

---

# **The Field Guide to Security Training in the Newsroom Documentation**

*Release 1.0.1*

**OpenNewsLabs**

**May 26, 2018**



---

## About This Guide

---

<b>1</b>	<b>About This Guide</b>	<b>3</b>
<b>2</b>	<b>Contributing</b>	<b>5</b>
<b>3</b>	<b>Authors</b>	<b>9</b>
<b>4</b>	<b>License</b>	<b>11</b>
<b>5</b>	<b>Chapter 1 - Being A Better Trainer</b>	<b>13</b>
<b>6</b>	<b>Chapter 2 - Lesson Plans</b>	<b>27</b>
<b>7</b>	<b>Chapter 3 - Resources</b>	<b>95</b>



In the weeks following the 2016 presidential election, daily downloads of Signal increased four-fold. Though the US Border Patrol has had the authority to search electronic devices at border crossings for almost a decade, they seem to be using that authority more often in recent months. With the inauguration of a president who is openly hostile to the press (whose own campaign benefited immeasurably when hackers released his opponent's private correspondence), reporters on all kinds of beats have started to ask how to protect their digital data from snoops of all stripes. Often there isn't anyone nearby who can offer solid, informed answers to those questions.

Often the person reporters turn to for help has to come up with smart answers on the fly. They're the one developer who uses GPG, or the reporter who's been trying to convince everyone else to install Signal — and now they're suddenly pressed into service as the newsroom security expert. Or they're the IT staffer tasked with keeping the mail servers running, only now they're also the in-house opsec consultant who doesn't have any formal training in what reporters and editors need.

We want to see a whole lot more people prepared to answer those questions and help newsrooms do a better job of communicating (and storing data) securely. BuzzFeed Open Lab and OpenNews teamed up to assemble a solid, thoughtful series of training modules and resource guides that folks can use to help colleagues step up their security literacy. We'd like to cover everything from how to explain why migrating to a password manager is worth the trouble, to how to convince whoever needs convincing that installing Secure Drop is worth the trouble.



# CHAPTER 1

---

## About This Guide

---

This resource collects the advice and experience of journalists, newsroom developers, and security experts, organized into a set of lessons and training materials available for newsroom staff who find themselves leading security trainings. In a moment when reporters are asking how to protect themselves and their sources, we want to see more people armed to answer those questions and help newsrooms communicate and store data more securely.

The curriculum is hosted by [OpenNews](#), a team that helps developers, designers, and data analysts convene and collaborate on open journalism projects, and [BuzzFeed Open Lab](#), an arts and technology fellowship program at BuzzFeed News. The first draft began during a two-day event in June 2017, with about 20 people working in-person and remote.





The Newsroom Security Curriculum is a collaborative project. It gets better every time anyone from the journalism, tech, and security communities shares advice, writes up an experience, asks a question, or even just spots a typo. We'd love to add your voice to this project.

## 2.1 Who should contribute

This project actively encourages contributions from people of all genders and statuses, races, ethnicities, ages, creeds, nationalities, persuasions, alignments, sizes, shapes, and journalistic affiliations. You are welcome here. By participating in this project, you are agreeing to abide by its *code of conduct*.

The curriculum also benefits from contributors of all skill levels. Sharing a resource that helped you understand something for the first time is awesome. Telling everyone about a training game your colleagues loved is awesome, too. And so is just asking a question, as you think about how your newsroom can better protect its journalists and sources.

If you're wondering what you might be able to offer this project, here are a few questions to get you started:

- Could you read through a lesson plan and tell us what seems helpful and what's confusing?
- Could you write up a case study about a security situation you've run into?
- Could you describe the cultural roadblocks you've run into trying to bring more security to your newsroom, and how you've pushed through them?
- Could you help add checklists at the ends of lessons?
- Could you describe how security needs might be different in different countries, or work on translating documentation into another language?

Even just adding a quick link or two is a great way to contribute. If you've got a timely article or an old favorite that really captures the value of taking a lesson seriously, those add fantastic context. We don't want to duplicate work that other people have done better already, and we recognize that this is just one of many great resources. So if you know of a great lesson plan or walkthrough somewhere else, there's a section in each lesson for links, and [our resource guide](#) is an excellent spot for links that don't fit a specific lesson. Share your favorites.

And one more way to help us make this project even better:

- Try out one of these lesson plans and let us know how it goes!

More than anything, we want this curriculum to be useful to people as they help their colleagues get better at security. We'd love to hear how well these lessons work in *your* newsroom, and what we can do to improve them.

## 2.2 Where to start

The documentation in this guidebook lives in a [GitHub repository](#), where we love to see comments, issues, and pull requests. If you're interested in contributing but you're not sure where to start, we have a [list of open issues](#)—pick one and dive in!

## 2.3 How to contribute

If you'd like to submit an update to this guidebook, first of all, thank you! If your changes could use some editorial consideration, please [open an issue on GitHub](#) so there's an easy place to have that conversation. Or if you're tackling [an existing issue](#), please leave a comment on the issue to let people know—that way someone else won't end up duplicating your effort.

If you're comfortable using git and GitHub, you should feel free to submit changes by cloning this project and [opening a pull request](#). (And when you do, we'd love it if you'd add yourself to the [AUTHORS list](#) as well.) If you're not used to git, we're also very happy to receive comments and updates at [fieldguide@opennews.org](mailto:fieldguide@opennews.org).

## 2.4 Localization

The first draft of this resource is largely designed for U.S. and Canadian newsrooms. We'd love to introduce similar lessons for journalists in other countries, but we understand that it's not as simple as translating existing material into different languages. If you're familiar with the laws and expectations involved in keeping journalism secure in a country outside our area of expertise, [we'd love to have your help](#).

## 2.5 Our process

This documentation is released under the [MIT license](#), so by submitting an update, you're agreeing to share your changes under this license as well. We may edit your work for style and consistency with the rest of the guidebook, or offer feedback about anything that might need to be revised.

When we merge your changes, this project will acknowledge you in the [AUTHORS list](#), and the Field Guide to Open Source in the Newsroom will just have gotten significantly better.

## 2.6 Code of conduct

OpenNews is committed to providing a welcoming and harassment-free environment. This project exists in a public space, so we think it's particularly important to identify our principles in creating a supportive community.

Participants in this project agree to:

- Be considerate in speech and actions, and actively acknowledge and respect the boundaries of fellow contributors.

- Refrain from demeaning, discriminatory, or harassing behavior and speech. Harassment includes, but is not limited to: deliberate intimidation; sustained or willful disruption of conversations or other work; use of sexual or discriminatory imagery, comments, or jokes; and unwelcome sexual attention.
- Be welcoming, friendly, patient, and kind. Ask questions. In disagreement or critique, explain why you feel the way you do, and recognize that other contributors also make decisions with good intentions and the best information available to them.

If anyone violates this code of conduct, project coordinators may take any action we deem appropriate, including but not limited to warning the participant or banning them from contribution.

Instances of abuse, harassment, or other unacceptable behavior may be reported by emailing [info@opennews.org](mailto:info@opennews.org), an address that reaches all OpenNews staff members.

## 2.7 Attribution

Language on welcoming all communities adapted from the [agate project](#). Code of conduct adapted from [SRCCON](#) and [INN](#).



## CHAPTER 3

---

### Authors

---

This resource began with a convening in Chicago where a dozen committed folks dedicated several days to writing the first draft. More folks stepped in to edit those drafts and offer feedback on them, or submit new lesson plans or workshop materials. This curriculum wouldn't exist without their hard work:

- Alan Palazzolo
- Amanda Hickman
- Blaine Cook
- Carol Waters
- Dan Sinker
- Eliot Stempf
- Emma Carew Grovum
- Erik Reyna
- Freddy Martinez
- Harlo Holmes
- Jason Reich
- Jennifer Henrichsen
- Kevin O'Gorman
- Lindsay Beck
- Lo Benichou
- Mago Torres
- Mariel García-Montes
- Martin Shelton
- Matt Perry

- Mike Tigas
- Norman Shamas
- Quinn Norton
- Rodney Gibbs
- Ryan Pitts
- Ted Han

## CHAPTER 4

---

### License

---

The MIT License (MIT)

Copyright (c) 2017 OpenNews, BuzzFeed Open Lab

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.





---

## Chapter 1 - Being A Better Trainer

---

We've organized this guide into three key sections. Chapter 1 is a resource for new trainers, or folks who are looking for ways to be better at training in general. We've written this with a newsroom audience in mind, and we've pooled a lot of valuable resources that already exist in the world.

### 5.1 Being a Better Trainer

It takes more than technical knowledge to be a great trainer. If you're convening 4-5 colleagues for a quick brown bag, you may not need to think too deeply about the training space you create.

There are some basic steps you can take to ensure a successful, effective training.

#### 5.1.1 Before: Plan Ahead

The time and effort that goes into preparing for a workshop can make a big difference in everyone's experience.

- Use a pre-survey to gauge the group's needs if you don't already know them well.
- Send out reminders a week before the workshop, a day before the workshop and (if you're convening colleagues in the office) an hour before the workshop. Every reminder should include everything you want participants to know, bring, or do to prepare.
  - Does everyone know exactly what to bring? Will they need a laptop? A phone?
  - Should participants do any pre-reading? A couple of recent news stories that give context to the material are always helpful.
  - Do participants need to download or install anything? Avoid a bandwidth fiasco by having everyone at least complete any downloads before you gather.
  - If your plans call for participants to install software in the session, make sure they all have the ability to actually do so – check with the organization's IT department beforehand if necessary.
  - Every email reminder should include everything that participants need, even if you've sent it all before. Don't make folks dredge up an old email to remember where to go or how to prepare.

- Consider offering office hours ahead of time, especially if you need folks to complete an installation.
- If you're planning a software walk-through, even if you've done 100 times, do it one more time on the machine you'll be presenting from. You'd be surprised how often a new version of something thoroughly scrambles your plans.
- Don't be afraid of a slide deck. Powerpoint probably deserves its **bad rap**, but that doesn't mean you can't create a slide deck that adds context and visual aids.

### 5.1.2 During: Run a Smooth Session

There are lots of great resources in the introduction that can help you facilitate a session that helps participants grow instead of alienating them. Here are few tips that will help you make the most of training time:

- When someone asks a question, repeating it back to the group is a great way to make sure that everyone hears the question. Plus, the practice helps make sure that you didn't misunderstand the question.
- There are no stupid questions! It's the golden rule of training. For every "stupid" question that someone asks out loud, there are three more people who are kind of wondering the same thing but afraid of sounding dumb. So encourage participants to ask questions, even questions that they think might be kind of dumb.
- Know what you don't know. If you've put yourself forward as an expert, it's easy to think you have to have an answer to every question. If you don't know the answer, you can say you don't know and promise to follow up with an answer.
- Watch out for rabbit holes – you almost never want to try to solve a new problem on the fly in front of an audience. Especially if you're already nervous but even if you aren't, if you don't know the fix off the top of your head, table it. Set aside a place – it might be a board, it might be your notebook, to log questions that you've punted during the training. Do come back to them later (see "After," below), but don't make the rest of the room sit through a lot of troubleshooting.
- It's okay to be nervous. Take a deep breath, make sure you have water handy, and you'll do fine.

If the group is larger than your own newsroom, definitely establish a code of conduct and some ground rules about photos and **quoting folks**.

### 5.1.3 After: Follow Up!

- Send everyone a "Thank You" note within a few days. It should probably include:
  - Next steps. If everyone left with a lot of good intentions, a short list of action items will help them make good on those intentions.
  - If you set aside any questions during the session, capture them in the follow up email. If you've figured out the answer, share it. If you haven't, just say so: "I haven't had a chance to take a closer look at this one." Follow up on any questions you promised to come back to.
  - Links to any sites that you mentioned.
  - A copy of your slide deck or handouts, so folks can refer back to it.
  - A repeat of any instructions you followed (or a link to them).
- Review and revise your session plan within a day or two of the session. Look back over your plan and update it to reflect what actually worked in the session. Make any notes you wish you'd had handy this time, while those thoughts are still fresh in your mind.
- Mark your calendar: if you gave participants any next steps, or even if you didn't, follow up with everyone a week or two later to check in about whether they took any action, how it went, where they got stuck.

### 5.1.4 Getting Better

If you're ready to start improving your skills as a trainer, there are some fantastic resources that can help you out. Some of our favorites include:

- Do you need to read about something to understand it? Or would you rather play with it with your own two hands? Not everyone learns the same way, and [Level Up's guide to adult learning](#) will help you think about lessons that work for different learning styles.
- Level Up's guide to [Creating Safe Spaces](#) is also an excellent resource to get you thinking about making everyone welcome in your workshops.
- Integrated Security maintains a number of guides that cover [facilitation](#), [learning styles](#) and [creating safe spaces](#).
- Aorta is a fantastic collective that does among other things, great work training facilitators and trainers. They publish a number of excellent [resources](#) including a guide to [Anti-oppressive Facilitation for Democratic Process](#). Their guide is geared more towards group decision making, but it is still a fantastic resource for trainers.
- Aspiration facilitates nonprofit technology convenings and they work hard to create collaborative and rewarding workshops. Their [facilitation guidelines](#) and [workshop design advice](#) are both worth checking out.
- Open News led the process of creating the curriculum resource you're reading right now. Their [SRCCON facilitation guide](#) is great, as is their roundup of [OpenNews posts on session design](#).

## 5.2 Organizational Self-Assessment

These questions should help you build a better understanding of how your organization approaches security already. They also make a good starting point for a best practices list.

### 5.2.1 How to use the information you collect

- Tailor your recommendations for best practices (especially as they relate to newsroom-wide policies or changes to infrastructure). In many news organizations, you'll find that the IT side and the newsroom side aren't communicating with each other on these topics. This training and these conversations are a great way to help an organization get started.
- Help select lessons and training modules to use from this curriculum.
- Share a summary of your findings with the key stakeholders (both on the IT side and the newsroom leadership) so they can create benchmarks and track progress over time.

