead choose "Use Custom Settings for History" and check the box marked "Always Use Private Mode."
- Trainers also draw participant's attention to the check box for "Clear History When Firefox Closes."

PART II: Creating a Secure Connection

Exercise #1: Confirming a Secure Connection in a VPN

In this exercise, participants will use Psiphon 3 to create a secure connection:

- In a browser, the trainer visits whatismyipaddress.com, and shows this to the class.
- Close the browser.
- The trainer now launches Psiphon 3 and, making certain that the application is set to connect via VPN, waits until a connection is obtained and a new browser window has opened.
- The trainer revisits whatismyipaddress.com and shows the new IP address to the class.
- Participants should repeat this exercise until they demonstrate they understand the steps clearly. While participants conduct this exercise, the trainer may wish to remind them that:
  - Traffic between their PC and that server is encrypted. HOWEVER, the traffic between that server and a website will not be if the site does not support an HTTPS connection.
  - Web pages they visit will load more slowly when using a VPN. This is normal and it is because they are not visiting the website directly.
  - If a participant has not established a VPN connection, they will not be using the VPN.

Exercise #2: Confirming a Secure Connection with Tor

In this exercise, participants will use Tor to create a secure connection AND change their "exit node":

- In a browser, the trainer visits whatismyipaddress.com or whatismyip.com and shows the results to the the class.
- Close the browser (and any others that are open).
- The trainer opens the Tor Browser Bundle folder and launches Tor ("Start Tor Browser.exe").
- The control panel (called Vidalia) will appear and show progress as a connection is established. *This may take several seconds.*
- When the status icon – an onion – turns green, a portable version of Firefox will open and should display the following message:

  "Congratulations. Your browser is configured to use TOR."

  If the application fails to make a secure connection, this homepage will come up with an alert message!
- In the Firefox browser window that has just opened, the trainer revisitswhatismyipaddress.com or whatismyip.com and sees that the IP address has changed. It is also possible that the geographic location will be completely blank.
- The trainer explains that it is always possible that the "exit node" – the server where the user "exits" onto the public Internet – may be in the same country they are in (!). If that happens, users may want to change their exit node by selecting the "Use a New Identity" button in Tor's control panel (see image, right) and waiting a few seconds for Tor to re-establish a connection.
- The trainer does this and then refreshes the page in the browser (whatismyipaddress.com or whatismyip.com). The IP address will have changed.
- Close the browser. At this point, both the browser and (a few seconds later) the control panel will close.

While participants replicate this exercise themselves, the trainer may wish to remind them that:

- If someone wants to use Tor, they need to launch the Tor Browser Bundle and use the special version of Firefox that comes with it. If a user has more than one browser (e.g., Chrome or IE) – or even has a regular version of Firefox on their PC – these browsers will not automatically use the Tor network. This can be confirmed by checking the IP address of a PC with the Tor browser and a non-Tor browser open simultaneously.
- Again, unless a user is browsing with Tor running, they will not be using the Tor network, so it is important to pay attention to which browser you are using.
- Because surveillance tactics and technology are always changing, it's very important that participants use the latest version of the Tor Browser Bundle. The browser will automatically check when first connecting and, if a newer version is available, the homepage will say so, but it will not download the update for the user. That has to be done manually.
- If participants are interested in learning how to use a VPN or Tor on an Android device, they have links to that information in their Class Notes.

For additional ideas and related activities, visit the LevelUp website.

NOTE: *Trainers should be sure to state the following during exercises related to Tor: Because surveillance tactics and technology are always changing, it's very important that participants use the latest version of the Tor Browser Bundle. The browser will automatically check when first connecting and, if a newer version is available, the homepage will say so, but it will not download the update for the user. That has to be done manually.*

5. SYNTHESIS / CONCLUSION (10 MINUTES)

We recommend that trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. Some important points that need to be reviewed:

- **What does a VPN protect?**
  A VPN protects the connection between a PC and server, but not the connection between a server and the websites we visit.
- **What are the differences between VPNs and Tor?**
  - A VPN is not anonymous – our Web traffic is still visible to the staff at the VPN. What we upload and download is also visible unless we are also connected to a website that supports HTTPS connections. Tor is more anonymous, however our traffic is still visible to the final proxy in the chain unless we are connected to a website that supports HTTPS connections.
  - A VPN goes through one proxy. Tor goes through three.
  - Tor is slower than a VPN because of these extra steps.
- **Do you think you will use one or the other in your work?**

NOTE: *Trainers should repeat the following to make sure participants understand: Because surveillance tactics and technology are always changing, it's very important that participants use the latest version of the Tor Browser Bundle. The browser will automatically check when first connecting and, if a newer version is available, the homepage will say so, but it will not download the update for the user. That has to be done manually.*

MAC OS X: RESEARCHING SECURELY

The following material includes applications and exercises that may be useful to participants with Mac OS X and iOS devices. Trainers working in pairs may wish to divide their efforts during Deepening exercises, with one trainer working with Windows/Android users and one trainer working with OS X/iOS users.

Software & Installation

- CCleaner
- Tor Browser Bundle
  - Guide
  - Video walkthrough
- Firefox Web browser
  - Guide

NOTE: *Neither BleachBit nor Psiphon 3 are currently available for Mac OS X. Mac OS X users who have access to a VPN service may wish to explore Tunnelblick, an application that lets users add and control OpenVPN connections.*

NOTES

- These can be identified:
  - IP addresses
  - MAC addresses
  - More ...
- Websites have identifiers, too.
- Our browsers have "fingerprints":
  - Version
  - Plug-ins
  - History
  - More ...
- Applications and Settings can help. Start with your Web browser:
  - Don't store passwords in the browser.
  - Don't save history or cookies.
  - Run CCleaner or BleachBit when done with session.
  - Install the add-ons called HTTPS Everywhere and NoScript (Firefox).
- A VPN (Virtual Private Network) provides a secure connection between a PC or mobile device and a server (another computer) on the Internet.
- Some VPN risks:
  - It is not private unless you visit a site with HTTPS.
  - It is not anonymous: Your VPN service knows what you do.
- Tor adds some steps to make the connection more anonymous:
  - Voluntary, global network.
  - Connection through three volunteers (or "proxies") – Tor adds anonymity by connecting through three "nodes."
- Some Tor risks:
  - As always, malware can defeat safety precautions and give away your location.
  - Your activity is not completely private unless you visit a site with an HTTPS connection.
- Because VPNs and Tor "mask" your IP and that of the website you are visiting, some journalists find they can access resources that were previously unavailable.

For Further Learning:

- "Journalist Security Guide" (CPJ).
- "Journalism Security Issues" (CPJ).
- Psiphon 3 and Tor on mobile devices:
  - Psiphon 3 for Android.
  - Tor for Android using Orbot, Orweb.
- "How to Bypass Internet Censorship" (howtobypass.org).

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

access point – Any point at which a device connects to the Internet, usually a wireless access point (Wi-Fi).

CCleaner – A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself.

circumvention – The act of bypassing Internet filters to access blocked websites and other Internet services.

cookie – A small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website.

domain name – The address, in words, of a website or Internet service; for example, *speaksafe.internews.org*.

encryption – A way of using mathematics to *encrypt*, or scramble, information so that it can only be *decrypted* and read by someone who has a particular piece of information, such as a password or an encryption key.

Firefox – A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

HTTPS – Hypertext Transfer Protocol Secure (or HTTP Secure). An encryption protocol widely used on the Internet to protect connections between websites and the people who use them. Also frequently referred to as SSL (Secure Sockets Layer).

Internet Protocol address (IP address) – A unique identifier assigned to your computer when it is connected to the Internet.

Internet service provider (ISP) – The company or organization that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.

portable applications – Programs that run from a portable device, such as a flash memory stick or memory card, and do not require installation under the PC's operating system.

proxy – An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy.

Secure Sockets Layer (SSL) – An encryption protocol that provides a secure connection between your computer and some of the websites and Internet services that you visit. When you are connected to a website through SSL, the address of the website will begin with HTTPS rather than HTTP.

security certificate – A way for secure websites and other Internet services to prove, using encryption, that they are who they claim to be. In order for your browser to accept a security certificate as valid, however, the service must pay for a digital signature from a trusted organization. Because this costs money that some service operators are unwilling or unable to spend, you will occasionally see a security certificate error even when visiting a valid service.

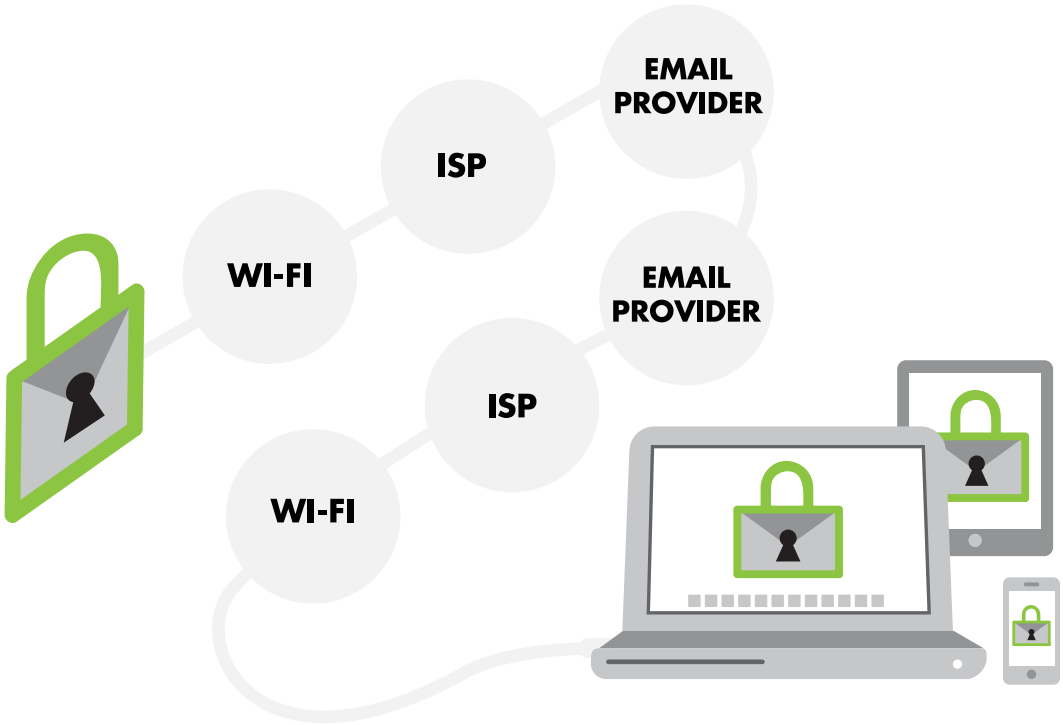
server – A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers.

service provider – A company, either private or public, that provides mobile phone service or Internet service to customers.