### 5.2.2 Questions for IT

As a general rule, you want to work with, not against, internal IT policies. So if the newsroom enforces password updates every six months, that's cool.

- Do staff use company-issued mobile phones?
  - Do you have remote wipe access on staff phones?
  - Do you distribute recommendations or requirements for mobile phone security? (Ask for a copy!)
- How do you manage newsroom laptop and desktop computers?
  - Do you enforce software and operating system updates?
- Do you provide remote access to your internal network? If so, how?

- Is device storage encrypted by default on internally provided computers? If not, are there policies or technical issues preventing this?
- How often do employees have to update their passwords? And how complicated are your password requirements?
  - Do you have a preferred password manager?
  - Do you require multi-factor authentication for email, CMS, and/or server access?
  - Do you use single sign-on (SSO) for unified login to externally-hosted services?
- Do you have a data-retention policy for when an employee leaves the company?
- Do you have a corporate policy with respect to use of cloud services? Are any explicitly encouraged? Forbidden?
- How often do you review third-party tools and TOS for security (i.e.: Slack deletion, multi-factor authentication, data retention, etc. in contracts)
- Where is your server infrastructure? On-site, in a data center, cloud?
- Do you have an incident response plan in place in the event of a DDOS attack or email system hack?
  - Have you communicated that plan to newsroom management?
  - Does that plan include post-mortem review?

### 5.2.3 Questions for newsroom leadership

- Do you use collaborative document editing and storage services (eg. Google Drive, Dropbox, Trello, Evernote)?
  - Do you have a policy about whether or not to store “sensitive” information in these services?
- Do you discuss information security as a newsroom?
- Does your newsroom currently have recommendations for secure communications (i.e.: protonmail, signal, etc)
- Are there reporters or teams that require a higher degree of security when dealing with sources than others?
- **BEST PRACTICE:** Does the newsroom regularly meet with someone from technology regarding infrastructure maintenance (password maintenance, shared accounts, where to store sensitive information, which collaborative document storage is preferred by the company, review incident response plan for high level sitewide issues)
- Are there legal issues or concerns with the implementation of a set of defined security best practices?
- Do you have recommendations or policies for secure communications with freelancers (i.e.: sourcing, payments, SSN for finance team, etc.)
- Does your newsroom and technology team have a workflow for incident response (hacking, doxxing, etc)
- What are your policies with regard to anonymous sourcing and have those policies been updated to include technological concerns?

### 5.2.4 Questions for reporters and editors

- What tools and techniques have you already tried?
- What have you been meaning to try? And what has stopped you?
- Are there tools or techniques you’d like to use but can’t because of internal editorial policies or internal IT policies?
- Have specific incidents prompted you to seek out additional tools and/or training?

## 5.3 Framing the Conversation

### 5.3.1 Overview

Many of the lesson plans in this guide are designed to stand alone, and some of the overview lessons can cover a few key topics in a lunch hour. But if you're thinking about launching a series of workshops, it is worth considering how you want to frame that series.

There are a lot of different ways to frame a conversation about digital security. Many trainers like to start with a review of basic digital literacy, to provide a foundation for subsequent trainings. Others start with threat modeling or risk assessment. This document is a great roundup of places to start a training series.

- For some participants, this workshop will be their first opportunity to reflect on a subject that is conventionally framed as the domain of experts. Facilitating means showing that participants, too, have what they need to participate in the process.
- No workshop starts from scratch. Everyone in the room brings some insight and some baggage. Participants will have useful digital security knowledge, but they also bring personal insecurities and myths that take time to debunk.
- Adults usually expect to understand the relevance of what we learn. That expectation can be challenging when we don't have existing mental landscapes that help us make sense of new concepts and tools. Facilitating means providing useful frames of reference.

The good news is that a lot of great trainers have already done the hard work of articulating foundational concepts for digital security work that then open the conversation up to other specific practice- and tools-based topics.

Here are examples of lesson plans you might use to facilitate a first session with newsroom colleagues, along with brief explanations of when these framings can be most helpful.

### 5.3.2 How the Internet Works

Mariel Garcia and Spyros Monastiriotis' [How the Internet Works](#) is a great introductory lesson plan that starts by walking through the basics of how information is stored and flows between devices on the internet. You can then talk about the vulnerable points in the chain—and start a conversation about the related good security practices. The lesson plan is intended for sessions lasting between two and four hours.

Tactical Technology Collective's [How the Internet Works](#), and the "How mobile communications work" module on [My Shadow](#) cover similar material in shorter 30-minute activities.

### 5.3.3 Assessing Risk

Internews' [SaferJourno](#) includes a nice module on risk assessment (see page 17). [Frontline Defenders Workbook on Security](#) and Tactical Technology Collective's [visual actor mapping](#) session are also good resources for facilitating conversations about risk and risk assessment. These can be good starting points for discussing concrete steps that are important to take.

This framing is most helpful in an environment where participants are working closely together and share common risks.

### 5.3.4 Where Your Data Lives

The [Data Backup Matrix](#), a Level Up activity, asks participants to reflect on the places where their data is stored by facilitating creation of an "information map." This exercise is based on the idea that understanding what exactly

is at stake in a digital security crisis and what the least and most vulnerable points are will enable subsequent risk assessment and tool learning.

This framing can be particularly helpful when working with groups that have had other digital security trainings but never really changed any of their practices, as this exercise can help them re-engage with the importance of better practices in their particular cases. This activity is intended for a session lasting 30 to 45 minutes.

### 5.3.5 A Day in Your Life

Tactical Technology Collective's [A day in your life](#) asks participants to create a timeline, or a time-based "information map". The exercise is based on the idea that thinking about the times you are most vulnerable can help participants prioritize changes they want to make as they build digital security skills.

This framing is helpful for groups where individual analysis is most appropriate, and when working with groups that have had other digital security trainings but never really changed any of their practices, as this exercise can help them re-engage with the importance of better practices in their particular cases. The activity is intended for a session lasting an hour.

### 5.3.6 Tracking – Who's Collecting Our Data? How? And Why?

Tactical Technology Collective's [My Shadow](#) includes a few great activities and workshops crafted around the idea that people can more easily make sense of best practices if they start by talking about services people already use and the data that is being collected.

This framing is particularly useful in newsrooms that cover low-risk topics but are interested in building digital security capacity. The activities are divided into 30-minute modules, which you should complement with discussions on the topic.

### 5.3.7 Reflecting on Existing Security Practices

This [holistic security exercise](#) by Tactical Technology Collective is based on the idea that people are not really starting from scratch in terms of security, even if they are coming to their first training. Exploring previous knowledge and practices is a good way of making the entire process more relevant for them.

This exercise isn't meant to be a stand-alone session, and can be a good warmup for a longer skill-based session.

### 5.3.8 Integrated Security

Some digital security trainers have used Kvinna's [integrated security facilitation approach](#), based on the idea that collective discussions on what security means and the practices we already take to protect ourselves are a good way to continue building our security capacity.

This framing can be helpful in newsrooms where security needs are much broader than what is typically covered in digital security curriculum. The lesson plan is intended for a session lasting two to four hours.

### 5.3.9 This is Awesome

It is easy to get caught up in everything that's wrong with the internet and digital communications. Some digital security trainers like to start by resetting that pessimism with a conversation about just how awesome the internet actually is. If this is a framing strategy that resonates for you as a trainer, the general idea is that you start with a roundup of everything that is fabulous about the internet and then shift gears to talking a bit about the value of digital literacy. Eg.

```
Today, if we want to talk to hundreds, or even thousands, of people, we can turn to
↳Twitter, or a host of other platforms. Networks with equivalent reach and ease of
↳access simply didn't exist for previous generations. Now it's a regular part of
↳life.

There are more books than we could hope to read, much less own, that fit on a three-
↳inch screen. There are more audiobooks, than we could ever listen to in the public
↳domain, read by random volunteers. We can book a flight to Seoul, order a box of
↳baby chickens, and find patient communities for dozens of rare diseases in the span
↳of 20 minutes, all from a phone, or a small box with more computational power than
↳took humanity to the moon.

We live in an age of working magic wands, an age with no muggles. We're all wizards,
↳but there's no Hogwarts: we're muddling through, and a world where everyone has all
↳these powers can look scary. But the world gets better as we all learn to use our
↳powers.
```

Practical privacy and security is just a part of digital literacy. Right now, for most people, learning how their computers work is hard enough. Learning how the network works seems out of reach. It's not impossible, it just takes a new perspective on the world we live in everyday. Digital privacy is digital literacy: It means learning how to use your network powers, and how to defend yourself in an environment of network powers.

Contexts in which this framing can be helpful: when you want to set a tone that none of this should be scary or overwhelming.

## 5.4 Setting Expectations

Once you've identified a framing that resonates with you as a trainer, or that will resonate with the group, let that framing help you identify, and (as necessary) gently adjust expectations for the group. Most of these framing suggestions start with activities that incorporate a conversation about expectations. Two other great resources on setting and managing expectations are Chris Michael guide to [getting participants in sync](#), and DJ and Nicolás Sera-Leyva's guide to [understanding and managing expectations in digital security trainings](#), both at [Level Up](#). Some of the places where there's often a gap between expectation and reality, in digital security trainings:

- There is no such thing as perfect security.
- There is no such thing as a permanent digital security solution.
- You are as secure as the most "un-secure" person you connect with online.
- Security is personal.

Participants who come in hoping to given The Right Answer™ will leave frustrated if you don't reset expectations at the outset of a series. Digital security is not just about knowledge: it is also about changing habits. Nobody changes long cultivated habits after a single two-hour workshop. As a trainer, you can set participants up for success by encouraging everyone to make realistic commitments, and to keep those commitments.

Privacy and digital security aren't solo endeavors. Normalizing secure communications is a way to work in solidarity with more vulnerable groups—as people use encrypted channels to touch base about what's for dinner, or what time to meet up, we all help make private and secure communication normal. By using secure communication tools for every day chatter, we can also identify, articulate and document bugs and issues that make those tools hard to use in high stakes situations.

Security is an effort we make for ourselves, for others we care about, and also for others we currently do not care about. We rely on each other – security might be an act of moral obligation, civic responsibility, or love.



## 5.5 Games Worth Playing

Games are a helpful way to keep your audience engaged, and to gently introduce them to technical concepts. It's unrealistic, and probably not useful, to try to provide a detailed description of how the Internet works in the time you'll most likely have. Instead, the games below will give your participants an intuitive understanding of basic networking concepts and the role that encryption plays in securing their communications - and hopefully add a little fun to your training sessions!

### 5.5.1 Cell phone game (generally for 10+ people)

Ask for volunteers to be cell towers, and get them to stand up.

Depending on the size of the room, ask for one or two volunteers to be cell phones. Ask the towers to spread themselves evenly around the room. Ask the cell phones to go to opposite sides of the room, or one side if you only have one cell phone.

Explain the rules thusly: When you call stop, the cellphones stop, and say loudly, "Where am I?"

The closest tower responds: "Marco"

The second closest tower responds: "Polo"

The third closest tower responds: "is a very interesting historical figure"

(Alternate for non-native English speakers: "Ping" "Pong" "is a game with two players")

Ask the cell phones to walk towards each other, or to the other side of the room, if there's only one cell phone. Quickly call "Stop!" Encourage anyone who is confused, and help them with any of the steps they are having problems with. It's normal for there to be some confusion on this iteration, especially for the person who must say "-is a very interesting historical figure." This is normal and desirable, as this is an engagement exercise as well as a technical one.

Once everyone has stepped through one iteration, stop the game and explain: Each cell phone tower has a circle around it that represents its range. Once you've checked in with three towers you know that the cell phone is within the overlap of the three towers. This creates a point that lets the towers know that a cell phone was in a place, at a time - also called "triangulation". Point out that this isn't surveillance, or something that companies or governments decided, this is how the physics of radio waves work. This is a good time to make it clear that if your phone is on, and working as a phone, the time and location must be known. Physics, not policy.

You should take this as a chance to explain that systems of surveillance are often built on top of how things just work in the real world. Moreover, that most of the surveillance systems people are worried about are built on top of the first and most prevalent form of infrastructure surveillance - billing systems. You can point out that while this is simplified, it is analogous to how cell phones work, checking in and using time and location data to handle connectivity.

Ask the cell phones to start walking again. Before they meet, call stop. Go through a second iteration, helping anyone confused or having problems as either a cell phone or a tower. Once the second iteration is done, show how two points make a line, and begin to construct path data. Walk the path of one of the phones to point it out.

Let the phones start walking again, meet, and do a third iteration when they meet. This shows they occupy the same point now. After the third iteration, ask the phones to walk away together. Depending on how it's going, you may or may not want to do another iteration, but at this point you can explain that two paths met and went on together, showing how the data looks to the tower/telecom perspective.

Thank the towers and cell phones, if it's a big room it's fun to clap for them, and ask everyone to sit down again.

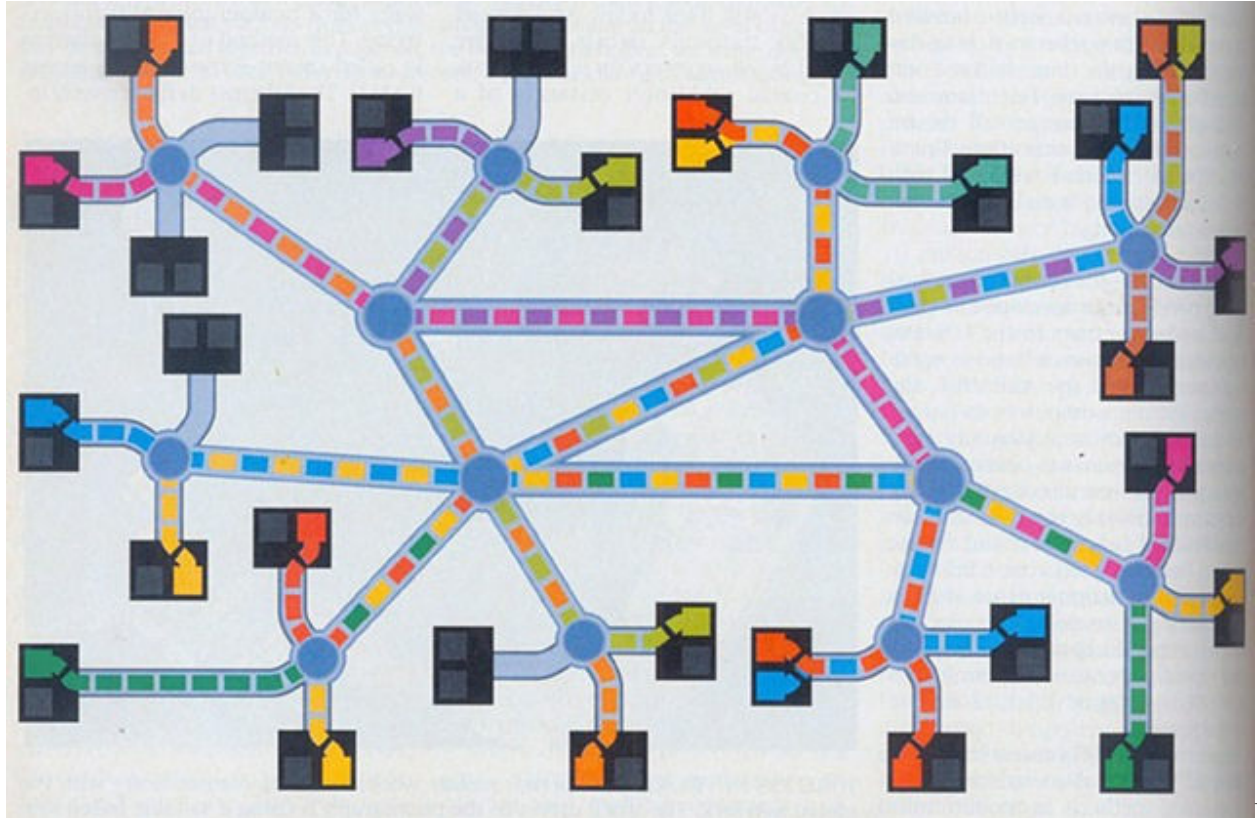


### 5.5.2 Packet switching/passing notes in class (Not easily playable with fewer than 6 people)

**Materials:** notes made out with *To* and *From* fields as well as a message, pen or pencil. (Pre-populate the notes with something funny or cute.)

This is an exercise that can be modified and extended throughout trainings to build new ideas on top of the basics of network architecture.

Start with a diagram or picture of a packet switching network, such as the example below:



Explain that the node on the end breaks the message into pieces, then passes the pieces to the node it thinks will get the message closer to the destination. That node hands the packet to the next that seems like it might be closer, and so on until it gets to the end point it was intended for. The destination node reassembles the message, and voila! The internet magic happens. This system is more like passing notes in an 8th grade classroom than anything else.

Ask for a volunteer source and destination. If people don't immediately volunteer, threaten to call on them, establishing yourself as the putative 8th grade teacher. Once you have your two volunteers, write their names on the from and to fields of the small note. Give the note to the source, and tell the room they have to pass the note to the destination without getting caught. Turn your back so they can get started passing the note. Turn back and patter a bit about networks, keeping an eye on the room. Try to catch them at the note passing, and fail. Once the note reaches its destination ask that person to raise the message, demonstrating they got it.

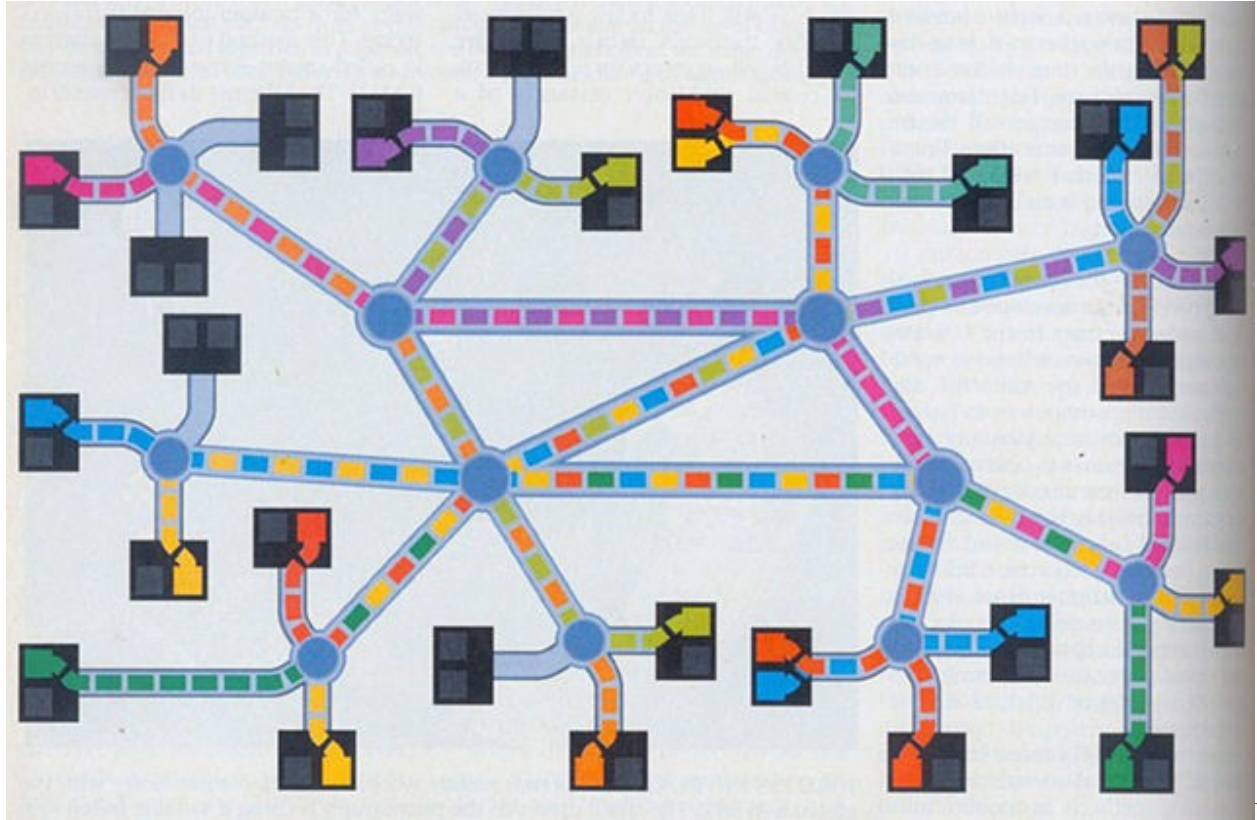
If the message is going by a circuitous route, it's fun, and true, to note that happens on the internet as well.

Once the note passing is complete, ask everyone who saw the note to raise their hands. Once their hands are up, ask what the problems are with a packet switching network. Discuss the fact that everyone on the network has the chance to see, and even modify the note. For example, one of the evil 8th-graders could change the name of a crush and ruin the rest of the semester for someone. Bring it back to the internet, pointing out that people can read and change messages on a packet switching network.

### 5.5.3 Packet switching/passing notes in class with encryption variations

**Materials:** notes with messages, envelopes with *To* and *From* fields, pen or pencil. (Pre-populate the notes with something funny or cute.)

Keep or return to a packet switching network image.



After you've run the first variation of passing notes in class, you can relax the pretense of teacher (though it may be fun to keep it up, depending on the audience) and begin to add layers.

Many kids started to encode messages in school, so you can point out that encoding messages helps solve all the problems the room identified in the first iteration of the game. An encoded message not only can't be read, it can't be altered, which may be even more important for news organizations. This time you can create the message, but then use the envelopes for one of two variations (you may want to do both, and not in this order):

- End-to-end encrypted message
- Server side encrypted message

#### End-to-end encrypted message variation:

Ask for two volunteers, and put them on the to and from field of the envelope. Give the envelope to the sender, and have them put the message in it, and seal it. The envelope here represents mathematical computer encoding, aka encryption. The rule this time is that only the receiver has the power to open the envelope. Begin the note passing again. If you're still playing teacher, you can try to catch them at it with threats of detention. Either way, don't direct the note, let the class route it themselves. If it's taking a long time, you can admonish them humorously for being a slow and clunky connection without good routing, while pointing out that this sometimes happens on the internet too. (Your class cannot make a mistake that doesn't also happen on the internet. The internet has all the problems.) When the note arrives, tell the recipient to open the envelope and take out the message.

Ask the room to raise their hand if they saw the message. Only the sender and receiver should raise their hands. Then ask them to raise their hands if they saw the envelope, so that the whole route taken should raise their hand now. Ask them what the term is for what they saw. They should answer metadata without too much coaching. Ask them further what metadata they know about that exchange. They will come up with to and from, but keep fishing. They should also arrive at the time of the class, and the people who handled the envelope. If you've got someone very on the ball they might say that it was passed in an envelope, which segues easily into detecting protocols and encryption on the net.

### **Server side encrypted message variation:**

You should start this game by pointing out everyone in the room has a gmail account (if people protest that they don't, remind them that Google has all their mail anyway, since everyone they mail has a gmail account). Ask for a volunteer to be Google. Often one of the more tech-savvy participants will volunteer. After that, ask two more volunteers to play sender and receiver. Importantly, in this variation you will need two identical copies of the message, and two envelopes: the first one to Google from the sender, and the second one marked from Google to the receiver. The rule in this variation is that the message must always go through Google to get to its destination. Give Google the second "From Google" envelope before note passing begins, and put the two copies of the message into the first envelope and seal it, writing the from on it. Begin passing the first envelope, and go stand by Google. Once the envelope reaches Google, tell them to open it up, take out both messages, *keep one of them*, and put the other into the destination envelope and reseal it.

You can write "HTTPS" on the envelopes in the Google variation to prime the room for talking about SSL/TLS, the protocols commonly used to encrypt Internet communications including web traffic and email.

Now, pretend to be a European or the American government, someone that has the ability to compel Google with a lawful order. Walk over to your Google volunteer, and make a show of being friendly, then asking to see the copy of the message Google has. Google will usually agree and hand it over, but if your Google volunteer doesn't, ramp up the playful threats (seizing assets, arresting employees, etc.) until they hand it over. Make a show of reading it and hand it back.

### **Iterating on these exercises**

You can follow these variations by combining them, putting another envelope inside the TLS/SSL HTTPS envelope that your Google volunteer has to be put into the envelope to the destination volunteer. You can either leave them with a "cyphertext" version or nothing, so that when you return as the government, you are frustrated by Google not having the message to show you. This presages a discussion of encrypted messaging, including Off-The-Record (OTR) protocol used by some chat apps, and double ratchet protocols such as that used by Signal Messenger. In all cases, you can demonstrate that the To: and From: data is preserved by Google, or potentially by the transiting network itself, for whatever part isn't covered by TLS.

### **Tor note passing variation**

**Materials:** Three nesting envelopes, one message (content isn't important.) Largest envelope should be addressed to "Node 1", second largest, addressed to "Node 2", smallest addressed to "Node 3".

This exercise demonstrates the basic concept of the Tor network. Before you start, ask for a show of hands of people who know what Tor is. If your participants aren't familiar with Tor, spend a little time describing the system to them before getting started.

Ask for five volunteers: Someone to play "the internet" ("Who wants to be the internet?!") Someone to play the Tor user, and three to play Tor relay computers. Number your Tor node volunteers 1, 2, and 3, and make a point that the other term for Node 3 is the exit node.

Give the supplies to the Tor user, and instruct them to put the message in the smallest envelope, and seal it. Then that envelop into the second envelope, and so on, until the user is holding the envelope addressed to Node 1 with all the other materials stuffed and sealed into it. Instruct the notes to pass to Node 1, and when Node 1 gets it, have them open the envelope and pass it to Node 2. As Node 2 opens the envelope from Node 1, point out that all Node 2 knows it who the first node was, and who the next node is; this is the “magical” step of Tor, since no one can know both where the message came from and where it’s going, as well as what it is, after this point. Node two passes the smallest envelope to Node 3, who opens it, and then passes it to “the internet”.

Ask what the problem is now, but also what this system is accomplishing (in short, neither Node 3 or the internet can figure out where the message came from, but they can see what the message is, without a further layer of encryption using one of the two models we’ve talked about in previous note passing exercises)

### 5.5.4 More games to use in training

These are great road tested games for teaching networking principles. If you’re looking for more ideas for games trainers play, check out:

- Games Trainers Play(<http://www.worldcat.org/oclc/6016638>) and Even More Games Trainers Play(<http://www.worldcat.org/oclc/30318772>) for some great ideas.
- Or take a look at the curricula and guides we’ve aggregated in our [Resource Guide](#).

## 5.6 Pathways: Choosing Lesson Plans

There is a lot of material in this guide – and a lot of different ways to approach it. The guide is designed to be modular. Lessons are ordered so that ones that tend to appear as pre-requisites come first, but some newsrooms already enforce two-factor authentication or support a preferred password manager, while others leave it to individual reporters to find their way.

Some users will want to lead a formal series of in-depth workshops, while others will respond to a specific newsroom need or just offer an occasional lunch hour session. Either way, less can be more. Rather than trying to cram everything into a marathon workshop, break goals down into short walks that build on each other, and let each tool sink in before adding another. Participants shouldn’t leave with more than one or two projects on their to-do list.

### 5.6.1 Sample Pathways

#### Just mobile

1. [Mobile Security Settings](#)
2. [Locking Down Mobile Devices](#)
3. [Setting up Signal](#)
4. [Backing up Mobile Devices](#)
5. [Physical Security](#) – iPhones are already encrypted but Android users should set up disk encryption.

### 5.6.2 Secure email use

1. [Passwords](#)
2. [Two-factor Authentication](#)
3. [Phishing](#)

Savvy readers will note that this guide doesn't currently include a guide to encrypting email with GPG or PGP. Why? It's hard to use and history has shown that most folks don't use it properly. As Martin Shelton has pointed out, [newsrooms have better options](#).