Tor – The Onion Router is an anonymity tool that, in some cases, allows the user to bypass Internet censorship. It hides the websites and Internet services you visit from someone monitoring your Internet connection, while also disguising your own location from those websites.

VPN – A virtual private network. VPNs use software on a PC or mobile device to create an encrypted connection with a server on the Internet. VPNs do not provide anonymity and users' online activity is visible to the VPN service provider.

5. PROTECTING EMAIL



WHY THE TOPIC MATTERS

Journalists depend on email for a variety of sensitive tasks, but may not realize that sending an email is like sending an old-fashioned postcard: As the postcard gets passed around through the postal system, it can be read by anyone who holds it.

Stories based on leaked documents from Edward Snowden illustrate how little privacy there is for most email and other online communication.

WHAT PARTICIPANTS WILL LEARN

Concepts: Lack of privacy in online communications, two-step verification, end-to-end encryption.

Skills: How to use Thunderbird and security add-ons, how to enable two-step verification for online accounts that support it.

IMPORTANT: It is essential that trainers who undertake the Advanced exercises in the Deepening section visually confirm that participants are using the recommended software correctly. It is common for participants to assume that their emails will be automatically encrypted once they have installed the applications. However, this is not the case. By default, none of the user's email is automatically encrypted unless the user changes their security preferences. Instead, users must manually choose to encrypt individual emails in order for them to be encrypted.

OBJECTIVES:
Learning how to improve privacy in email.

PRACTICAL USES:
Communicating more safely with sources and colleagues.

PREREQUISITE SKILLS:
The module assumes that the participants are able to install applications, add email credentials to an email application, and locate and save files on their computer.

NOTE TO TRAINERS: This module involves the distribution and demonstration of software that may not be permitted in some countries. It is strongly recommended that trainers research local laws that govern Internet access in the country in which they are training. In some locations, for instance, the use of encryption (including VPNs) is not permitted.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- "How to Keep Your Internet Communication Private" (Security in-a-box).
- "Safer Email" (SpeakSafe).
- Video: "Gmail Security Tips" (Google support).
- "Check Your Gmail Settings" (Google support).

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Handouts

- Class Notes.
- Glossary.
- Notes for Mac Users.
- "How to Keep Your Internet Communication Private" (Security in-a-box).

(Advanced only)

- Guide: "Thunderbird with Enigmail and GPG" (Security in-a-box).

NOTE: *Trainers requiring information related to Apple devices should consult the "Mac OS X" training notes found immediately afterthe Synthesis section of this module.*

RELATED MODULES

- Mobile Phone Safety.
- Malware and Basic Protection.
- Researching Securely.

LESSON PLAN:

ABOUT THE CONTENT: This module is divided into Basic and Advanced activities, lecture notes and exercises. We strongly advise against introducing any of the Advanced material (labeled "Advanced") until participants have completed a review of basic webmail tools (labeled "Basic").

1. ACTIVITY (20 MINUTES)–BASIC

(This exercise was drawn from the LevelUp project, and was developed by the Tactical Technology Collective.)

Preparation

This activity requires some materials:

- Markers.
- Blank postcards.
- Two copies of a small cipher (see image below).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	.	,	!	?

You can use this grid (above) to turn words into numbers. Each letter and each punctuation mark correspond with two numbers – one in the row running top to bottom, and one in the row running left to right. Using this system, the letter A becomes "11" and B becomes "12". HELLO! would be become 23 15 32 32 35 64.

REMINDER:
If this module is the first in a larger course, we recommend you spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

Conducting the Activity

Part 1: Unprotected Connections

The trainer divides the participants into three groups and separates them physically, with one group situated between the other two.

1. The trainer explains: We have gone back 25 years and there's no more email – all we have is the postal service. Participants will need to send an urgent message(s) to the other team on these postcards, and will have to get the postal service (group in the middle) to come and collect their postcards, and deliver them.
2. The trainer asks participants to "address" their postcards, including the "sender" name and a short message. After all, this is what we all need to do in real life.
3. The trainer explains to the other group (in the middle) that they are the postal service and will have to convey messages between the two groups receiving and delivering messages. But they're not just any postal service – they're collecting all the information that is being sent and will report back to the group after the activity.
4. The trainer allows both sides one "round" of communication, then thanks them for indulging in old fashioned communication – successfully.
5. The trainers asks participants: Is the postal service to be trusted?
6. Then, the trainer invites a representative of the postal service to report back on the messages. There's often funny stuff here. The trainer also can prompt: Did you see who sent a message to so-and-so? Did you see the message? Were there any funny messages?

Discussion

At this point the trainer can encourage a discussion about what was learned. Some questions that can help:

1. Did the postal service ever work this way in your country?
2. Would you trust it if it did?
3. If you knew that this was the way the system worked, but it was your only way to communicate, what would you change?
4. Do you think the Internet works this way?
5. If it does, what can we change to make it safer?

Before moving to the next step, the trainer should explain that the exercise, though very simple, shows how regular Internet traffic – sometimes called HTTP traffic – works. When we send information out, such as a blog post, that information goes through many hands and many people can see what we're up to.

Part 2: Protected Connections

1. The trainer asks the participants to return to their spots to repeat the exercise. However, this time, the trainer hands a copy of the cipher (above) to each of the two sender/receiver groups.
2. The trainer asks one or two participants on each "side" to write messages to the other, using the cipher for the body text. They cannot use it for the address, however, because the postal service would not know how to deliver it.
3. Ask the sender/receiver groups to "send" their messages.

Discussion

The trainer thanks the participants for their help in illustrating another kind of web traffic – encrypted traffic, and encourages discussion:

1. Did the people sending the messages find it difficult to understand the cipher?
2. Did the people in the middle have any idea of what the code might be? Did they try to break it?
3. Looking at the cipher, is this even a complicated form of encryption?
4. Did the people sending messages enjoy the exercise?
5. Would they like to do the same thing with their online communications?

1. ACTIVITY (30 minutes)–ADVANCED

In this module, we provide alternative activities and links to more information related to the use of public key encryption in email. Trainers should not present this material to participants until the basic-level material has been reviewed.

ADDITIONAL MATERIALS:

- Markers.
- Blank postcards.
- Envelopes (two sizes).
- Index cards, or premade cards for elements in the Web (see the list immediately below: "Sender," "Access Point," etc.).

Postcards and Candy Thieves

The purpose of this activity is to illustrate the journey of most email and to introduce one method for protecting the contents of email. (Based on the "The Postcard Game," appearing on LevelUp.)

Preparation

The trainer makes one card for him or herself but does not show this to the class. The card should have an illustration that indicates the trainer is a "villain," such as angry eyes or pointy horns.

Before the training begins, the trainer prepares two envelopes. Both need to be filled out with the following information, as if they were letters:

From: me-user@yahoo.com
To: you-user@gmail.com
Subject: Urgent and Important
Address: Email 101, Snowdonia

Getting Started

The trainer guides the participants through the following steps:

- Asks participants to organize themselves into a U-shaped line (this works best with up to 10 participants, or subgroups that size).
- Asks for two volunteers, one at each end of the "U," to represent two friends who are email pen pals or "friends."
- Assigns the remaining participants to play other parts of the Internet, with each person wearing or holding a card that identifies them as:
  - Sender
  - Wi-Fi access point
  - Local ISP (ISP = Internet service provider)
  - National ISP
  - Mail Service: Yahoo!
  - Mail Service: Gmail
  - National ISP
  - Local ISP
  - Wi-Fi access point
  - Recipient
- Distribute the cards in such a way that the mail (Yahoo! and Gmail) services are at the "bottom" of the U and standing next to each other.
- Ask one participant to pretend that he or she lives in a country with Internet restrictions and possible surveillance.

Conducting the Activity

The trainer compliments participants for their dramatic representation of the Internet and asks them to prepare themselves for their most difficult role: depicting a typical journey for an email message. The trainer guides the participants through the following steps:

- The Sender is asked to write a message on an index card, which is then put in an envelope that was prepared before the event (see Preparation, above).
- The Sender then passes the envelope to the person representing a Wi-Fi access point, who holds it while the trainer explains:
  - As a sender is sending an email, the first place that the bits of the email travel to is the Wi-Fi access point.
  - This access point is like the router in an office. If the office has a network administrator, that person is able to see the traffic on the network and can likely see the information on the outside of this envelope (To, From, Where, etc.).
  - Sometimes people talk about "secure connections" and something called "HTTPS." If we assume that is the case here and that the network administrator cannot read the contents of the email, then what can he or she see?
- The Wi-Fi access person hands the card along to the Local ISP person. The trainer explains:
  - This is the company that you or your organization pays in order to get Internet access. Everything you do on the Internet goes through the company's servers.
  - It has the ability to record activities and, like your network administrator, can see everything on the outside of the envelope.
  - If it is your email service provider, it can see the contents of the message, too.

- The Local ISP person hands the card to the National ISP person. The trainer explains:
  - Very often, local ISPs are small companies that rent equipment and bandwidth from national providers. Those national providers might be private companies or they might be state institutions.
  - Just as with the Local ISP, everything you do on the Internet goes through the National ISP's hands. It has the ability to record activities and, like your network administrator, can see everything on the envelope.
- The National ISP person hands the card to the Yahoo! person. The trainer explains:
  - The email here has arrived at Yahoo! because our Sender is a Yahoo! customer and the Sender's address is a Yahoo! address.
  - Staff at Yahoo! have the ability to read everything in the postcard including the message.
  - The trainer asks the Yahoo! person to open the envelope and remove the letter inside.
- The Yahoo! person hands the letter to the Gmail person without an envelope. The trainer explains:
  - Because our Recipient has a Gmail account, Yahoo! has to hand over the email to Google. Sometimes, these connections between really big email providers aren't protected.
- At this point, the trainer reveals his or her own card, showing a menacing cartoon face and steps between the Yahoo! and Gmail people. The trainer explains:
  - This is what some people are concerned may be happening in one of the NSA surveillance programs.
- The Gmail person holds onto the letter. The trainer explains:
  - Just like at Yahoo!, the staff at Gmail have the ability to read everything in the postcard including the message. And the postcard will sit around until someone picks it up. That could be a long time.
  - The trainer asks this question: How long do you think Yahoo! and Google will hold onto this postcard even after it is delivered? Answer: Forever. These companies have copies on many servers so that you don't lose your email. And they are required by law in some countries to maintain those copies for six months or longer.
- The trainer now announces that the Recipient has logged on, and asks that the postcard be sent through the remaining people in the chain:
  - The Gmail person sticks the letter into the second envelope.
  - The trainer congratulates everyone for a job well done. Yahoo!