---

## Chapter 2 - Lesson Plans

---

Chapter 2 is an ever-expanding collection of lesson plans and training materials to help people cover key topics with their peers.

### 6.1 Chapter 2: Lesson Plans

This chapter includes lesson plans for the most common newsroom needs. If there's a lesson you're looking for and you don't see it here, definitely [let us know](#). If you have a favorite resource that you think we should include, we'd love to hear about that, too.

Every lesson plan includes an overview of the lesson, prerequisites and materials that trainers and participants will need, and a good walk through of the tool and concepts. If you run one of these lessons and find that it goes a lot faster (or a lot slower) than our estimate, we want to know. Each lesson concludes with a round up of links in the news that illustrate the importance of the material in the lesson, and a round up of links to other teaching resources that cover the material well. If you have resources that should be included in those link round ups, please do share them with us.

#### 6.1.1 What Is Included

**Mobile Security Settings** This is the first short module in a series of three trainings dedicated to securing your mobile device. In this module, iPhone and Android users will learn how to review the security settings on their mobile devices. In later trainings, they will learn how to encrypt their device, set a secure locking mechanism, and install an encrypted messaging system (Signal). These three modules are meant to be short and simple. Each can serve as a quick win in a larger session about something else, or can stand alone as a short session. Or the three mobile sessions can combine nicely into a 60- to 75-minute block of training around securing a mobile device.

**Locking Down Mobile** This lesson plan helps participants secure their mobile devices by setting up lockscreens and securing lockscreen notifications, applying system updates, and encrypting device storage. This module is meant to act as the second in a series of three, building up a 60-75 minute training block on secure mobile communications.

**Setting Up Signal** Signal is a secure messaging platform that utilizes end-to-end encryption. Before starting this lesson, participants should have already been through a [mobile application settings review](#) and added secure lockscreens to ensure that their device is ready to use with a program like Signal. Some benefits of Signal: they do not store

messages on their servers, participants can set their conversations to “self-destruct,” and users can customize what information (contact name, message preview) is available on their phone’s lockscreen. This lesson plan is intended to be taught as the third in a series, following [mobile app security settings](#) and [locking down mobile devices](#).

**Mobile Backups** Creating regular, secure backups of data on mobile devices is important, whether users want to protect against loss, theft, or catastrophic error (e.g. accidentally wiping a device while encrypting it). This session covers the creation of encrypted backups for iOS and Android users, and make recommendations on a backup schedule.

**Good Hygiene for Apps** Overview: Don’t let orphaned apps degenerate into an unlocked back door to your account.

**Passwords and Password Management** Passwords are the bedrock of account security, but they’re hard to get right. This lesson explains how to take a harm-reduction approach to password management. Participants should have a clear understanding of [phishing](#) and [two-factor authentication](#), or you should cover those topics as part of this lesson.

**Two-Factor Authentication** Enabling two-factor authentication (2FA) is one of the easiest steps people can take to protect their online accounts. Even if someone gets ahold of a user’s password, 2FA will ensure that they can’t get very far. 2FA adds extra protection by requiring additional information for login, which is provided by text message, a code from an authenticator app, or the use of a hardware security key. This lesson plan introduces key concepts about 2FA, and guides participants through the process of setting up app-based 2FA for their primary email accounts.

**Phishing** Phishing is an email-based social engineering tactic that uses misplaced trust to extract information and access. Like other forms of social engineering, its purpose is to trick you (the target) into divulging information that can be used to gain access to private data, networks or resources. Participants will learn about phishing in the context of trust decisions, and develop awareness and techniques to make these decisions when interacting on the web.

**Physical Security** What happens to a person’s data if their device is seized or stolen? How should people prepare to cross international borders safely? This session discusses ways to approach border crossings, and walks through the process of enabling full-disk encryption, which can help ensure that someone who has a physical device doesn’t necessarily have access to all its data. This module makes a few assumptions about participants’ threat models, and is written with American journalists in mind. If participants’ work puts them in conflict with hostile state actors, they should seek out more specialized training.

**Scrubbing Metadata** Files such as Word documents and JPEG images usually contain information about the systems used to create them. This information, commonly referred to as metadata, could inadvertently reveal personally identifiable details about sources to anyone given access to the files. This lesson plan teaches participants how to find metadata in Word documents and JPEG files, and ways to share or publish content from these files without exposing metadata.

**Secure Drop** SecureDrop is an anonymous whistleblowing tool designed to provide users with a high degree of protection from detection through Internet-based surveillance. This lesson plan covers the keys to using SecureDrop effectively: establishing a culture of security, setting up SecureDrop securely, and making sure sources know how to use it safely.

### 6.1.2 What Is Not Included

This guide doesn’t currently include a guide to encrypting email with GPG or PGP. Why? It’s hard to use, and history has shown that most folks don’t use it properly. As Martin Shelton has pointed out, [newsrooms have better options](#). However, there are use cases when GPG is the best option. If you want to [help build this resource](#), we welcome a lesson plan that introduces email encryption. There are a few good resources out there on the subject: This one, from [Riseup](#), is a good start.



## 6.2 Mobile app security settings

### 6.2.1 Overview

This is the first short training module in a series of three trainings dedicated to securing your mobile device. In this module, participants will learn how to review the security settings on their mobile devices (for iPhone and Android users). In later trainings, they will learn how to encrypt their device, set a secure locking mechanism, and install an encrypted messaging system (Signal). These three modules are meant to be short and simple. Each can serve as a quick win in a larger session about something else, or can stand alone as a short session. Or the three mobile sessions can combine nicely into a 60- to 75-minute block of training around securing a mobile device.

### 6.2.2 About this lesson plan

**Review date:** June 5, 2017 **Lesson duration:** 20-30 minutes **Level:** Introductory. This session is for journalists who may not realize how many permissions they have given to the third-party apps on their phone, and for those who are not regularly doing good security hygiene on their devices.

#### What will participants learn?

A better understanding of how mobile apps utilize a phones sensors and components, including location services, microphones, cameras, and call history, as well as insight into how those components may be exploited.

#### What materials will participants need?

Everyone should bring their smartphone (iOS or Android).

#### How should participants prepare?

Most should have read at least a few articles from [\[#links\]\(Links in the News\)](#), so that they can come in with some context.

#### What materials will the instructor need?

A white board, chalkboard or big sticky pads will help, but you can certainly make do without.

#### How should the instructor prepare?

Review the materials, and review the [resources on how to be a better trainer](#).

### 6.2.3 Lesson Plan

#### Icebreaker

This can be a quick session and an opportunity to “get something done” that helps everyone take a basic step towards better security.

Have participants to name as many data collection points on their smartphones as they can (think: gyroscope, compass, microphone, camera, GPS, barometer, etc). Note which could be used for malicious purposes. Use a white board or giant sticky note if you have one. Review some recent news stories about consumer applications that abuse access.

### 5-minute discussion

Any mobile device has a few unique identifiers, the International Mobile Equipment Identification or IMEI distinguishes the actual device, while the SIM serial number is unique to each SIM card. These unique identifiers can be used by marketing companies to track a specific device or subscriber through multiple apps.

Android devices allow apps to request access to “Device ID and Call Information.” iOS does not allow apps to ask for the device ID, though it is still possible to fingerprint devices using other identifying information.

### Walk through

Ask participants to break into pairs (try to group them by OS), so they can help each other troubleshoot. Each pair will open the settings on their phones together and review the applications that have access to their location, microphone, and camera. (Some participants may feel more comfortable doing this solo, which is fine.)

While the group is reviewing their privacy settings, it’s a good time to talk about why an application might ask for access to the camera, microphone or location services.

#### For iPhone users:

Open settings, go to **Privacy** (a small gray icon with a hand)

- Location Services: these applications have access to your location based on GPS, Bluetooth, wifi hotspots and cell tower locations.
  - Apps will either have two or three options for this setting: Never, While Using the App, or Always. If “Always” is an option, it means that the application can have access to your location even if you do not have the application open.
  - The app will often have a one-line explanation as to why it is asking for your location. (E.g.: Yelp says, “This app needs your location to search for nearby businesses.”)
  - A small arrow-shaped icon is used to indicate whether an application has used your location recently or within the past 24 hours.

●●●○ AT&T

3:56 PM

72%

< Privacy

## Location Services



Wallet

While Using >



Weather

Never >



WeChat

Never >



Weekender

Never >



Wells Fargo

While Using >



Wikipedia

Never >



Yelp

While Using >



Yelp Eat24

While Using >

System Services



A purple location services icon will appear next to an item that has recently used your location.



A gray location services icon will appear next to an item that has used your location within the last 24 hours.



An outlined location services icon will appear next to an item that has used your location within the last 24 hours.

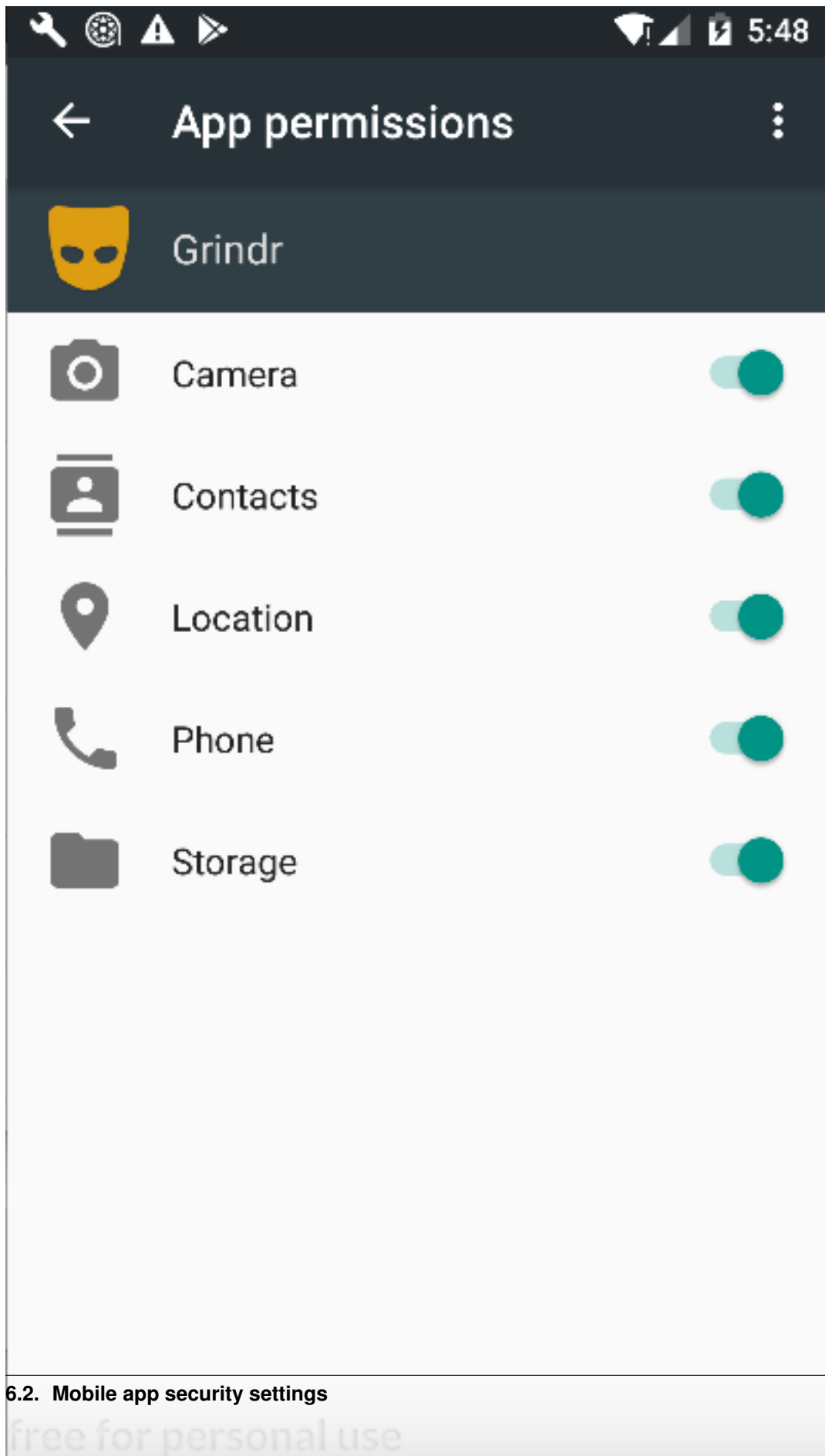
- Microphone: Any application that has requested access to the microphone should appear in a list with a set of toggles (the only settings are “on” and “off”)
- Camera: Any application that has requested access to the camera will appear in a list with a set of toggles (again, the settings options are “on” and “off”). This includes access to the camera itself, as well as access to the photos stored on your phone.

*Note: Phone settings change all the time. If you're planning on working with a large group, double check that these steps still apply, and consider [submitting an issue](#) with updated instructions if they don't.*

### **For Android users:**

The process of checking application permission settings differs between Android versions. To find out which version of Android your phone is running, check Settings > System > About Phone.

- Marshmallow (6.0) or later: Open Settings > Apps. Click the gear icon and open **App Permissions**. A list of permissions will be displayed including features such as Camera, Location, and Microphone, along with their current settings.
- Android versions before 6.0: Open Settings > Apps and select an app - you have to review permissions per app, rather than per-sensor.



## 6.2.4 Recommended Reading

### Links in the news

- [Uber uses rider location data and ride history \(BuzzFeed News\)](#)
- [Macy's uses shopper location data \(ABC News\)](#)
- [Facebook could be listening all of the time: \(Independent\)](#) (So you should probably stop letting FB access your microphone. QZ)
- [Uber is fingerprinting your device, even across factory resets \(arstechnica\)](#)
- [Motherboard Guide to Safe Sexting](#)

### Other great training resources:

- [Tactical Training Collective: Data Privacy](#)

## 6.3 Locking down your mobile devices

### 6.3.1 Overview

This lesson plan will guide participants through the process of securing their mobile device by setting up a lockscreen and securing lockscreen notifications, applying system updates, and encrypting the device storage. This module is meant to act as the second in a series of three, building up a 60-75 minute training block on secure mobile communications.

### 6.3.2 About This Lesson Plan

**Review date:** June 6 2017 **Lesson duration:** 30 mins (estimated), longer if some Android phones need to be encrypted. **Level:** Intermediate. This session assumes participants are able to make a reliable backup of the key data on their phones and have done so very recently. If they haven't, you *should not* proceed.

**Gotcha:** Consider how much time you have available before choosing to do this session. Are all your participants' devices either brand new or recently [backed up](#)? Do you have 30+ minutes and a low participant to trainer ratio? If not, you may want to either do this session in two parts on subsequent days (cover mobile device backups where you cover encrypted backups on one day, then actual encryption on the second day), *or* you share a link on backups and require participants to complete (or verify cloud backups) *before* this session.

#### What will participants learn?

Participants will learn how to set up a secure lockscreen and encrypt their mobile device storage. In conjunction with the previous lesson on [mobile application permissions hygiene](#), this prepares the device for the installation and use of a secure messaging system.

#### What materials will participants need?

They'll need their mobile devices (iPhone or Android) and device chargers.

#### How should participants prepare?

Everyone should back up their mobile devices before the workshop. If folks haven't done that or aren't confident that they're backing up everything they need, start with a session on [mobile backups](#).

#### What materials will the instructor need?

If you don't already know the group well, make sure you've checked in about their technical capacity and check out Chapter 1 to make sure you're planning ahead.

### How should the instructor prepare?

You probably want participants to tell you in advance what phone OS they're using.

Read through: <https://theintercept.com/2017/05/01/cybersecurity-for-the-people-how-to-keep-your-chats-truly-private-with-signal/#lockdown>

Consider setting a calendar appointment for a week after the training, to remind yourself to follow up with any participants who opted to put off updating or encrypting their phone. They're more likely to follow through if they get a reminder before too much time has passed.

## 6.3.3 Lesson plan

**Introduction** Survey the room:

- Who's lost their phone before? (Bonus points for the best story! If anybody lost theirs and got it back, might be a good time to ask if they were worried about the time it spent out of their control)
- Which device types people are using (iOS/Android/other? The "others" may need special attention)
- How many already have a passcode or password lock screen set up?
- How many have encryption set up?
- How many apply updates regularly?

Spend some time on what makes a good passcode (length and randomness are good, birthdays and sequential numbers are bad). The [password](#) lesson has more great resources on this question.

**Walkthrough** Split people into groups by device types - instructions will differ for iOS vs Android. Everyone is going to ...

- set a password or passcode,
- review lockscreen notification settings,
- check for system updates and apply them (or make a plan to apply them later). Note that system updates can sometimes take 20-30 minutes to download and install. In some cases it is more appropriate to

**Trainer notes:** For *lock screens*, a strong password is always recommended. A PIN or passcode is an acceptable alternative, but it should be at least 6 digits long. For example, in the US you can be legally compelled to provide your biometrics to unlock a device by a court.

Biometric locking (eg. face or fingerprint recognition) is not recommended, as both are fakeable and do not offer the same degree of legal protection. For example, in the US you can be legally compelled to provide your biometrics to unlock a device by a court.

Android phones offer pattern locking, which is also problematic. It's not as secure as a passphrase, and weak to shoulder-surfing.

When you tackle *lockscreen notifications* keep in mind that some users may opt to keep convenient but insecure notifications coming for day to day use and change the settings when they're in more vulnerable situations or traveling.

*System Updates* can take 20-30 minutes or more to download and apply. In some cases it might be more appropriate to have everyone check for system updates and commit to actually applying them later.

*Encrypting* a phone's hard drive can take even longer than a system update and this **should not** be undertaken unless the user is 100% confident that their data, settings, and authentication codes are backed up.

### For iOS:

#### Set a passcode:

- To set a passcode, open `Settings > Touch ID & Passcode` (it's a little red icon with a fingerprint on it)
- If you already have a passcode in place, you will be asked to re-enter your existing passcode.
- Click “set passcode” to reset your passcode or create a new one. The default is a 6-digit code, but if you click “passcode options” you can also choose Custom Alphanumeric Code, Custom Numeric Code, and 4-Digit Numeric Code.
- Enter your new passcode twice to verify it
- You will also be asked for your Apple ID password to verify your new passcode
- The default setting for an iPhone with a passcode is that it is required “immediately” after locking the phone.
- iPhones offer an “Erase Data,” option. If you select it, **all data on the phone will be wiped after 10 failed passcode attempts**. This is strongly **not recommended** for clumsy people or people with small children.

#### Secure lockscreen notifications:

- Open Signal and select the gear icon to open its settings
- Select `Notifications > Background Notifications > Show`.
- The “No name or message” option will ensure that Signal lockscreen notifications will not include the senders name or message content.
- To completely disable Signal notifications, or any other sensitive notifications, open the iOS Settings app, select `Notifications`, and change the notification settings for Signal and any other sensitive apps.

#### Apply system updates:

- Make sure your device is fully charged and connected to its charger. It's also a good idea to backup your device data before applying system updates.
- Updates can take 20-30 minutes to download and install, and during that time the phone will be unusable.
- Open the Settings app and go to “General”. If a software update exists, there will be a small, red circle with a 1 inside of it.
- When you click through, choose “Software Update,” > “Install Now,” enter your passcode and let it run.

**Encryption:** iPhones are already encrypted. Congratulations!

### For Android:

#### Set a passcode:

- Open the Settings app and select `Security > Screen Lock`
- Select a lock screen type. A strong password is the most secure option.
- Depending on Android version, you may also be prompted to enable a setting called “Require password to start device” – this setting will lock your device on startup, preventing it from receiving calls or messages until the password is entered. It's recommended but not required.
- Memorize and enter your new password or passcode.

#### Secure lockscreen notifications:



- Open the Settings app, select Sound & notification and look for an option called When device is locked.
- Select hide sensitive notification content (or don't show notifications at all). These options work, more or less, as described.

**Apply system updates:** Have everyone open the Settings app and check About Phone > System Updates. If you do have an update waiting...

- Make sure your device is fully charged and connected to its charger. It's also a good idea to backup your device data before applying system updates.
- Follow the on-screen instructions to apply any available updates.

**Encrypt your device:** The process of encrypting a phone can take an hour or more. You should make sure that participants know their phone will be unavailable while it is being encrypted. Do not encourage anyone to encrypt their phone unless it is a new phone or they're 100% confident that everything on the [device is backed up](#). If someone loses their authenticator app and doesn't have backup codes, they may have a very (very) difficult time restoring access. So just to reiterate: don't encourage anyone to encrypt their phone unless you're 100% confident that all the data and settings they need to restore their phone are backed up.

- Make sure your device is fully charged and connected to its charger - encryption can take a while (an hour or more) and can not be interrupted once it starts.
- Open the Settings app and select Security > Encrypt phone.
- Follow the instructions to complete the encryption process.

### 6.3.4 Follow Up

If anyone (or everyone) opted to put off applying system updates or encrypting their phone, make a plan to touch base in a week and remind them to set aside time to actually do it.

### 6.3.5 Recommended Reading

#### Other Great Tutorials and Curriculum

- [Why You Should Be Encrypting Your Devices and How to Easily Do It](#) (Gizmodo, Sept 2017)
- Mobile Phone Settings from [Me and My Shadow: Tactical Tech](#) Training Curriculum

#### Links in the News

- [John Kelly's personal cell phone was compromised, White House believe](#), Politico, Oct 4, 2017

\*Note: it would be great to include a few links to stories about phone search and seizure here. If you want to help the curriculum grow, we'd love your help adding recommended reading links. [Submit an issue](#) or a pull request if you have good links to add.

## 6.4 Setting Up Signal

### 6.4.1 Overview

Signal is a secure messaging platform that utilizes end-to-end encryption. Participants should have already been through a [mobile application settings review](#) and added secure lock screens, to ensure that their device is now ready to use with a program like Signal.

Benefits of Signal include the fact that they do not store your messages on their servers, participants can set their conversations to “self-destruct” and users can customize what information (contact name, message preview) is available on their phones lock screen.

This lesson plan is intended to be taught as the third in a series, following [mobile app security settings](#) and [locking down mobile devices](#).

### 6.4.2 About This Lesson Plan

**Review date:** June 6, 2017 **Lesson duration:** 15-30 minutes **Level:** Beginner

#### Preconditions

This lesson assumes users have already reviewed their [mobile app security settings](#), and walked through [locking down mobile devices](#).

#### What will participants learn?

Participants will learn why encrypting messaging is important and easy to set up. They will install Signal, learn how to set and review their privacy settings, verify safety numbers, and explore some of the application’s advanced features.

#### What materials will participants need?

Smartphone: iPhone or Android

#### How can the trainer prepare?

Two excellent resources on how and why journalists are moving to Signal:

- [Martin Shelton on Signal for Beginners](#)
- [Cybersecurity for the People: How to Keep Your Chats Truly Private With Signal \(The Intercept\)](#). This lesson draws from both.

Review the Verification process for [Android](#) and [iOS](#).

Review the [Glossary](#) to think about how you want to explain encryption to the group.

Read [Signals, Intelligence](#) for a good critique of some of the things Signal doesn’t protect users against.

Additional readings that will help prepare the trainer for questions that come up: [Martin Shelton](#), [Jillian York](#), and [Micah Lee](#) all have great walk-throughs on using Signal without giving out your phone number.

### 6.4.3 Lesson Plan

Discussion: Why would you want to encrypt calls and text messages? What does it mean to send them in cleartext?

Remind folks that, in addition to keeping their own conversations private, by using encrypted messaging, they can normalize the use of encrypted messaging, which makes it safer for vulnerable people to use encryption without standing out.

*Note: this lesson would be much stronger with a better explanation of who does have access to cleartext SMS, and under what circumstances. We’d love it if you wanted to [submit an issue](#) with some resources or readings that do a good job of articulating this.*

The conversation should include some review of what Signal can protect (messages traveling over the network) and what it can't protect (messages are still stored on your phone, so anyone who is able to unlock your phone has access to them.)

Real questions that users might have: who actually has access to your text messages? The answer is a bit complex. While it is relatively trivial for someone else to read messages sent in cleartext over a public wifi network, messages sent from your phone over the cell network are not as easily intercepted. However, your phone company does have access to the contents of all of your cleartext SMS messages, which means they can be subpoenaed or otherwise acquired by local police, the FBI, or the NSA. It is relatively well documented that the NSA has, historically, [swept up phone records in bulk](#). And that's just inside the US. Around the world, privacy protections can vary widely. And as long as privacy protection is legal, and not technical, individuals are vulnerable to changes in the law or to government overreach.

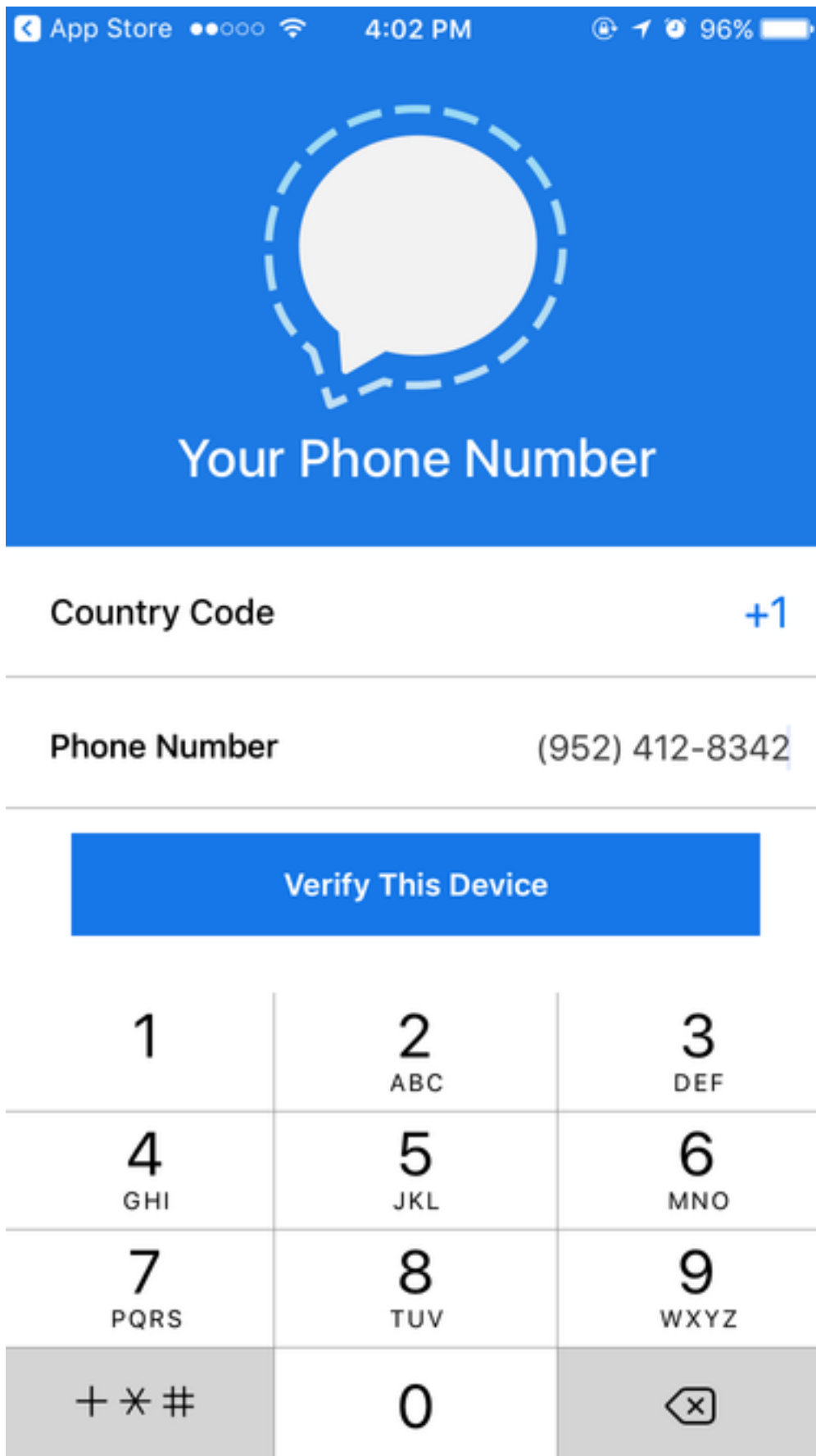
If you're sure you don't mind the FBI reading all of your text messages there are still good reasons to encrypt them:

- You might change your mind. And by using Signal now, you can ensure that it is there, and working, when you decide you need it.
- Other people need it. The more people there are who use software, the easier it is to use. That's because the simple act of using a tool like Signal effectively creates community around that tool.
- Privacy should be normal. If democracy activists and vulnerable journalists are the only ones encrypting their text messages, their communications stand out. But if everyone encrypts the boring stuff – the 25 message exchange about who is bringing what to a holiday meal, the back and forth about what time to meet or the dressing room photo of a questionable coat – then we all clear the way for vulnerable users to use encryption without standing out.
- You never know when you might find yourself working on a story where the risk of a subpoena is higher than usual. By making some small shifts now, you can ensure that the next time you find yourself thinking “I should probably not be sending this in cleartext” your next thought is “oh, right, I'm not. :)” instead of “Ack, what was that app?”