The trainer now asks participants to remain in their spots and explains that they will now look at one method for protecting emails – including the content of emails. The trainer:

- Holds up a bag of candy and announces that the Sender wants to send it to the Recipient, but (with a smile) doesn't trust the other participants to deliver it.
- Produces a small metal box which can be locked and places the candy inside, closes the lid and locks the box.
- Explains that he or she doesn't have the key to open the box.
- Sends the box down the line of "Internet" representatives, explaining that this is like sending an email that has been sealed with PGP.
- When the box is received at the end, the last person produces a key and unlocks the box. Hopefully, they share the candy with the rest of the participants!

NOTE: *In this exercise, trainers need to alert participants that there are additional steps, or "nodes," that we have skipped, including national gateways, in order to keep the illustration to a reasonable size.*

A partial demonstration of how this exercise works is available on YouTube.

2. DISCUSSION (15 MINUTES)

With the activity completed, trainers may wish to have participants sit in a circle or a half circle, so they can address one another. The following questions may help start the discussion. Trainers are welcome to add to this list or improvise as they see fit.

- Were people in the group aware of how many steps an email takes before it reaches its destination?
- Was it clear to the participants that sending an email to a person actually means sending it to an email service that holds onto it until the recipient logs on and asks to collect their email?
- In the Internet chain, who could access the name and subject of the email? Who could read the email itself?
- Who had a copy of the email?
- Was it clear to the participants that even if they have a protected connection to those services, the content of the email itself is not protected from the services?
- Who (in this country) do the participants think is likely to be interested in reporter's emails?
- What email service do they use? Why?
- Is anyone currently taking steps to protect their email? How?

Materials that may help the discussion:

Video: "Story of Send" (Google). This animated marketing video reinforces the concepts of the Activity, showing email as it travels from a PC to Google's servers. However, trainers should bear in mind that it is a marketing video and will contain messages from Google promoting their services.

3. INPUT / LECTURE (30 MINUTES)

Below, we have provided a case study, key messages and some materials to help get the point across.

Trainers are welcome to update, add or improvise as they see fit.

Case Study

Edward Snowden

Introduction: It is unlikely that Guardian journalist Glenn Greenwald would have been able to meet Edward Snowden without learning to use software that protected some of their conversations.

Story: When former National Security Agency contractor-turned-whistleblower Edward Snowden, now in Russia, revealed that the agency was collecting private phone calls and monitoring foreign leaders' conversations, he took special care to protect his communications with the journalists who later wrote about him and his leaked documents.

Articles published in Salon reveal that Snowden first contacted Guardian reporter Glenn Greenwald in early 2013 and wrote to him about having information of "great interest" to communicate. However, Snowden only wanted to communicate using encryption – a way of concealing a message so that only people with a special password or key can read it. When Greenwald wrote back that he did not have encryption software, Snowden sent him a step-by-step setup video with instructions for installing PGP.

Encrypted email, when done using public key cryptography, is extremely effective as intended end users are the only ones who should be able to decrypt the protected communications. But it also can be complicated and lengthy process to set up. Greenwald reportedly watched the video, but never got around to installing it.

Snowden then contacted documentary filmmaker Laura Poitras and asked for her public encryption key. Unlike Greenwald, Poitras had covered surveillance issues and had worked with sensitive sources when she was filming WikiLeaks and was more comfortable encrypting her communications. She sent her public encryption key that would allow him to send an encrypted email that only she could open with her private key.

"I already had encryption keys," she told Salon. "But what he was asking for was beyond what I was using in terms of security and anonymity."

Snowden then sent her instructions to create an even more secure system to protect their communications and sent Poitras an encrypted message that outlined a number of secret surveillance programs run by the government that he could prove existed. When Snowden suggested that Poitras work with Greenwald, she helped Greenwald install encryption software and Greenwald and Snowden began to communicate using an encrypted chat program.

Case Study based on:

- "How Laura Poitras Helped Snowden Spill His Secrets" (The New York Times).
- "Cryptic Overtures and a Clandestine Meeting Gave Birth to a Blockbuster Story" (The New York Times).
- "How Glenn Greenwald Began Communicating With NSA Whistleblower Edward Snowden" (HuffingtonPost.com).
- "How We Broke the NSA Story" (Salon.com).

Related videos:

- "Glenn Greenwald Full Interview on Snowden, NSA, GCH" (BBC Newsnight).
- "PRISM Whistleblower – Edward Snowden in his own words" (Freedom of the Press Foundation).

Interaction with Participants:

The case illustrates the value of protected email. Some questions to consider:

- Knowing what we do now about the scope of surveillance by some intelligence services, is it likely that Greenwald and Snowden would have been able to meet later in Hong Kong if they had not used encryption in their email?
- Have you ever worried that your emails and chats were being intercepted?
- What steps have you taken to learn about protecting your communications (step-by-step videos, online guides)?
- Although Glenn Greenwald wrote about highly sensitive issues, he admitted that he found encryption to be too complicated (he even ignored the video and the step-by-step guide that Snowden sent him). What would you have done in his place?

Talking Points for the Trainer (BASIC)

With the case study concluded, the trainer now direct participants to their Class Notes.

- On the Internet, personal communications always go through someone we don't know.
  - ✔ Some people have this access by design – such as our ISP (or mobile service provider), some for legal reasons – such as the NSA or other intelligence services, and some due to weaknesses in the systems used – such as hackers.
- A "secure connection" to an email service does not protect the content of your email from the person/company running that email service.
  - ✔ Lavabit, the email service Edward Snowden used when communicating with Glenn Greenwald, was shut down by its owner when the NSA demanded the keys that enabled protected connections to its servers. If they had been able to get the certificate, the NSA would now be able to observe emails on the Lavabit service just as if there was no secure connection.
- A more secure way to protect your communications is through an HTTPS connection (Hypertext Transfer Protocol Secure). This is also sometimes called SSL (Secure Sockets Layer).
- In webmail, HTTPS can protect your connection when you sign into your account and may also protect messages between you and your email service provider.
  - ✔ One example is the service provider Google. If you use Gmail, you will see the letters HTTPS appear at the start of your address (https:mail.google.com), located at the top of your browser. This means your connection is protected between your PC and Google.
- Not all Web mail services support HTTPS connections. You can test this by typing the "s" at the end of HTTP in the address.
- The add-on called HTTPS Everywhere also can direct you to the HTTPS version of some popular sites automatically.
- Some things to keep in mind:
  - HTTPS protects your connection, not the email content.
    - ✔ This means that your email content could be visible to your service provider.
  - The person who receives your email must use HTTPS, too, for their connection to be protected.
    - ✔ This means that your email content is visible to your recipient's service provider, not just your own.

TRAINER'S NOTE:
Text with a ✔ does not appear in the student version of the Class Notes.

  - If you see a warning message when visiting an HTTPS site that tells you the certificate is not recognized, do not proceed.
    - ✔ Investigate. This type of warning may mean that someone has created a website pretending to be the one you were seeking.

- A more advanced method for protecting your email's content is to use public key encryption – sometimes called end-to-end encryption.
  - ✔ An example of this is called PGP (or Pretty Good Protection) and this won't be covered in this basic module.
- Other steps we can take to protect our accounts, so that others can't break into them:
  - Use strong passwords (find tips at Security in-a-box).
  - Turn on two-step verification (this video clip shows how).
    - ✔ Two-step verification is sometimes described this way: When signing in, you are required to provide something you know (like a password) AND something you have (like a fingerprint). In our next exercise, we will see how to use a password AND a code on our mobile phone(s) in combination to make an email account more secure.
- A variety of services support two-step verification in some form:
  - Dropbox.
  - Facebook.
  - Google (all services).
  - Microsoft.
  - Twitter.
  - Yahoo!.

Talking Points for the Trainer (ADVANCED)

With the case study concluded, the trainer now direct participants to their Class Notes.

TRAINER'S NOTE:
Text with a ✔ does not appear in the student version of the Class Notes.

- On the Internet, personal communications always go through someone we don't know.
  - ✔ Some people have this access by design – such as our ISP (or mobile service provider), some for legal reasons – such as the NSA or other intelligence services, and some due to weaknesses in the systems used – such as hackers.
- A "secure connection" to an email service does not protect the content of your email from the person/company running that email service.
  - ✔ Lavabit, the email service Edward Snowden used when communicating with Glenn Greenwald, was shut down by its owner when the NSA demanded the keys that enabled protected connections to its servers. If they had been able to get the certificate, the NSA would now be able to observe emails on the Lavabit service just as if there was no secure connection.
- A more secure way to protect your communications is through "public key encryption."
  - ✔ This is what we demonstrated in the "Postcards and Candy Thieves" Activity.
- PGP is one method that provides:
  - Confidentiality
    - ✔ Encrypting the content of your message so that even the service provider or anyone else who manages to intercept it cannot read it – this is also known as "end-to-end encryption."
  - Authentication
    - ✔ Only allowing the message to be read by someone who has the correct key. It does not encrypt the "metadata" of the email, however (the information that includes the To, From and Subject fields, as well as the time the email was sent and received). Metadata is visible, just like the outside of a traditional letter envelope.

- PGP protects the content of your email only. It does not encrypt other information.
- We can take steps to protect our accounts, so that others can't break into them:
  - Use strong passwords (find tips at Security in-a-box).
  - Turn on two-step verification (this video clip shows how).
    - ✔ Two-step verification is sometimes described this way: When signing in, you are required to provide something you know (like a password) AND something you have (like a fingerprint). In our next exercise, we will see how to use a password AND a code on our mobile phone(s) in combination to make an email account more secure.
- A variety of services support two-step verification in some form:
  - Dropbox.
  - Facebook.
  - Google (all services).
  - Microsoft.
  - Twitter.
  - Yahoo!.

4. DEEPENING (90 MINUTES)

This section is divided into Basic and Advanced exercises and focuses on Windows applications. Trainers and participants who need equivalent applications for Mac OS should review the handout Notes for Mac Users.

BASIC

PART I: Two-Step Verification (20 minutes)

The trainer walks the participants through the set-up process for two-step verification, showing how to enable the feature online and how to activate Google Authenticator on the trainer's smartphone. When the demonstration is complete, the trainer can assign participants to enable the feature for themselves. However, to save time we recommend that this be assigned as homework. Complete instructions are located on this Google Support page.

Some things to mention about two-step verification:

- Users have a choice: They can either retrieve codes from Google Authenticator or have them sent as SMS messages.
- Users need to print out "backup" codes for their accounts when this is offered during the set-up process. These backup codes grant emergency access to the account in case the phone is lost, stolen or confiscated. These codes need to be protected.
- Users can create a special "exception" code for an email application (like Thunderbird or Outlook) that, otherwise, would not be able to use two-step verification.

Materials that May Be Useful:

- Video: "2 Step Verification" (Google support).

PART II: HTTPS Everywhere

In this exercise, the trainer asks participants to install the HTTPS Everywhere add-on in their browser and demonstrates its effect when visiting a website that has both an HTTP and an HTTPS version.

1. The trainer should begin by launching either the Firefox or Chrome browser.
2. Then, using the projector, the trainer should demonstrate how to reach the download page for HTTPS Everywhere.
3. Asking participants to wait, the trainer installs HTTPS Everywhere and restarts the browser, if required.
4. The trainer opens a second browser (e.g., Internet Explorer or Safari) that does not have HTTPS Everywhere installed.
5. For demonstration purposes, the trainer uses the second browser to visit microsoft.com and points out that the address begins with "HTTP" (without the "S").
6. The trainer also shows in the second browser that a user can type "S" at the end of HTTP and reload the page. The page will now be protected by HTTPS and a small padlock icon should appear next to the address to confirm this.
7. The trainer now shows the first browser and types the same address: microsoft.com. The resulting page should display https://www.microsoft.com, begins with the "S" already in place.
8. The trainer now asks participants to replicate the demonstration and should visually confirm that they have been successful.

SOFTWARE AND INSTALLATION:

- Firefox web browser or Chrome web browser
- The HTTPS Everywhere extension (EFF.org)
- Google Authenticator (for Android or iPhone)

(ADVANCED ONLY):

- Thunderbird
- Enigmail (an add-on for Thunderbird)
- GnuPG

Some things to mention about HTTPS Everywhere:

- It contains a list of popular websites that support HTTPS connections. However, the list is limited.

PART III: Other Gmail Tools

In this exercise, the trainer introduces participants to the Details link in Gmail, which shows them where and when their account has been accessed.

1. The trainer explains that, while Gmail is not the only public webmail service available, it has been the first to offer safety features that are becoming standard, such as HTTPS connections and two-step verification.
2. The trainer continues that another useful feature in Gmail can be the Details link located in Inbox.
3. The trainer, already having logged into the account that he or she is using for demonstration purposes, goes to Inbox and scrolls to the bottom of the page. At the bottom right, the trainer points out the following:
   - There is a message that tells the user when the Inbox was last accessed.
   - There is a link called Details. Clicking on this link will open a new window that displays:
     a. Access type: Was the activity through a browser? Through a special application like Outlook, Mail or Thunderbird? Was it through a mobile device?
     b. Location (IP): Where does the access appear to be coming from? What is the digital "address" of the access? The "IP" means the Internet Protocol address – every device that connects to the Internet is assigned one during that connection.
     c. Date/Time: When did this happen.
4. When the trainer has shown the information in the Details window, he or she should encourage participants to investigate this tool on their own.

Some things to mention about Details:

- If you see something strange in your Details window, such as your email being accessed regularly from another country or city, it could mean that someone has gotten your email credentials.
- In that case, you may want to click the "Sign Out All Other Sessions" button at the top of the Details window and then change your password.
- If you then continue to see similar behavior, check if you have given other services permission to access your email. Sometimes, people who travel frequently give travel applications access for alerts.

ADVANCED

PART I: Two-Step Verification (20 minutes)

Trainers should refer to this same exercise in the Basic section (above). However, trainers should avoid asking participants to enable this feature during class. If two-Step Verification is enabled during this exercise, it will require that trainers also instruct participants in creating an exception code called an App-Specific Password.

PART II: Thunderbird & GnuPG (60 minutes)

Participants need to have downloaded and installed the recommended software for this module prior to class or during a break. If participants were not sent the hands-on guide "Thunderbird with Enigmail and GPG – Secure Email Client" prior to class, this would be a good time to distribute it.

The trainer reminds participants that they are about to learn the method that Snowden and Greenwald used to communicate – the same sort of protection that the "Postcards and Candy Thieves" Activity illustrated at the start of the module.

Before beginning, it may be useful to show the following clips to participants to illustrate the concept:

- Video: "Gambling with Secrets: 8/8 (RSA Encryption)." Trainer only needs to show up to 01:57.

Exercise #1: Create a Key Pair

The trainer demonstrates how to make a "key pair" – the equivalent of a key and the box to which it belongs. Participants should be asked to wait until the process is completed before attempting to repeat it:

1. Launch Thunderbird (GnuPG and Enigmail installed on the same PC).
2. Open the Key Management window (in the menu, select Open PGP → Key Management).
3. From the menu, choose Generate and then New Key Pair.
4. Select an email address for which you'd like to generate the key pair.
5. The trainer will be asked to create a password – another way to protect the use of a new key and lock; for the sake of time. The trainer may choose to check the box marked No Passphrase. However, this needs to be acknowledged during the demonstration.
6. Click Generate Key. This process can take several minutes. During that time, and before the trainer asks participants to try this on their own, two points can be made:
    a. Even though the new key pair was made "for" one specific email address, you can use the same key for more than one email address.
    b. Because you will never be able to open PGP's email without your personal key, it's crucial that everyone protect their key with a backup (and an encrypted one is best). Information about encryption can be found in our Keeping Data Safe module.
7. Click Generate Revocation Key and save it on the desktop. Explain: The revocation key is an "emergency" tool that is used to invalidate your public key in the event your private key is lost or stolen. Just like the private key, the revocation key needs to be protected.

When the trainer is done, every participant needs to be asked to repeat the process for him or herself. To reinforce the steps of creating a key pair and sending it to someone, the trainer may wish to ask for a volunteer to try the process in front of the class (with helpful coaching from classmates).

The trainer congratulates the participants for having accomplished the most difficult part of the exercise!

Exercise #2: Share Your Public Key

The participants can now send one another their public keys – and ONLY their public keys. The private key must never be shared or emailed. (Alternatively, if the trainer has created a mailing list for the training event, public keys can be sent to that address to reach everyone at once.)

Method 1: By hand

To conduct the exercise:

1. Launch Thunderbird (GnuPG and Enigmail installed on the same PC).
2. Open the Key Management window (in the menu, select OpenPGP → Key Management).
3. Highlight the email address for which a new key pair was generated in the previous exercise.
4. Right-click the address and select Export Keys to File.
5. Select "Export Public Keys Only." (It must ONLY be the public key.)
6. Export to a USB flash drive or other external drive.

Key Messages:
Trainers may wish to point out that an in-person exchange of keys is the most secure method because both parties have control of their keys and can plainly see each other. However, that is not always possible.

Method 2: By email

To conduct the exercise:

1. Launch Thunderbird (GnuPG and Enigmail installed on the same PC).
2. Open the Key Management window (in the menu, select OpenPGP → Key Management).
3. Highlight the email address for which a new key pair was generated in the previous exercise.
4. Right-click the address and select Send Public Keys by Email.
5. Fill in the To address field of your email and Send (for the purpose of the exercise, the trainer can either send to him or herself or send to the group's mailing list, if one has been created).

When the trainer is done, every participant repeats the process. As participants conduct the exercise, the trainer mentions that this is only one method for sharing a public key. Public keys can be copied to external devices and shared that way. Also, public keys can be pasted into the text of an email. We recommend that those who are interested in learning more about PGP in email review the handout "Thunderbird with Enigmail and GPG – Secure Email Client."

Exercise #3: Import a Public Key

This last exercise will have participants adding classmates' public keys to their "library" of keys. The trainer may wish to demonstrate this step first and to remind participants not to accidentally share their private keys.

Method 1: By hand

To conduct the exercise:

1. Launch Thunderbird (GnuPG and Enigmail installed on the same PC).
2. Receive a USB flash drive with participant's public key on it.
3. Open the Key Management window (in the menu, select OpenPGP → Key Management).
4. Choose File and then Import Keys from File.
5. A pop-up window will ask the user to point to the public key(s) that are to be imported.

Method 2: By email

To conduct the exercise:

1. Launch Thunderbird (GnuPG and Enigmail installed on the same PC).
2. Find an email sent by someone wanting to share their public key and save that key somewhere easy to find in the demonstration, such as the Desktop.
3. Open the Key Management window (in the menu, select OpenPGP → Key Management).
4. Choose File and then Import Keys from File.
5. A pop-up window will ask the user to point to the public key(s) that were downloaded.

Participants need to be asked to repeat the sharing and importing process until everyone in the group has received everyone else's public key.

Exercise #4: Validate and Sign

This exercise emphasizes the importance of confirming the authenticity of public keys. We direct trainers to review section 4.4 of the handout "How to Use Enigmail with GnuPG in Thunderbird" and to follow the steps described there – first as a demonstration, then asking participants to replicate that demonstration.

Exercise #5: Use It!

If the previous exercises have been completed and the trainer has confirmed that each step has been followed, participants can send test messages, either to the trainer or to a partner in the group.

As before, the trainer should first demonstrate the process. In this case, by:

1. Composing an email.
2. Selecting a recipient whose key has already been imported.
3. Choosing the OpenPGP button on that email.
4. Selecting "Sign Message."
5. Selecting "Encrypt Message."
6. Sending the message.

After five minutes, the trainer can ask the participants to stop for a moment to report whether they have succeeded. It is likely that some participants will find that they have sent or received email that was not encrypted.

If so, the trainer should now review these key messages. If time allows, the trainer can demonstrate the process of creating a per-recipient rule.

Key Messages:

- These applications (Thunderbird, Enigmail and GnuPG) will not encrypt email by default unless directed to do so.
- You can encrypt all email from an address by default by viewing that address's settings in Thunderbird, selecting OpenPGP Security, and then checking the box to "Encrypt Messages By Default." However, your email will not be encrypted unless you have the public key of your recipient. Enigmail will ask you to supply it.
- You can also encrypt email to a specific person's address by default by creating a per-recipient rule. To get started, open an email from the person for whom you want to create the rule, right click their address in the From field and select "Create OpenPGP Rule from Address…."

NOTE: *Trainers may wish to consult the walk-through from the Enigmail developers for guidance.*

SPECIAL CONSIDERATION (REPEATED):

It is essential that trainers who undertake this module visually confirm that participants are using the recommended software correctly. It is common for participants to assume that their emails will be automatically encrypted once they have installed the applications. However, this is not the case. By default, none of the user's email is automatically encrypted unless the user changes his or her security preferences. Instead, users must manually choose to encrypt individual emails in order for them to be encrypted.

5. SYNTHESIS (10 MINUTES)

We recommend that trainers use this wrap-up session for informal questions to the group, covering the material that has been covered in the module. Following are some questions that may help participants think about using what they have learned:

- What does two-step verification do?
- Some other popular Web services also now offer two-step verification, including Facebook, Twitter, Microsoft (e.g., SkyDrive) and Dropbox.
- There are other security features in Gmail that you can learn about from Google's support site (the links included in the Before You Start section of this module may help.)
- We also discussed how you can protect the content of the emails you send by using PGP.
- PGP does not encrypt the subject heading of your email or hide who sent it and who received it.
- It's possible to add similar protection to chat conversations, but participants need to read the chapter called "Pidgin with OTR" on the Security in-a-box website.
- Are there other ways that you protect your email and email accounts that we have not discussed?
- Final point: There are different levels of protection for email and other communications. This class has addressed one that is considered very secure because it protects the content of your email. If you would like to learn more about other ways that email connections can be protected, please go through the additional resources we've provided below.