### Installing Signal

These screenshots reflect the iOS install process.

1. Start by downloading and installing Signal. Visit <https://signal.org> for quick access to the most current download links.
2. You will be prompted to confirm your device and phone number.



The screenshot shows a mobile app interface with a blue background. At the top, there is a status bar with icons for App Store, signal strength, Wi-Fi, time (4:02 PM), location, alarm, and battery (96%). Below the status bar is a large white speech bubble icon with a dashed outline. Underneath the icon, the text "Your Phone Number" is displayed in white. Below this, there are two input fields: "Country Code" with a blue "+1" value and "Phone Number" with the value "(952) 412-8342". A blue button labeled "Verify This Device" is positioned below the input fields. At the bottom, there is a numeric keypad with digits 1-9, 0, and symbols for call, star, and hash, along with a backspace button.

App Store ●●○○○ 4:02 PM 96%

Your Phone Number

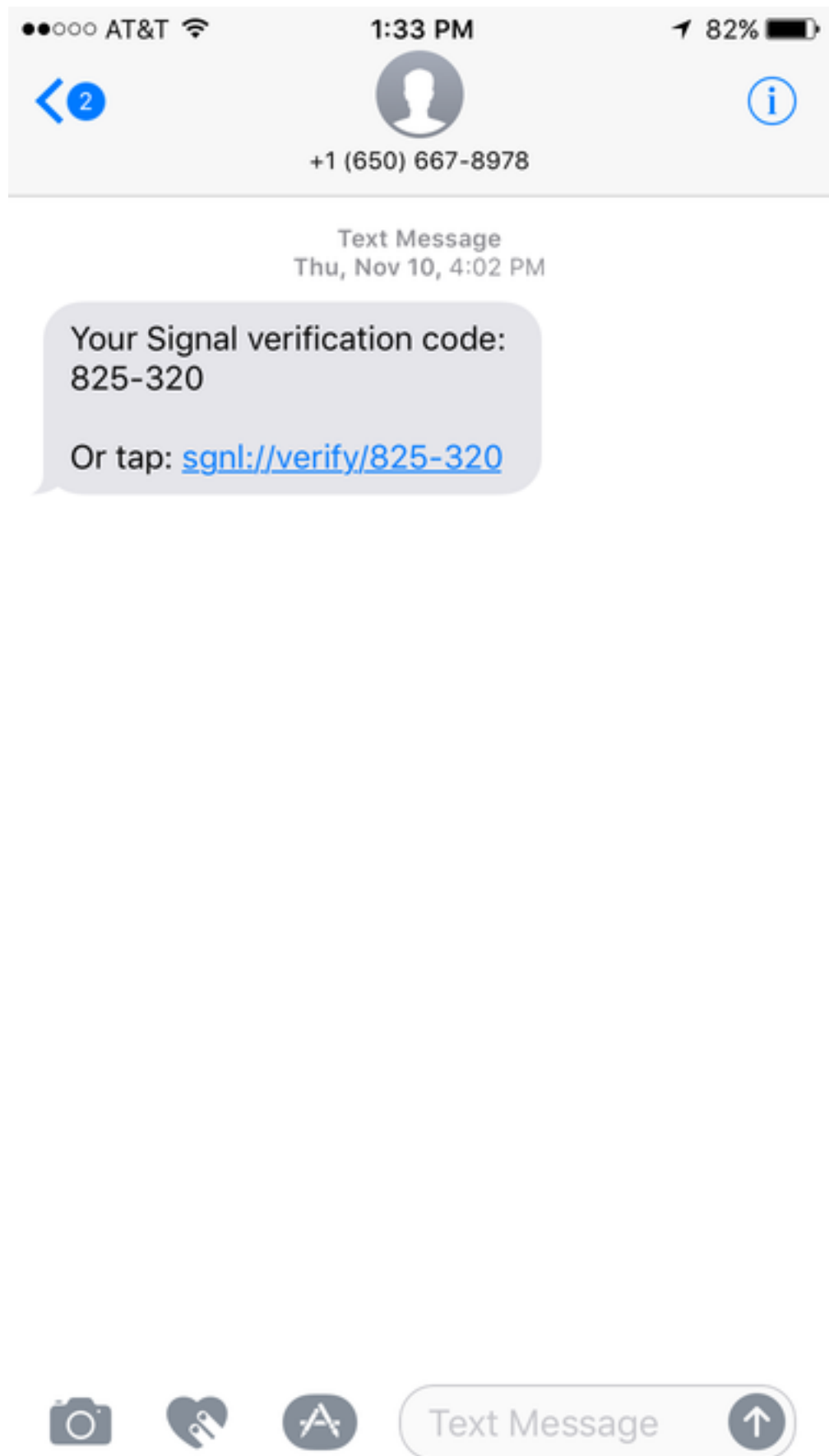
Country Code +1

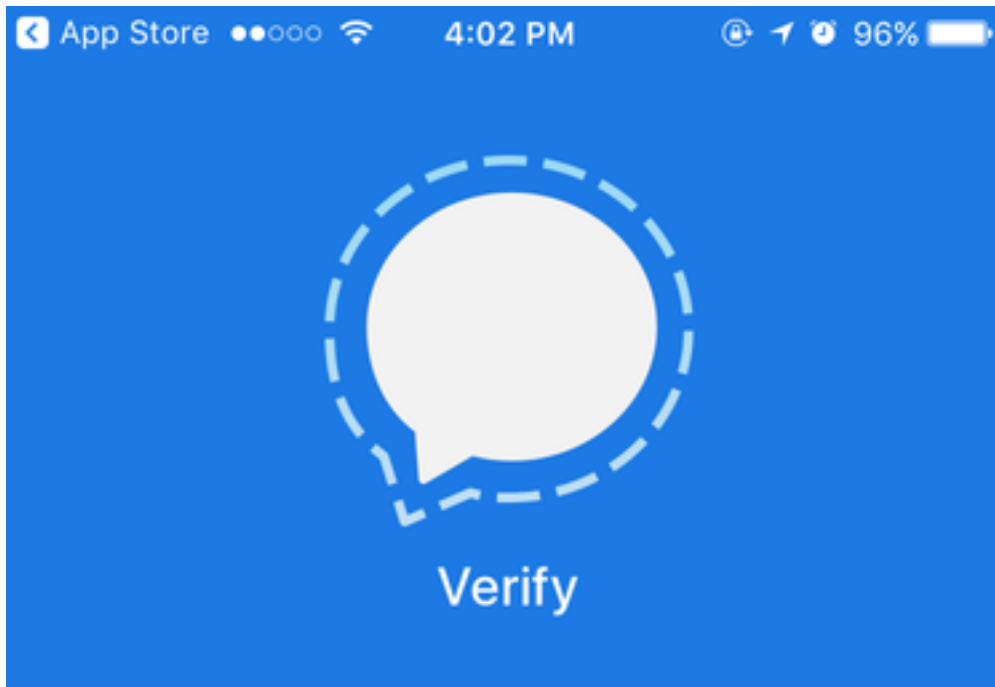
Phone Number (952) 412-8342

Verify This Device

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
+ * #	0	⌫

3. Next, Signal/Open Whisper Systems will send you a six-digit verification code. Add





Verification Code

Submit Verification Code

Request Code Again

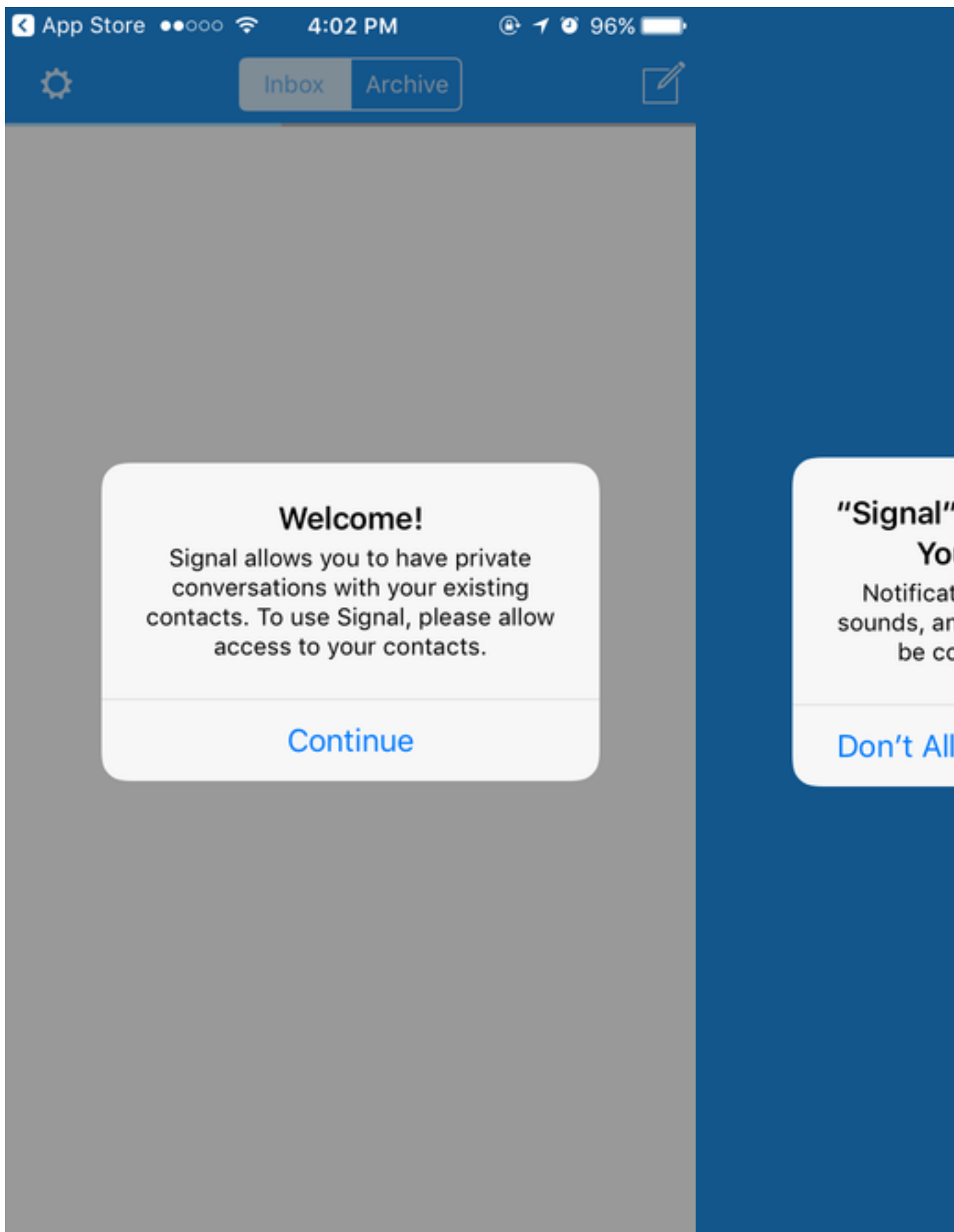
Call Me Instead

+1 952-412-8342

< Change Number

4. Android users: Signal will offer to become your default messaging app. Say yes! You can still use Signal to send cleartext messages to contacts who don't use the app, and you won't miss messages.
5. You'll know that you've set Signal up correctly when you see the Welcome! popup. You can allow the system to access your contacts and send you notifications. *(NOTE: in the newest version of iOS, it is possible to continue without giving access to your contacts)*





### For Android:

The steps are very much the same. Signal will offer to become your default messaging app. Say yes! You can still use Signal to send cleartext messages to contacts who don't use the app, and you won't miss messages.

If you do integrate your SMS with Signal messages, you can always long press on the send icon to send cleartext messages to other Signal users (useful when you don't have data but do need to communicate by text.)

### Additional privacy and security settings

iPhone users: click the white settings gear in the upper left corner to access privacy settings for Signal

In the Privacy tab, you can see and change:

- Numbers you've blocked
- Whether or not to show message previews when you switch apps.
- whether or not you want Signal calls to be integrated with iOS calls (shown on lock screen, show caller's name and number, show in the phone's call history)
- whether or not to relay calls through Signal's server to avoid revealing your IP address to the person on the other end (which can reveal your location).
- You can also clear all history logs in Signal (all messages, attachments, call history)

In the Notifications tab, you can select whether or not to show the sender's name and message, just the sender's name, or no name or message in your push notifications.

You can also decide **how long to keep messages** after you've read them.

- Select a name in a conversation, which will bring you to the contact information and conversation settings.
- There you can enable a setting called "Disappearing Messages," which allows messages to disappear after they have been read. You can set the timer to any length from 5 seconds to 1 week.