MAC OS X: PROTECTING EMAIL (ADVANCED ONLY)

The following material includes applications and exercises that may be useful to participants with Mac OS X and iOS devices. Trainers working in pairs may wish to divide their efforts during Deepening exercises, with one trainer working with Windows/Android users and one trainer working with OS X/iOS users.

Software & Installation

(For Advanced sessions only)

- Thunderbird.
- Enigmail (an add-on for Thunderbird).
- GPG Suite (GPGTools).
    - Guide: "First Steps".

Deepening

Exercises #1 & #2: Please refer to the official walk-through "First Steps" from the developer for instructions

Key messages:

- When uploading a public key so that others may find it, GPGTools will automatically upload your new key to the default keyserver set in the GPG Keychain Preferences. This may not be the same as the default keyserver for Enigmail. Therefore, some users may have trouble locating and downloading other users' public keys if they've used either Enigmail or GPGTools to generate and upload their first public key.

  We recommend manually going into the Preferences section of GPG Keychain Access, cycling through each of the keyservers listed and then right-clicking (CTRL + click) on your key and selecting, "Send public key to keyserver." This way your public key is available on more than one keyserver.
- We also recommend adding the keyservers available in Enigmail that aren't included as the default keyservers in the GPG Keychain Preferences under Keyserver. To do this, type into the current text space for the keyserver and hit return, then select it as a keyserver before "send[ing your] public key to keyserver."

Exercise #3: Importing a Public Key

To conduct the exercise using GPGTools' GPG Keychain Access:

1. If searching via a known email address: Go to Key → Search for Key → type in the email address to search according to email address.
    a. Select the appropriate key and click "Retrieve Key."
    b. Similar to uploading public keys, you may have to check multiple keyservers as GPGTools doesn't search all keyservers at once. To do this, go into Preferences → Keyserver and try different keyservers. If you know or think a particular key is hosted at a specific keyserver, add that keyserver to your list in Preferences. Two of the most commonly used keyservers by most gpg users are gpg.mit.edu and http://pool.sks-keyservers.net.

Exercise #4: Validate and Sign

- **Verifying:** If possible, you should always attempt to verify that a key belongs to the person you expect by confirming their key's fingerprint. (You should do the same for your key with others.) You can find the fingerprint for a key by double clicking a key in your Keychain and locating the fingerprint under Key.
- **Signing:** In order to send either encrypted or signed messages to a user, you need to "sign" that person's key. We recommend that you sign keys on your device. To do this, right click (CTRL + click) on an entry and select "Sign…." The key you will sign with will be your own (and will be the default). You then have the option to say how carefully you've verified that a given key is that of the person to whom you believe it belongs. Last, you can set an expiration date for your signature, and select "Local Signature."

Key messages:

- Public signatures can lead to sensitive networks being "mapped out" by assessing which keys have been signed by whom. We recommend you select "Local Signature" when signing a key unless asked otherwise by the owner of the key.
- If searching via a Key ID that you have for a contact, which is the last eight characters in a key fingerprint preceded by "0x" (such as "0xAC5409EC"), go to Key → Retrieve from Keyserver and enter the Key ID. Select the appropriate key and click Retrieve Key.

NOTES

- On the Internet, personal communications always go through someone we don't know.
- A "secure connection" to an email service does not protect the content of your email from the person/company running that email service.
- A more secure way to protect your communications is through an HTTPS connection (Hypertext Transfer Protocol Secure). This is also sometimes called SSL (Secure Sockets Layer).
- In webmail, HTTPS can protect your connection when you sign into your account and may also protect messages between you and your email service provider.
- Not all Web mail services support HTTPS connections. You can test this by typing the "s" at the end of HTTP in the address.
- The add-on called HTTPS Everywhere also can direct you to the HTTPS version of some popular sites automatically.
- Some things to keep in mind:
  - HTTPS protects your connection, not the email content.
  - The person who receives your email must use HTTPS, too, for their connection to be protected.
  - If you see a warning message when visiting an HTTPS site that tells you the certificate is not recognized, do not proceed.
- A more advanced method for protecting your email's content is to use public key encryption – sometimes called end-to-end encryption.
- We can take steps to protect our accounts, so that others can't break into them:
  - Use strong passwords.
  - Turn on two-step verification.
- A variety of services support two-step verification in some form:
  - Dropbox.
  - Facebook.
  - Google (all services).
  - Microsoft.
  - Twitter.
  - Yahoo!.

NOTES (ADVANCED ONLY)

- On the Internet, personal communications always go through someone we don't know.
- A "secure connection" to an email service does not protect the content of your email from the person/company running that email service.
- A more secure way to protect your communications is through "public key encryption."
- PGP is one method that provides:
  - Confidentiality.
  - Authentication.
- PGP protects the content of your email only. It does not encrypt other information. In this lesson, we learned about:
  - Thunderbird.
  - Enigmail (an add-on for Thunderbird).
  - GnuPG.
  - Google Authenticator (for Android or iPhone).
- We can take steps to protect our accounts, so that others can't break into them:
  - Use strong passwords.
  - Turn on two-step verification.
- A variety of services support two-step verification in some form:
  - Dropbox.
  - Facebook.
  - Google (all services).
  - Microsoft.
  - Twitter.
  - Yahoo!.

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

access point – Any point at which a device connects to the Internet, usually a wireless access point (Wi-Fi).

domain name – The address, in words, of a website or Internet service; for example, speaksafe.internews.org.

encryption – A way of using mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

email client – An application installed on a PC or mobile device that organizes email and allows users to read and write messages offline. Popular examples include Microsoft's Outlook and Mozilla's Thunderbird.

Enigmail – An add-on for the Thunderbird email program that allows it to send and receive encrypted and digitally signed email.

Firefox – A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

HTTPS – Hypertext Transfer Protocol Secure (or HTTP Secure). An encryption protocol widely used on the Internet to protect connections between websites and the people who use them. Also frequently referred to as SSL (Secure Sockets Layer).

Internet Protocol address (IP address) – A unique identifier assigned to your computer when it is connected to the Internet.

Internet service provider (ISP) – The company or organization that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.

multi-factor authentication – A method of protecting a Web account that requires the user to provide at least two kinds of information when signing in, instead of just one password. Two-step verification systems used by Google, Facebook, Twitter and Dropbox are examples of what is more generally called multi-factor authentication.

Off the Record (OTR) – An encryption plugin for the Pidgin instant messaging program.

PGP – Pretty Good Protection, a popular method of encrypting the content of email and email attachments. It requires correspondents to share "public keys" with one another, which are then used to encrypt email. The email can only be decrypted with the recipient's "private key" (which is never shared).

Pidgin – A FOSS instant messaging tool that supports an encryption plugin called Off the Record (OTR).

portable applications – Programs that run from a portable device, such as a flash memory stick or memory card, and do not require installation under the PC's operating system.

server – A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers.

service provider – A company, either private or public, that provides mobile phone service or Internet service to customers.

SSL – Secure Sockets Layer. An encryption protocol widely used on the Internet to protect connections between websites and the people who use them. Also frequently referred to as HTTPS (Hypertext Transfer Protocol Secure).

Thunderbird – A FOSS email program with a number of security features, including support for the Enigmail encryption add-on.

two-step verification – A method of protecting a Web account or a file that requires the user to provide two kinds of information when signing in, instead of just one password.

6. MOBILE PHONE SAFETY

WHY THE TOPIC MATTERS

A cellphone or smartphone might be a journalist's most valuable tool for work. It contains contact lists, photographs, email and instant messages, among other things. But phones are also excellent tracking and monitoring devices. While it's unlikely we will ever live without them, as journalists we should know how they work and make informed decisions about how to use them.

WHAT PARTICIPANTS WILL LEARN

Concepts: Insecurity of mobile phone networks. Habits can mitigate the risks.

Skills: Installation of Orbot, Orweb and ChatSecure; enabling encryption and strong passwords on Android phones.

NOTE TO TRAINERS: This module involves the distribution and demonstration of software that may not be permitted to use in some countries. We recommend that trainers do basic research about local laws that govern Internet access in the country where they are training before using this module to train journalists. In some locations, for instance, the use of VPNs is not permitted.

OBJECTIVES:

Learning about risks and safety precautions to use when using mobile phones.

PRACTICAL USES:

Avoiding surveillance, protecting data on phones, avoiding exposure of information in calls and text messages.

PREREQUISITE SKILLS:

This module assumes that the participants are able to install applications on their phone.

BEFORE YOU START

The following resources may help trainers improve their knowledge about this module's topic prior to class:

- "Surveillance Self-Defense: Mobile Devices" (eff.org).
- "How to use mobile phones as securely as possible" (Security in-a-box).

MATERIALS NEEDED

In addition to the common training materials we recommend in the Guide for Trainers (see the "Training Tips" section), trainers will need the following for this lesson:

Handouts

- Class Notes.
- Glossary.
- Guide: "How to Use Mobile Phones as Securely as Possible" (Security in-a-box).
- Guide: "How to Use Smartphones as Securely as Possible" (Security in-a-box).

NOTE: *Trainers requiring information related to Apple devices should consult the "Mac OS X" training notes found immediately afterthe Synthesis section of this module."*

RELATED MODULES

- Assessing Risks.
- Protecting Email.
- Keeping Data Safe.

OTHER

Additional Requirements

At the time of writing, the Android operating system (supporting phones as well as tablets) offers the most open-source applications that provide the privacy discussed in this module. While various privacy tools are available for iOS (which supports both iPhones and iPads), at the time of writing the only open-source app we recommend is ChatSecure on iOS. While there are a number of other exciting apps becoming available for iOS that are worth considering as alternatives (such as Wickr and Lookout), they are not open source. Given the fact that there have been multiple vulnerabilities discovered in closed-source iOS apps (Snapchat as the most public example as of the time of writing), we do not suggest using or recommending these to users. For more information about open-source software, please refer to the Guide for Trainers.

LESSON PLAN

1. ACTIVITY (30 MINUTES)

VIDEO (10 minutes)

We recommend that trainers start this module by showing this video clip from a recent TED Talk:

- **Video:** TED Talks: Malte Spitz: "Your Phone Company is Watching" (10 minutes).
- **Alternative video:** Shortened version of Malte Spitz's talk (8.5 minutes).

NOTE: *As with all video clips located on YouTube, trainers can enable the subtitles feature for any video clip if the sound is unclear.*

About This Video

TED – the Technology, Entertainment, Design association that holds semiannual gatherings – frequently provides talks about trends in tech and science.