### Activity: 10-15 minutes

#### Verifying contacts and sending messages

- Ask participants to pair up with a neighbor and exchange phone numbers.
- They can practice finding a contact on Signal, sending a message, setting it to disappear, and verifying that it was sent securely. (On Android devices, they will see a lock icon and a pair of checkmarks. On iPhones, messages will simply display the word "sent" and "delivered")
- Each participant should practice Verifying one another's Safety Numbers. The EFF has a nice walk-through of that process for [Android](#) and [iOS](#).
- If users are not in the same space, they can check verification numbers using a separate channel, such as a phone call, iMessage, Facebook message, Twitter DMs, etc.

#### Sending documents

- When composing a message, users can click the paperclip icon to attach photos, videos, gifs, and documents to a message. Sending attachments through Signal is secure and encrypted, and does not automatically save a copy to the mobile device.

## Creating group chats

- Pairs should pair up in groups of four to set up group chat. A mix of OSs helps here but isn't necessary.
- To create a group chat, select the Compose icon, then select the Group icon.
- Name the group chat, then add multiple contacts who are also Signal users.
- Android users will immediately see who else is in the group and what the group is named, even before you send the first message. iPhone users may not.
- You cannot delete a group once you have created it, but any member can leave the group at any point.

*Note: we'd love to know what kinds of questions come up for participants when you lead this session. Feel free to [submit an issue](#) and share your experience.*

## Wrap up

Remind participants that each conversation is only secure as the most insecure member of the conversation. Signal is a tool that has good options to protect both sides, but if a journalist is using Signal with a source who doesn't have a secure passcode or has left message previews exposed on their lock screen, the conversation may still be exposed.

Similarly, the journalist should take as many steps and precautions as possible to protect their sources by encouraging their sources to read guides on using Signal (such as this one, or the ones linked for trainers above).

## 6.4.4 Recommended Reading

### Links in the news

- [How To Keep Your Chats Truly Private With Signal](#)
- [Martin Shelton on Signal for Beginners](#)
- [Cybersecurity for the People: How to Keep Your Chats Truly Private With Signal \(The Intercept\)](#).

### More great lesson plans

- [EFF's Security Education Companion, on How to Install Signal](#)

## 6.5 Backing up your mobile device

### 6.5.1 Overview

Creating regular, secure backups of data on your mobile devices is important, whether you want to protect against loss, theft, or catastrophic user error (eg. accidentally wiping your device while encrypting it). This session will cover the creation of encrypted backups for iOS and Android users, and make recommendations on a backup schedule. Even if you don't get on a regular schedule, you should always backup your phone before you make any major changes to it.

Getting everyone started backing up their phones is a great way to make sure everyone leaves a workshop with something solidly accomplished.

## 6.5.2 About This Lesson Plan

**Review date:** Dec 5, 2017 **Lesson duration:** This should take under an hour. **Level:** Introductory

### What materials will participants need?

Any phones or tablets they want to back up.

### What materials will the instructor need?

#### Links in the news

- BuzzFeed's Nicole Nguyen has a nice [round up of backup apps](#)
- Hackers Stole My Life by [Mat Honan on Wired](#) is a great lesson in the perils of cloud backups.

## 6.5.3 Lesson Plan

Read [EFF on Harm Reduction](#) – it's an important perspective to keep in mind here. And remember that it is better to acknowledge it when you're [out of scope](#), than to bluff or share bad information.

Everyone should take stock of what is actually on their phone that isn't already backed up. Most folks are syncing calendars and contacts with [Nextcloud](#) or Google or iCloud or iTunes already, but if anyone isn't, start there.

Have everyone go through the apps installed on their phones (this is also a fine time to think about deleting apps you don't use). Some things, like email, are easily restored from settings, but if you know you're going to do a hard reset on your phone, take a moment to make sure you have a record of those settings.

- Social Media (eg. Tumblr, Twitter, What's App) is easy to restore if you know your login information.
- Email often requires you to know a few settings.
- Two Factor Authentication can really throw you – if you're using 2FA open your authenticator app and make sure that you have backup codes for every service listed. If you aren't, make that sure that's one of your next sessions. :)
- Photos might be backed up automatically but if you'll be devastated to lose them, consider copying them to a hard drive somewhere.
- Podcast subscriptions probably aren't dire, but you can usually export an OPML that will make it easy to restore your subscriptions after a reset.

As other things come up, add to this list. Does the app contain data or settings that need backing up? What's a good strategy for making that backup happen?

Note: we'd love your help expanding this lesson. Consider filing an [issue](#) or pull request if there are valuable backup points that you think belong here.

### Automated Backups

By default, Android phones back up quite a bit of data to Google, iOS phones to iCloud. These baked in cloud backup services are far and away the easiest way to make sure that your contacts, photos and calendar are backed up someplace off of your phone. However, commercial cloud backup services are not a good fit for everyone. Commercial cloud providers may not be willing or able to fight a subpoena for contacts you've backed up to their server.

Where you back your work up depends a lot on your values and threat model. For some folks, the risk of losing all their data outweighs their discomfort with or handing over evermore personal data to Google or Apple.

Setting up and hosting your own service ([Nextcloud](#) or [ownCloud](#) are good options if you want to go that route) is not a trivial undertaking. Keeping up with updates and ensuring that your server is configured securely are all you as the host. You can also [pay someone to maintain Nextcloud for you](#).

Users should make a conscious decision about their own needs and values: if you're fine backing up to Google or iCloud, then go for it. If you'd rather backup to them than lose all your data, then go ahead and make sure things are getting backed up while you work on setting up a more perfect solution. And if you'd rather risk losing your contacts than backing up to a Google or iCloud, at least take a moment to export your data and back it up manually from time to time.

Some folks like to start over with a clean slate from time to time – they're fine not backing up at all.

Everyone's backup strategy is going to be different. Your goal is to find a strategy that you'll actually stick with, and that suits your values.

## Android Users

In addition to backing up to a cloud or web-based service, Android users can back up directly to a laptop or desktop via USB. Just watch out for power-only USB cables that don't support data transfer. You should see a prompt inviting you to allow file transfer when you connect your phone to your laptop via USB – it might be labeled “MTP” or “FTP”. Once you accept that, your phone should mount as a drive on your laptop. If you're going to make a one-off backup like this, especially if you're going to be resetting your phone consider also . . .

- Export your contacts to a .vcf file (Import/Export is one of just four menu options) and back that up.
- Most podcast apps will let you export an OPML file so you can restore your subscriptions.

## iOS Users

*You can help us make this lesson stronger by [contributing](#) insights on backup strategies for iOS users.*

# 6.6 Connected App Hygiene

## 6.6.1 Overview

Overview: Don't let orphaned apps degenerate into an unlocked back door to your account.

## 6.6.2 About This Lesson Plan

**Review date:** October 9, 2017 **Lesson duration:** 30 minutes

### Level

Introductory. This is a great exercise to do as a group. Sometimes people need to convene and be reminded together to do this little bit of homework. This could also be a great icebreaker to a longer and more challenging lesson – everyone will leave knowing that they got something done! Think of it as an install party, for uninstalling.

### What materials will participants need?

Everyone should have their laptop.

### What materials will the instructor need?

You want some way to share links with folks. <https://etherpad.opennews.org/> is handy for that, or you can send out this URL in advance.

### How should the instructor prepare?

Review the recommended reading.

Take stock of any social networks that your own office is active in that aren't on this list and find the privacy settings and connected apps for that network. Consider [filing an issue](#) or pull request if those instructions should be part of this lesson plan.

### 6.6.3 Lesson Plan

Imagine that every time you gave someone a key to your place – an overnight guest, a contractor, a cleaning service – that key continued to work even after you changed your locks. And imagine the last contractor you gave your keys to hung it on a board full of keys, with your address on the tag. Picture the contractor throwing a party in their shop. Or quitting the contracting business and opening a bar without ever clearing up that key wall. Abandoning the whole warehouse to go find themselves at Naropa. Those are your connected apps. Side doors to your social media accounts that stay open, even if you change your password.

Even if you have great password policies and two-factor authentication in place, you might be vulnerable to some hacks if you've left old apps connected to your social media accounts.

So go through the apps connected to your social media accounts and make sure that they're all things you're still using. Disable anything you aren't using anymore. Be ruthless.

#### Google

- <https://myaccount.google.com/permissions?pli=1>

#### Twitter

- <https://twitter.com/settings/applications>

#### Facebook

- <https://www.facebook.com/settings?tab=applications>

#### Github

- <https://github.com/settings/applications>
- <https://github.com/settings/apps/authorizations>
- <https://github.com/settings/installations>

## What's Missing?

It is worth taking a moment to take a look at any additional social networks that you're active on but aren't on this list. Look around in the privacy settings and tweak them as appropriate.

## Bonus: Recognized Devices, Cookies, Keys

This is also a good opportunity to explore the “recognized logins” section of each platform. Even though old logins and expired keys are less likely to serve as a vector for an outsider, it's a great opportunity to spot any suspicious logins or behavior.

### Github

- Active sessions: <https://github.com/settings/security>
- SSH keys that grant access to your account: <https://github.com/settings/keys>
- Email addresses on file: <https://github.com/settings/emails>

### Facebook

- General privacy settings: <https://www.facebook.com/settings?tab=privacy>
- Active logins: <https://www.facebook.com/settings?tab=security&section=sessions&view>

### Twitter

- Privacy settings: <https://twitter.com/settings/safety>

### Google

- Active sessions: [https://myaccount.google.com/security?utm\\_source=OGB&utm\\_medium=act#activity](https://myaccount.google.com/security?utm_source=OGB&utm_medium=act#activity)

## 6.6.4 Recommended Reading

### Other Great Tutorials

- How to Geek
- Better Cloud

### Links in the News

- The Google-phish-that-was-also-a-worm – what happened and what to do (Naked Security)

## 6.7 Passwords and Password Management

### 6.7.1 Overview

Passwords are the bedrock of account security, but hard to get right. This lesson provides a methodology for understanding how to take a harm reduction approach to password management. Participants should have a clear understanding of [phishing](#) and [two factor authentication](#), or you should cover those topics with Password Management.

### 6.7.2 About This Lesson Plan

**Review date:** Oct 5, 2017 **Lesson duration:** Variable, depending on objectives and time available:

1. Overview, basic introduction, and securing primary email: **30 minutes**.
2. Strategies for protecting secondary accounts: **30 minutes**.
3. Setup and use of password managers: **30 minutes**

#### Level Introductory **Preconditions**

#### What will participants learn?

Participants will learn how to protect their online accounts, and how to understand the risk associated with compromises of those accounts. At a minimum, participants will learn how to choose a secure password, and use that skill, alongside two-factor authentication, to secure their primary email account.

They will also learn strategies to minimize possible exploits associated with reuse of passwords, including the use of delegated authentication and password managers.

#### What materials will participants need?

Their own laptop and (optionally) their phone.

#### How should participants prepare?

Read Martin Shelton's Medium piece, [Journalists, You Are Worthy of a Data Breach](#).

#### What materials will the instructor need?

A projector would help, but isn't essential.

#### How should the instructor prepare?

Read EFF's essays on [Harm Reduction](#) and [Knowing When You Are Out Of Scope](#) – both are particularly relevant to this session.

1. Get participants to tell you how they currently manage low-stakes passwords (eg. your Wordpress login, or your Walgreens Photo login). Most have a lot of logins saved in their browser – find out which browser.
2. Talk to IT: If you're working with a group in a single office, does their IT department have a preference? Anything they explicitly ban? Some organizations want staff to use a preferred solution for work passwords.
3. Take your own medicine: configure a strong password and two-factor authentication for your primary email account.
4. If you're going to recommend a password manager make sure you try installing it across the platforms in use in your office, which might include MacOS X, Windows, Ubuntu, Android, and iOS. Even if you've been running the tool for a while, walking through a fresh install will help avoid surprises in the training.
5. Read the lesson plan and think about how you want to structure sharing these core concepts with participants.



A deeper understanding of threat modeling, the high-level mechanics of delegated authentication, password hashing, and encryption would also be helpful, though is by no means essential.

This is a lesson where it is very important to make sure that you, as the instructor, aren't making things up or sharing bad information with participants. So be very clear and honest about what you don't really know.

**Harm Reduction** - a guiding principle of this lesson is that people will *not* use passwords properly, they will not store passwords securely, they will forget passwords, they will lose passwords, they will sign up for services that do not store passwords securely and those services will be hacked. The goal of this exercise is to *reduce the harm* that individuals (and the teams they work with) experience *when* (not *if*) things go wrong.

This is not a workshop that can guarantee that users will adopt strong, unique passwords and strong two factor authentication in all situations. Not only is that goal unrealistic, it's counter-productive because it's an overwhelming goal for most people, and when people are overwhelmed they're more likely to give up. The reality is that if a good approach to passwords is used in just a few key places, a majority of the benefit and protection can be gained.

### Basic Digital Literacy (Accounts and Encryption)

There's a lot of history and context to understanding *why* we have passwords in the first place, and too often this bit of digital literacy is missing. What it comes down to are two models of use for passwords:

1. Service authentication - so a service can confirm that you are who you say you are
2. Encryption - a key to unlock a secret lock



In the first case, a service has some data that's associated with you. Because there's no way to identify "you" on the internet, that data is normally tied to your email address. To gain access, the most common approach is to prove that

you (1) know the password associated with your email address on that service or (2) have access to your email (and can then reset the password).

In the second case, the password is a mathematical key – there’s only one key to unlock the data, and using the key doesn’t prove anything about the identity of the person using the key, only that they have the key.

### Password Security (A Harm-Reduction Approach)

No one cares about passwords. No one should need to care about passwords. Passwords are never a means to an end, they’re a hurdle between us and the thing we want to do.

There are a few strategies that can be applied incrementally to increase personal security and simultaneously reduce friction to “doing the right thing.”

There are two hard and fast rules:

1. Password security does not need to be uniform. For most people, strongly securing your primary email address(es) will provide the biggest benefit for the least amount of effort.
2. Passwords should never be reused.