Green Party politician **Malte Spitz** in Germany explains what he learned about cell phone privacy (or the lack of it) when he sued service provider Deutsche Telecom (DT) to reveal the data that it had been storing about his phone. When Spitz received his data in a raw format, he worked with journalists at Zeit Online to create **an interactive map that demonstrates how Spitz's location was clearly tracked,** right to the minute. (The map requires an Internet connection to access.)

On the map, the gray lines immediately below the map represent days; a small red box that appears on a selected day represents the specific time, and this can be adjusted by sliding it up or down.

What Is on Your Phone? (20 minutes)

Once the video has concluded and participants have seen the level of detail that is available to (and stored by) service providers when tracking their customers, participants should be reminded about what is actually on their phone, as well. This activity can be carried out either with a single volunteer participant, or with a crowd-sourced information map.

Conducting the Exercise with a Single Participant

The trainer recruits a volunteer from among the participants and talks to this person beforehand to ensure that they're aware that they will be asked to share information about what they have on their phone. The trainer then goes through the following steps:

- Asks the participant to list everything they have on their phone and write it on the flipchart. Some examples might include:
  - Contacts.
  - Pictures.
  - Text messages.
  - Notes.
  - Emails.
  - Auto login (social networking sites: Twitter, Facebook accounts).
- Have the volunteer rate the sensitivity of each type of information on a scale of 1-5, with 1 being not sensitive at all, 5 being it could get you or someone in your network in trouble. (The trainer may wish to ask the volunteer to provide ratings for different "adversaries": What if the police had your phone? A professional competitor? Someone in your personal life?)

REMINDER:
If this module is the first in a larger course, we recommend you spend the first 10 minutes working with the group to define guidelines for behavior and security. For details, see the "Creating a Contract" section in the Guide for Trainers.

Conducting the Exercise With the Whole Group

Trainers can also do a crowd sourced version of the same exercise, and get the whole group involved. For this, the trainer:

- Explains to the group that they are going to map the information on their phones and asks them to think about "categories" of information that are stored on the phone. Some examples may include:
  - Telephony information (i.e., call records, text messages, contacts).
  - Email apps.
  - Social networking apps.
  - Media apps (video, sound and pictures).
  - Browsing apps (Google, Firefox, Safari).
- Writes categories along the top of a flipchart, or writes them on stickies on the wall.
- Divides the area (flip chart or wall) into two sections, "public"' and "private," the difference being that "public" represents information we are happy to share publicly, and "private" being for a limited audience or ourselves only.
- Distributes Post-it stickies to participants and gets them to write the types of information they store on their phone under each category. Gets them to categorize them in terms of whether they're public or private and sticks the stickies on the chart paper/wall.
- Once the map is created, asks participants to make observations about the type of information that is stored on the phone.
- Looking at the information map, the trainer then asks participants to consider the information they don't choose to put there, but which is automatically generated by the phone's functioning, such as location data, call records, phone usage statistics, etc. If they are not on the map, the trainer adds them, perhaps in a different color to distinguish them.

Drawn from "What Is on Your Phone?" available at the LevelUp website.

2. DISCUSSION (15 MINUTES)

With both portions of the Activity section completed, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion.

Trainers are welcome to add to this list or improvise as they see fit.

- Were you surprised by what you saw in the TED Talk clip? Did you learn something new?
- Spitz explained that DT, his service provider, keeps all data for at least two years. Do you know what the policies of your service provider are? How could you find out?
- Were you surprised by how many things we keep on our phones?
- Recently, there have been many news stories based on documents leaked by Edward Snowden about projects at the NSA. Do you think that the NSA is the only organization that conducts surveillance programs or do you think that all intelligence services do, or something in between?
- Since the Edward Snowden documents have been reported on, have you changed your mobile phone habits in any way? Have you changed settings in any way?
- How do you protect your phone now (both your use of the phone and the information you store on it)?
- What questions do you still have about mobile phones and privacy that you want to have answered in this class?

3. INPUT / LECTURE (30 MINUTES)

This section includes a recommended case study, key messages and some materials to help get the point across.

Trainers should feel free to add or improvise as they see fit.

Case Study

Phone Hacking in the News

Introduction: While many people have been alarmed by mobile phone surveillance among intelligence services, its use by some news organizations has muddied the issue.

Story: In September 2010, Sean Hoare, a former show-business reporter for the News of the World, revealed to the New York Times Magazine that he had been "actively encouraged" to hack into the voicemail accounts of people he was covering.

In what would turn out to be a drawn-out case involving celebrities, law enforcement, money and scandal, and ultimately lead to the shutting down of a paper, Hoare told the New York Times that a desk executive could locate information about a person's movement and locations via their mobile phone number and that the tabloid reporters were encouraged to engage in the practice regularly.

A follow-up story in the UK's Guardian quoted him as saying: "Within 15 to 30 minutes someone on the news desk would come back and say: 'Right, that's where they are.'"

Five years earlier, the tabloid had been charged with listening to voice messages of various newsworthy people, including Britain's royal family. The clue: Voice messages in recipients' mailboxes that they had not listened to yet were appearing as heard and saved. Subsequently, information that only a few people had access to was being published in the tabloid.

The UK's Metropolitan Police Service (known as Scotland Yard) got involved and indicted reporter Clive Goodman, who covered the royal family, and Glenn Mulcaire, a private investigator who was paid by the paper.

Although the police seized files from the private investigator's home containing several thousand mobile phone numbers, mobile phone PIN codes and a recording of him walking a journalist through the steps of hacking a soccer official's voice mail, they focused on the royals' case, which culminated with the imprisonment of Mulcaire and Goodman.

At the same time, however, the British police appeared to have failed to pursue leads that suggested that the abuse went beyond the royals and extended to other citizens. There was a public outcry against the paper and its owner Rupert Murdoch when in July 2011 it was revealed that the phones of a murdered schoolgirl, relatives of deceased British soldiers and victims of the July 7 London Bombings were also accessed.

Police and law enforcement agencies, reportedly, regularly use this method of tracking, where they ask mobile phone companies to provide them with real-time location information about the whereabouts of suspects or missing people at regular intervals. Police can also ask for a data dump, which can give them a complete historical record of the whereabouts of a person's cell phone and their location. There are two ways location data through mobiles is obtained:

- Details of a user's location are used when a phone is used for a call or SMS message.
- When a phone is not in use, it can be "pinged" by sending signals to the phone and triangulating the results from cell phone masts. The level of accuracy varies depending on the proximity of the masts (from a few hundred yards to a mile).

Compiled From:

- "Tabloid Hack Attack on Royals, and Beyond" (The New York Times Magazine).
- "News of the World Phone-hacking Whistleblower Found Dead" (The Guardian).

Supporting Video for the Case Study: "Sean Hoare – NoW Whistle-Blower Found Dead – Speaking About Hacking in March 2011." (NOTWPhoneHacking)

Interaction with the Participants:

This case study illustrates that mobile phones are inherently insecure. We recommend trainers use the study to encourage discussion among participants. Some questions that may help:

- Should journalists be hacking into conversations of private citizens?
- Is it different from law enforcement agencies tracking cell phone use? How?
- Can you imagine a scenario where eavesdropping would be justified by journalists? By intelligence services? By the phone company?
- How do you use your mobile phone? Would anyone be interested in your mobile phone calls? Could someone be eavesdropping on your conversations?

Talking Points for the Trainer

With the case study concluded, the trainer should now direct participants to their Class Notes.

TRAINER'S NOTE:
Text with a ✔ does not appear in the student version of the Class Notes.

1. Mobile phones are easily stolen or confiscated.
   - ✔ Article: "Mobile Phone Crime Soars" (The Daily Mail).
2. Mobile Phones are like Radios.
   - ✔ This means that they broadcast their location to cell towers and, as a result, allow owners' locations to be tracked and targeted. In early 2014, the Ukraine authorities used this ability to send warning text messages to demonstrators at a political rally that turned violent.
     - ✔ Article: "Ukraine's Opposition Says Government Stirs Violence" (The New York Times).
   - ✔ This also means that we are surrounded by thousands of phone calls in the air around us. Some people with special equipment have an opportunity to listen in.
     - ✔ Article: "Smart Trash Can Knows How Fast You Walk and Which Smartphone You Use" (TheVerge.com).
3. More and more people want to monitor us.
   - ✔ Monitoring software has now made it to ordinary consumers:
     - ✔ **Video**: Phone Tracker (YouTube). This clip for phone-track.net claims the site provides search engine service to link phone numbers with location data. We do not recommend using the service. We mention the clip as one example of the burgeoning industry of tracking services and software.
     - ✔ **Website**: "Ultimate Cell Phone Monitoring Software" (Mobistealth.com).

4. Your service provider can record "metadata":
   - Your location.
   - Calls (duration, to what number).
   - Text messages.
   - Use of Web services.
     - ✔ Article: "Spy Scandal Grows: Telekom Accused of Tracking Journalists' Mobile Phone Signals" (Spiegel Online).
     - ✔ Article: "Chinese Sell Iran £100m Surveillance System Capable of Spying on Dissidents' Phone Calls and Internet" (Daily Mail).
     - ✔ Article: "EU Company Admits Blame for Sale of Phone-snooping Gadgets to Iran" (EUobserver).
5. Handsets have unique identifiers called IMEI numbers (International Mobile Equipment Identity).
   - ✔ This number does not change even if you change your SIM card (the part of the phone where your phone number is stored).
6. Ways to be physically safer:
   - Be aware of your environment.
     - ✔ Who is standing nearby?
   - Don't show it off.
     - ✔ Don't set it on the table at a restaurant. That invites theft.
   - Decide what you need on the phone.
     - ✔ In case of theft or confiscation, the less you have on the phone, the better. It is recommended that participants make a habit of reviewing their phone's contents at least once a week.
7. Ways to be digitally safer:
   - Enable strong passwords.
     - ✔ Many people use PIN codes (usually a 4-digit sequence you need to type in order to make a call). But Android, iPhone and Blackberry all support strong passwords, which is safer. You can enable these in the phone's Settings.
   - Enable encryption.
     - ✔ A PIN or password will prevent someone from making a call on your phone, but it may not protect data you keep on the phone – especially if you use an SD card or similar memory card with the phone.
8. Things to avoid:
   - Unnecessary applications, wallpapers, ringtones.
     - ✔ These things are fun, but they can contain viruses.
   - Applications that ask for access to information they don't need.
     - ✔ An example might be an alarm clock application that wants access to your call logs.
   - Leaving Wi-Fi and Bluetooth on when not being used.
     - ✔ These not only waste your battery, they leave the phone open to potential attacks.

4. DEEPENING (80 MINUTES)

This portion of the lesson will introduce participants to some phone settings and several applications. The material below pertains to Android devices. Trainers who need information pertaining to iOS devices (iPhone or iPad) will find that information in the iOS Devices handout.

Due to the number of applications introduced, trainers may find that 90 minutes is insufficient time to cover them all. With that in mind, we suggest that trainers give the highest priority to the communication applications TextSecure and ChatSecure.

NOTE: *Participants should prepare an account for these exercises prior to class. Any of the following will do: Facebook chat, Gchat (Google), VKontakte, Yandex, Hyves, Odnoklassniki, StudiVZ, LiveJournal, Jabber and Apple's Bonjour (ZeroConf).*

PART I: System Settings

The first portion of Deepening will be fairly quick. The trainer will walk participants through the steps to enable a locking mechanism and encryption on the phone and (if applicable) on an additional SD card.

Overview: Trainers may wish to read this short article at Ghacks prior to the class to familiarize themselves with features and their purpose: "Encrypt All Data on Your Android Phone."

NOTE: *We suggest that trainers demonstrate each exercise twice before asking participants to follow, and that they allow every participant to complete one task before moving on to the next.*

Exercise #1: Enable Locking with Long Passwords on Android

1. Go to Settings → Security → Screenlock.
2. Choose "Password."
3. Set a password.

Material that may be Useful:

- **Guide:** "Creating Strong Passwords" (Security in-a-box).
- **Video**: "Enabling or Changing Screenlock." Note: This clip refers to the Samsung 4G. The steps are accurate across Android devices. However, there may be cosmetic differences on other devices.

Exercise #2: Turn On Encryption for the Phone

1. Go to Settings → Security → Encryption.
2. Select "Encrypt phone."

ALERT: The encryption process can be lengthy and, in some cases, manufacturers require that the phone be plugged into a power source before the process can begin. For this reason, we suggest only showing participants how to enable the feature, rather than trying to complete the encryption task. If training on security topics across several days, trainers can assign the encryption task as homework. Also, it is important that participants understand that, even though Android devices are designed to back up almost all of a user's data when paired with a Google account, this doesn't mean that all of the data on a device is backed up, particularly photos, email drafts, and users' other third-party application data. **We recommend that users back up anything they value before encrypting their device that isn't already automatically backed up to their Google account.** For most users this is primarily photos, but it may involve more data.

SOFTWARE & INSTALLATION*:

- TextSecure.
  - Guide.
- ChatSecure.
  - Guide.**
- Orbot.
  - Guide.
- Orweb.
  - Guide.

* These must be downloaded from the Google Play store directly to the participants' phones. Trainers may wish to recommend that participants pre-install these applications prior to attending class to avoid delays.

** ChatSecure is the new name for Gibberbot. This installation guide from Security in-a-box reflects the old name. However, the principles described remain valid.

Exercise #3. Turn on Encryption for an SD Card

1. Go to Settings → Security → Encrypt SD Card.
2. Choose "Enable."

NOTE: *The same considerations apply in this exercise as for Exercise #2 (above).*

Material that may be helpful:

- **Video**: "How to Encrypt Files on your SD Card using your Android Phone" (YouTube: Howik.com).

PART II: Applications

Overview: The following applications are designed to provide secure SMS text messaging, secure chatting (with one other person) and improved privacy when browsing the Web.

A. TextSecure

TextSecure is a free, open-source application that encrypts the contents of SMS messages between phones that have it installed, and also stores SMS messages in a password-protected database.

Installation and Demonstration of TextSecure

- Walk-through: "Text Secure for Android Devices" (Security in-a-box).

Exercise

Establishing and Testing

- This exercise follows a walk-through provided by Security in-a-box and asks participants to authenticate the identities of one another's devices before sending each other test text messages.
- The trainer should ask participants to pair off into two-person teams.
- Reviewing the walk-through provided by Security in-a-box, participants should add the phone number of their partner and then initiate a secure session.
- Once partners have exchanged keys, they can test the system by sending a test message to one another. This additional walk-through from Security in-a-box may help. It is important that participants confirm that the **padlock icon** has appeared on their Send button. Otherwise, their text will not be protected.

Partners can end their secure session.

Key Messages

While participants conduct this exercise, the trainer should emphasize the following:

- If the padlock icon is not visible on the Send button during an SMS session, the text will not be protected.
- While TextSecure encrypts the contents of SMS messages, it does not encrypt other information related to those messages, such as the sender or receiver or the day/time the message was sent.
- TextSecure is only intended to encrypt SMS messages and it does not provide protection for any other type of communication on your phone.

B. ChatSecure

Until very recently, ChatSecure was called Gibberbot and some of the materials we reference still call it that. ChatSecure is a chat application that lets two people "authenticate" the identity of the other and lets them encrypt their chats between their phones using popular services such as GTalk or Facebook Chat. An encrypted chat is one that the phone's service provider cannot read.

Installation and Demonstration of ChatSecure

- Walk-through: "How to Chat Securely" (The Guardian Project).

  NOTE: *As of October 2013 screens in this walk-through describe "Gibberbot," the predecessor to ChatSecure. The instructions remain the same for ChatSecure. However, the appearance of the screens may initially confuse some participants. It is best to alert them that some of the screens are temporarily outdated.*

Exercise

Exchanging Authentication Keys:

- Prior to starting the exercise, participants add one chat account to the ChatSecure application.
- Participants pair off into two-person teams.
- Reviewing the walk-through provided by The Guardian Project, participants exchange 1) usernames, and 2) authentication information that is necessary to establish a protected chat with one another.

  NOTE: *The Guardian Project walk-through suggests exchanging this information via a "trusted channel" online. Because participants in this class will be in the same room, it is worth pointing out that in-person exchange is always the most secure method for sharing information. However, other channels (any channel that is not the ChatSecure application itself) may be the only alternatives when it is impossible to meet in person.*
- Participants should begin a chat with their partner using the insecure mode (default). They should note the indicator at the top of the screen that shows the chat is not secure.
- Participants should then attempt to switch to secure mode. They will be asked to authenticate one another and should follow the on-screen steps.
- Once secure chat has been established, teams should split up and repeat these steps with someone else in the class. Goal: To "collect" authentication for secure chat with all other participants.

Key Messages

While participants conduct the exercises to validate one another and conduct chats, the trainer may wish to remind them that:

- ChatSecure is intended to protect chats between two people using the ChatSecure application. It does not protect anything else or any other applications on the phone. It does not protect, for example, your SMS messages (i.e., "texts"), which are plainly visible to your service provider.
- ChatSecure can run over the Tor anonymity network, and the next exercise will introduce Orbot, which provides access to that network. Trainers who are unfamiliar with Tor (The Onion Router) can read more about the network at the developer's website.

C. Orbot

Orbot is the Android version of Tor (The Onion Router) and allows you to use the Tor anonymizing network. When using Tor, one does not connect directly to a website. Instead, the user connects securely to three other computers in a chain – each one only knowing the identity of the computer immediately "in front" and "behind" it. Connections between each computer in this network are are encrypted. As a result, the Tor network can provide a high level of anonymity to its users:

1. The websites that people visit through Tor do not see the true location of the user. Instead, they see the location of the last computer in the network that the user reached.
2. The Tor network computers do not know what website *you* are visiting, only that someone is visiting a particular website.

Installation and Demonstration of Orbot & Orweb

This walk-through illustrates how to install and launch the Orbot application (which connects to the Tor anonymizing network) and then the Orweb browser (which uses that network).

Walk-through: Using Orbot & Orweb to browse freely (Guardian Project).

NOTE: *Some of the slides in this walk-through contain animations that are delayed. You may find that, on some pages, it takes several seconds before the "Next" button (for navigation) appears.*

Exercise

Confirming a Secure Connection

In this exercise, participants will confirm that their phone's data connection is going through Orbot (the Tor network):

- Launch Orbot and wait until a connection is obtained.
- Launch the Orweb Web browser and wait for the message from the Tor network that confirms (or denies) that a Tor connection has been established.
- Open the Orweb Web browser and navigate to the following URL: whatismyipaddress.com.
- Participants should make a note of the address that is displayed.
- Participants should repeat these steps. However, they should use their regular browser – not Orweb.
- Participants make note of the location that is displayed at whatismyipaddress.com. As they will not be using the Tor network, they should see their actual location reflected.
- Participants should repeat these steps until they feel comfortable with them. It is recommended that they locate the icons related to these applications somewhere they can access reliably.

For additional ideas and activities, visit the LevelUp website.

Key Messages

While participants conduct the exercise to confirm their secure connection, the trainer may wish to remind them that:

- Orbot (and the Tor network) only provide protection for Web browsing. They do not automatically protect anything else you might do.

5. SYNTHESIS (15 MINUTES)

In other modules, we recommend using this time to wrap up the material that has been covered. In this case, however, we have a suggestion for a five-minute exercise that we think will also serve the purpose of review:

Personal Security Plan

The trainer asks participants to form teams of two. Each team should spend five minutes drafting notes that they can use as a personal safety plan. This guideline may help them put their plan onto paper:

- Phone calls. (How will they handle phone calls? Sample answer: "If someone from my office contacts me about something sensitive and I am standing on a crowded train, I may postpone the call until I reach my destination and can be more private.")
- Text Messages.
- Applications:
    - Apps to delete (e.g., "I will delete the 'Map my location' app.").
    - Apps to use with caution.
    - Apps to actively use.

After five minutes, the trainer asks participants to come back to the same circle they formed during the Discussion section and asks each team to report back to the group on what they concluded as possible strategies.

MAC OS X: MOBILE PHONE SAFETY

The following material includes applications and exercises that may be useful to participants with Mac OS X and iOS devices. Trainers working in pairs may wish to divide their efforts during Deepening exercises, with one trainer working with Windows/Android users and one trainer working with OS X/iOS users.

Software & Installation

- TextSecure (still in development).
  - Request notification when stable release is available.
- ChatSecure.
  - Support.

NOTE: *If you are training users on the iOS version of ChatSecure, we suggest installing it beforehand to become familiar with it, or having a co-trainer do so. Once installed, ChatScure on iOS will behave as it does on Android.*

Deepening

PART I: System Settings – iOS Devices (iPhones or iPads)

The first portion of Deepening will be fairly quick, especially since encryption is already turned on by default for iOS devices starting with iOS 4. However, there are some limitations to the feature.

Exercises #1 & #2: Enable Locking With Long Passwords on iOS

- iOS offers a four-digit passcode by default (called a "simple passcode"), which is better than none at all, but we strongly recommend using a longer alphanumeric passcode!

To set a "simple passcode" of four digits:

- Go to Settings → General → Passcode
- Follow the prompts to create a four-digit passcode.

To set a stronger passphrase for your device **(recommended)**:

- On the same screen, disable "simple passcode," then follow the prompts to enter a longer alphanumeric passcode. The longer and more complex that you can remember the better! Refer to Security in-a-box "Elements of a Strong Password" for tips.

After setting a passcode: Set "Require Passcode" to "Immediately" in order to quickly auto-lock your device after it's been idle.

Key Messages

- Apple provides encryption ("data protection") on devices running iOS 4 or later, and on iPhone devices 3GS and later. However, users must have a passcode to use the built-in encryption feature.
- Unlike Android's built-in, full-disk encryption feature, Apple's "data protection" is technically not full-disk encryption, which means not everything on the device may be encrypted even if you have "data protection" on. This is because third-party developers have to enable their apps to work with Apple's encryption system. Therefore, if users have a passcode that enables data protection, all of Apple's apps and those app's data will be encrypted, but there is no guarantee that apps from non-Apple developers or the data associated with them will be encrypted. Often, it is nearly impossible to tell whether third-party app developers have designed their apps to use iOS's built-in encryption feature or not, especially if they are not

open source, which most are not. This is useful to share with participants in case users depend heavily on a third-party app to manage and/or store sensitive data on their devices.

Exercise for Mac Only: Enable Erase Data Feature

- iOS also offers a feature to erase all the data on your device after 10 failed attempts to unlock it. We recommend that users turn this feature on. While it will not prevent advanced attacks by well-resourced adversaries who have unlimited time and uninterrupted access to a device, it will prevent most attacks and attempts to access the device in short periods of time (e.g., when a device is temporarily left unattended and an adversary tries to quickly access it).

To enable the feature:

- Go to Settings → Security → Encryption.
- Enable "Erase Data."

Material that may be useful:

- Guide: "Elements of a Strong Password" (Security in-a-box).

NOTES

- Mobile phones are easily stolen or confiscated.
- Mobile phones are radios and always broadcasting.
- More and more people want to monitor us.
- Your service provider can record "metadata":
  - Your location.
  - Calls (duration, to what number).
  - Text messages.
  - Use of Web services.
- Handsets have unique identifiers called IMEI (International Mobile Equipment Identity) numbers.
- Ways to be physically safer:
  - Be aware of your environment.
  - Don't show it off.
  - Decide what you need on the phone.
- Ways to be digitally safer:
  - Enable strong passwords.
  - Enable encryption.
- Things to avoid:
  - Unnecessary applications, wallpapers, ringtones.
  - Applications that ask for access to information they don't need.
  - Leaving Wi-Fi and Bluetooth on when not being used.

For Further Learning:

- "Surveillance Self-Defense: Mobile Devices" (EFF.org).
- "Safer Cellphones" (SpeakSafe).

GLOSSARY

The following definitions of technical terms are provided under the Creative Commons Attribution-Share Alike 3.0 Unported License and feature entries created by the Tactical Technology Collective, Front Line Defenders and Internews.

Vocabulary words related to this module's topic:

Avast! – A freeware anti-virus tool.

Bluetooth – A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions.

circumvention – The act of bypassing Internet filters to access blocked websites and other Internet services.

encryption – A way of using mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

email client – An application installed on a PC or mobile device that organizes email and allows users to read and write messages offline. Popular examples include Microsoft's Outlook and Mozilla's Thunderbird.

firewall – A tool that protects your computer from untrusted connections to or from local networks and the Internet.

free and open source software (FOSS) – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

hacker – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

IMEI – International Mobile Equipment Identity. This is a unique identification number for a mobile phone's handset and is separate from a customer's phone number, which is contained in the SIM card. The IMEI number is sometimes used by service providers to block devices that have been reported as stolen.

malware – A general term for all malicious software, including viruses, spyware, Trojans, and other such threats.

metadata – Information related to digital communications and media that may not be visible to the user, but may contain identifying details. For instance, phone calls may include the date and time of a call, a photograph may contain the location where a picture was taken or the model of camera used. A document may contain the name of the PC that created it.

proxy – An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy.

service provider – A company, either private or public, that provides mobile phone service or Internet service to customers.

SIM card – A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.

Tor – The Onion Router is an anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you visit from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites.

two-step verification – A method of protecting a Web account that requires the user to provide two kinds of information when signing in, instead of just one password.

VPN – A virtual private network. VPNs use software on a PC or mobile device to create an encrypted connection with a server on the Internet. VPNs do not provide anonymity and users' online activity is visible to the VPN service provider.

QUICK START:

TIPS FOR SECURING YOUR SMARTPHONE

Mobile phones are attractive targets for thieves and others. They contain call logs, contact lists, photos and other sensitive data. In addition to keeping your phone with you at all times, here are some common recommendations to get you started in making your mobile phone or smartphone more secure:

- **Lock it with a strong password:** Make sure your phone is locked with a PIN code -- or much better, a passphrase. In both Android and iOS, you can enable screen locking and passwords in your device's Security settings. iOS users can also instruct their phones to automatically delete all data after a certain number of incorrect unlock attempts.

  For recommendations on strong passwords, see "Elements of a Strong Password" at the Security-in-a-box website.

- **Delete sensitive information:** Phones are easily lost, stolen or confiscated, so avoid keeping sensitive data on one:
  - Take inventory of the data on your device. What do you actually need?
  - If you must keep sensitive data on the phone, consider transferring it from the phone's memory or SIM card to a separate SD card that can be more easily removed or destroyed.
  - Visit your manufacturer's website for instructions on securely deleting data from your phone before you re-sell it.

  For additional information, see "How to Use Mobile Phones as Securely as Possible" at the Security in-a-box website.

- **Encrypt what you keep:** Today's smartphones can protect files and other information we store on them with encryption – a way of encoding the information so that it can't be read without the correct password. Examine the security settings of your device to enable this feature and, remember, it is always a good idea to back up your phone's data before you begin encrypting to avoid accidentally losing it if an accident occurs.

- **Use privacy software:** Android users can download free, open-source applications to add privacy to their chat sessions and Web browsing. Learn more about these applications at Security in-a-box:
  - TextSecure: Private SMS text messages.
  - ChatSecure: Private chat messages.
  - Orbot: Anonymizing network.
  - Orweb: Anonymizing browser.

For Further Learning

- "How to Use Mobile Phones as Securely as Possible" (Security in-a-box).
- "How to Use Smartphones as Securely as Possible" (Security in-a-box).

NOTE: This supplement is not a replacement for in-person training or a thorough online resource, both of which offer more detailed information.

QUICK START:

TIPS FOR SECURING YOUR PC AND ONLINE ACCOUNTS

A clean and protected PC is fundamental to your digital privacy. If your PC is infected with a virus or if it doesn't take advantage of some common safety features, other efforts to protect your data may be undone.

Here are some common recommendations to get you started in making your PC and online accounts more secure:

- **Get an anti-virus application:** An anti-virus application protects against malware – malicious software – that can damage your PC or give someone remote access to your files. If you already have an anti-virus application, make sure it's genuine. One free anti-virus that scores well in tests alongside paid anti-virus applications is Avast!.

  For more recommendations, see this "How to Protect Your Computer from Malware and Hackers" at the Security in-a-box website.

- **Update everything:** Your anti-virus application needs to be updated frequently to keep it current with new viruses and other exploits. Most antivirus applications allow you to stay updated automatically, but some require manual updating. Take five minutes to see which method is available for your anti-virus application and confirm that your application is up-to-date. Similarly, learn how to update your other applications – A free utility like Secunia PSI can help.

  For further information, see "Keeping Your Software Up-to-Date" at the Security in-a-box website.

- **Enable Automatic Updates:** In Windows, visit the Control Panel and type "Windows Update" and select "Turn automatic updating on or off." Confirm that your PC is set to receive automatic updates. In Mac OS X, find your App Store preferences (Apple menu → System Preferences → App Store) and confirm that you are set to install system data files and security updates.

- **Make sure your PC's firewall is on:** Both Windows and Apple PCs have built-in firewalls – software that tells your PC to ignore Internet connections you didn't request. To confirm that your firewall is turned on in Windows, visit the Control Panel and type "Windows Firewall" and then click on the link to check your status. In Mac OS X, click the Apple menu icon to access your Security preferences, and then look for your Firewall status.

- **Use strong passwords:** Passwords that are short or easy to guess (e.g., "passw0rd") don't offer much protection for your PC or your online accounts. Follow these guidelines to improve your password strength:
  - Make it long – if you do only one thing to increase the strength of your passwords, do this.
  - Don't make it personal.
  - Avoid using the same password for more than one account.

  For more password tips, see "How to Create and Maintain Secure Passwords" at the Security in-a-box website.

- **Encrypt everything:** Encryption programs let you lock up the files on your PC with a password so that someone else can't read them. If you don't already encrypt your files, you may want to consider using the free utility called TrueCrypt.

  For more information, see "How to Protect the Sensitive Files on Your Computer" at the Security in-a-box website.

NOTE: This supplement is not a replacement for in-person training or a thorough online resource, both of which offer more detailed information.

- **Protect accounts with two-step verification:** Two-step verification, used with a strong password, can make it very difficult for someone to access your online accounts. When you configure one of your accounts to use this feature, it means that you will need to provide both a password and a second piece of information, like a code sent your mobile phone. Several popular sites now support this feature:
  - Dropbox.
  - Facebook.
  - Google.
  - Microsoft.
  - Twitter.
  - Yahoo!.

- **Think first:**
  - Only download software **directly from a developer's website**, or from a site that tests for malware, such as FileHippo or Softpedia.
  - **Don't click on links in email.** If you want to visit an address someone has sent, copy and paste the link into your browser, or re-retype it.
  - **Don't open an attachment in email** unless you know the person who sent it. You can always scan an attachment with your antivirus application before you open it, or you can open the attachment in Google Drive.
  - **Don't install pirated software.** It may be cheap, but it can come with extras you don't want, like computer viruses.

About Internews

Internews is an international non-profit organization whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect and the means to make their voices heard.

Internews provides communities the resources to produce local news and information with integrity and independence. With global expertise and reach, Internews trains both media professionals and citizen journalists, introduces innovative media solutions, increases coverage of vital issues and helps establish policies needed for open access to information.

Internews programs create platforms for dialogue and enable informed debate, which bring about social and economic progress.

Internews' commitment to research and evaluation creates effective and sustainable programs, even in the most challenging environments.

Formed in 1982, Internews is a 501(c)(3) organization headquartered in California. Internews has worked in more than 75 countries, and currently has offices in Africa, Asia, Europe, the Middle East, Latin America and North America.

INTERNEWS WASHINGTON, DC OFFICE
1640 Rhode Island Ave. NW Suite 700
Washington, DC 20036 USA
+ 1 202 833 5740

INTERNEWS ADMINISTRATIVE HEADQUARTERS
PO Box 4448
Arcata, CA 95518 USA
+1 707 826 2030

www.internews.org
E-mail: info@internews.org
Twitter: @internews
facebook.com/internews

Internews
Local voices. Global change.