And even rule #2 is not really that hard and fast: every security expert has a go-to password for those IDGAF moments – hobbyist forums or your login to the local parents group – forums where the worst case scenario is that someone uses your login to post spam or malicious content in your name.

You’re always better off if you don’t re-use passwords, but if you’re going to re-use passwords, you can probably safely use the same password for your neighborhood parents newsletter that you use on a game forum.

Lead a brief brainstorming exercise with participants to come up with different “classes” of accounts where reusing a password might be ok, so that they can think about the different security properties of those accounts in a concrete way. Some categories that they might come up with are: online shopping, games, discussion forums, commenting accounts on blogs, and so on).

## 6.7.3 Lesson Plan

### Introduction

Start with a discussion of why we should care about passwords, and some of the consequences of getting them wrong. Martin Shelton has a [great writeup](#) as a starting point – we recommend asking folks to read it in advance.

Your discussion should cover these bases:

1. What passwords are for.
2. This system isn’t perfect.
3. Establishing a hierarchy.
4. Choosing and using a strong password.

### Secure Your Primary Email Account

Email is used by 99.9% of services as a password-reset mechanism, which means that if someone can gain access to your email, they can gain access to just about every other account you have. Because email is almost always the weakest link, securing email accounts is the absolute #1 priority for everyone. Thankfully, it’s easy!

## Choosing a Strong Password

We'll get to password managers later, but an email account is the main thing that someone will always need access to. For that reason, everyone should have a password that they remember *without writing it down* for their primary email.

[Security in a Box](#) includes a great segment on [secure, unique, and memorable passwords](#) – this section is really an exercise in how to choose a password, and some of the reasons *why* it's important to choose a strong password.

1. Computers are really good at quickly guessing passwords (think millions of attempts per second).
2. Modern storage means that lists of most passwords ever used, plus likely combinations are stored and available for download online.
3. If someone can guess your password, it's the easiest way to access your accounts, and the hardest to detect.

There are a few useful rules-of-thumb for choosing a password:

1. Make it long – the longer the password, the harder it is to crack.
2. Make it complex – the more variation of characters you use, the harder it is to crack. Use punctuation, non-latin characters, and numbers in addition to upper- and lower-case latin characters.
3. Make it practical – a password isn't helpful if you can't remember it.
4. Don't make it personal – don't use personally identifiable information (eg. family names, birthdates) in your password.
5. Keep it secret – never share your password. A password must be a secret between you and the service you use it on. This is especially true for your email password. Never, ever share your email password with anyone, and never use it on any other sites or services.

The strategy we'd recommend is to come up with a short password based on a memorable phrase. To quote Tactical Tech:

Passwords can also take advantage of more traditional mnemonic devices, such as the use of acronyms. This allows long phrases to be turned into complex, seemingly-random words:

'To be or not to be? That is the question' becomes '2Bon2B?TitQ'

'We hold these truths to be self-evident: that all men are created equal' becomes 'WhT2bs-e:taMac='

'Are you happy today?' becomes 'rU:-)2d@y?'

These are just a few examples to help you come up with your own method of encoding words and phrases to make them simultaneously complex and memorable.

\* DISTRACTION ALERT: Many participants will have heard of some other strategy for developing a strong memorable password. As long as your password is long, practical, and complex, you're good. Don't get lost comparing password strategies or sharing stories.

**Activity:** Everyone should come up with a secure password and change their email password so that it is strong and secure.

Links to change passwords for common email providers:

Google: <https://www.google.com/settings/passwordchange>

Hotmail: <https://account.live.com/password/change>

Apple iCloud: <https://support.apple.com/en-us/HT201355>

### Keeping that Password Secure

If you force yourself to type your email password every time you check your email, you'll do a much better job of remembering your password. But a strong password isn't enough to keep your email safe. You also need to enable [two-factor authentication](#). If you haven't already covered 2FA, do it now.

Slightly trickier is securing other central services. The same basic rules apply: secure, unique password plus 2FA. Examples of these services include: Apple ID (for participants with iPhones, iPads, or Macs), Google Account (especially for Android, even if not using Gmail), Facebook, Twitter, WhatsApp, Signal.

**Activity:** Have participants brainstorm a list of these “primary accounts” that offer special access to their phones, messaging, etc.

Either have everyone set a secure password and enable 2FA or have everyone make that list and assign password resetting as homework.

### Never, Ever Reuse Passwords

If you reuse the same password all over the place, you run the risk that one service's poor password management will compromise all of your accounts. Troy Hunt's [Have I Been Pwned?](#) is a great resource for tracking database breaches to see if your username or email address is included in the latest batch of pwned accounts. It's also a great teaching tool for your participants - chances are, at least one of their email addresses is listed for at least one service. If they are, and they reused a password for that service, their other logins are also at risk.

The challenge is that **not** reusing passwords is really inconvenient. So there are a few strategies you can use to avoid worrying about it:

#### Option 1: Password Manager

Using a password manager is the most secure approach. It is also the most unwieldy, and it isn't without tradeoffs. Martin Shelton has a [great roundup of password managers](#). You want a password manager that will keep your passwords accessible if you lose access to your primary computer, but won't store them in plain text or make them available to anyone who shouldn't have them.

Martin's review covers LastPass, 1Password, and KeePass, all of which are excellent solutions. Note that if you go with KeePass, [Martin Shelton's installation guide](#) is the best way to get it running on OSX.

Some people think password managers are annoying and terrible. Some people genuinely love them. They are not a silver bullet. As a trainer you should share what works for you, but make sure participants understand that your preferred solution isn't their only option.

**Activity:** Installing a password manager together. As the trainer, you should pick one and have everyone install the same one. Have everyone ...

1. Export their saved browser passwords. There's a [good Firefox plugin](#) for this, in Chrome users should be able to go to `chrome://flags/#password-import-export`.
2. Install the password manager that you've decided to focus on.
3. Set a strong password for the password manager vault.
4. Decide where to store the vault.
5. Import their stored browser passwords and ...
  - delete them from the browser
  - disable password storage

1. Add a browser plugin to integrate the password manager with their primary web browser.

Now everyone is in a good position to use the password manager as their primary password repository for a while and decide whether or not it is a fit.

*Note:* The password manager exercise might seem like a good opportunity to change *all* their passwords to secure unique passwords, but this isn't typically practical in the time available. We recommend starting by just moving from your current system (which is probably a combination of sticky notes and passwords saved in the browser) to a password manager, and focusing on changing key passwords. Once they have a password manager set up, people can replace old passwords with more secure versions as they use them.

### Option 2: Use Your Inbox

Remember that we're taking a harm reduction approach here. Some people just won't use a password manager. If you already know your team isn't on board, or if folks try a password manager and confess that it didn't stick, this is a slate of "good enough" strategies:

1. Have everyone strongly secure their primary email account. If you only do one thing, do this.
2. Encourage everyone to use single sign on wherever it is available (This is "Sign In With Google" or "Sign in With Facebook"). If you have secured your single sign on account, this is a good option. Click approve the first time, any subsequent login is automatic but **still secure**. Note: make sure every one knows how to watch for the difference between using Facebook or Google to sign in and giving an app or service permission to access your Facebook or Google data. Sign-in With Google is totally secure and fine, but be very careful about what other access you grant apps that are using Google Sign-In. Don't just "click okay" and accept whatever access they are asking for. (Note to trainers: consider covering [Mobile Security Settings](#) to ensure that participants understand this.)
3. Use the "reset my password by email" link. It's very secure (almost as secure as single sign-on) and as long as you don't use a weak or reused password to start, it guarantees that no-one will be able to sign in as you later without access to your account.
  - Use a random password and don't save it! Especially for sites you don't visit often, just using a throw-away password can be the most secure thing.
  - Use a password manager to generate a password; if you can reset the password later with an email link, then you don't need to worry about the password manager backups, etc.

More notes about harm reduction: Many security experts will recoil at this strategy. They're right: password managers are far more secure, but this is a viable backup option for those who can't or won't use a purpose-built password manager.

Participants should take stock of all the points of entry to their email inboxes: are messages stored locally on their phone or laptop? Will someone who accesses their laptop or phone have access to all of their account information? Remind participants that this strategy is good enough for most threat models but won't protect them from police search, for instance.

### Follow Up

- Homework: if you assigned 2FA or password resets as homework, be sure to send everyone a follow up note reminding them to DO IT.
- Remind everyone to disable stored passwords and set up the password manager on their secondary computer and on their phone.
- Remind everyone to take stock of whether they're still using their password manager. If they are, a week out is a good moment to look at all the other places

## 6.7.4 Recommended Reading

### Password Dumps in the news

- <https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>
- <https://www.buzzfeed.com/blakemontgomery/one-billion-more-yahoo-accounts-have-been-hacked>
- <https://www.wired.com/story/yahoo-breach-three-billion-accounts/>
- <http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/>
- <https://haveibeenpwned.com/>
- [http://www.espn.com/mlb/story/\\_/id/13089501/report-fbi-investigating-st-louis-cardinals-hacking-houston-astros-database](http://www.espn.com/mlb/story/_/id/13089501/report-fbi-investigating-st-louis-cardinals-hacking-houston-astros-database)
- <https://www.accessnow.org/doubleswitch-attack/>
- <https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118>
- <https://www.csoonline.com/article/3266607/password-security/1-4b-stolen-passwords-are-free-for-the-taking-what-we-know-n.html>
- – Twitter discovered 336 million passwords stored in plaintext (that is, not encrypted) on an internal server. They don't think that anyone actually accessed the password list, but the announcement is a good reminder that re-using passwords is a bad practice, precisely because you can't assume that services outside your control are storing your password responsibly. (Wired, May 2018)

## 6.8 Two-Factor Authentication

### 6.8.1 Overview

Enabling two-factor authentication (2FA) is one of the easiest steps you can take to protect your online accounts. Even if someone gets ahold of your password, 2FA will ensure that they can't get very far. 2FA adds extra protection by requiring additional information for login, provided by either a text message to your phone, a code from an authenticator app, or the use of a hardware security key.

This lesson plan will introduce key concepts about 2FA, and guide you through the process of setting up app-based 2FA for your primary email account.

### 6.8.2 About This Lesson Plan

**Review date:** Dec 2017 **Lesson duration:** 30 mins (estimated) **Level:** Introductory.

**Gotcha:** Make sure participants have a reliable strategy for keeping backup codes, so they don't get wholly locked out of their accounts.

**What will participants learn?** Participants will set up an authenticator app and 2FA on at least a few services and will learn how to use it.

**What materials will participants need?** They'll need their mobile devices (iPhone or Android) and laptop computers.

**How should participants prepare?** Have participants read [Two-Factor Authentication for Newsrooms](#) and [The 12 Days of 2FA: How to Enable Two-Factor Authentication For Your Online Accounts](#)—both are good overviews of the process.

If folks will be sharing unreliable wifi (eg. if you're at a conference center or hotel) encourage folks to install your preferred authenticator app in advance of the workshop. Make sure to include install links for iOS and Android versions in your pre-workshop communications.

### What materials will the instructor need?

EFF's [Two Factor Authentication Handout](#) is a great resource to provide to participants.

### How should the instructor prepare?

- Read through the lesson plan.
- Set up an email account to use to demo 2FA—a secondary or dummy gmail account is a good option for this.
- Read the two recommended participant readings.
- If you're unfamiliar with concepts in the lesson plan, the recommended readings at the end of this lesson are an excellent way to build your own knowledge store. You should also review the [phishing](#) lesson and recommended readings—they'll help you articulate the importance of 2FA.
- If you're working with a larger organization, check with their IT team to find out if their organizational email supports 2FA. It may not be supported—or they may require and enforce it already. Either way, you'll want to tailor your conversation to their circumstances.
- If possible, check with participants to find out their primary email provider (Gmail, Hotmail, corporate, etc.). The lesson plan covers setting up 2FA for Gmail—you may need to review instructions for other providers beforehand based on the needs of your participants.

### Followup Opportunities

When you follow up after the workshop, remind folks to confirm that the spot they stowed their backup codes still makes sense, and remind them to follow through on enabling 2FA on any services they didn't get to in the workshop.

[Twofactorauth.org](#) and [TurnOn2FA.com](#) are great followup resources to share.

## 6.8.3 Lesson Plan

### Discussion

If someone gains access to your primary email account, they can easily use that access to reset passwords and take over your other accounts. Two-factor authentication (2FA), along with [strong passwords](#) and alertness to [phishing](#), will go a long way towards protecting your online accounts. So have everyone start by identifying their primary email account and setting up 2FA there. Single Sign-On (SSO) accounts, used for logging into multiple services, are also a high priority. Common examples of accounts used for SSO include Google, Facebook, Twitter, and Github. If someone is able to take over your Facebook account, that may give them a back door to all kinds of other accounts and services.

Note: it's easy to get lost in a “is this really going to happen to me?” spiral, or a “sure, but what's the worst that could happen” discussion. Some clarity about what is at stake is certainly valuable but it probably isn't useful to get to caught up in horror stories. Remind folks that 2FA is relatively straightforward once it is part of your workflow. You can either get in the habit of carrying your keys and locking the door behind you, or you can stop and think everytime you leave the house “Have I left anything valuable out? What are the odds that someone will break in today?” [Mat Honan](#) lost a lot of personal archives because some hackers wanted his Twitter handle. For a while hackers were doing a good job of taking over email accounts to send out desperate pleas for money—“Help, I'm traveling and I was hit by a car and I can't reach my parents, but I desperately need you to wire \$400 to this random stranger so I can pay my hospital bill and come home.”—even though the apparent sender was safe at home. If you work in a newsroom with someone working on sensitive investigations, if anyone who trusts you is doing sensitive work, you owe it to them to ensure that you're not the vector for an attack.

There's very good reason to believe that the Clinton email hack was made possible because [John Podesta didn't have 2FA turned on](#). Don't be John Podesta. He fell for a spearphishing scam that told him he needed to change his password. With 2FA enabled, just knowing his new password wouldn't be enough to give a hacker access to his emails.



It's also possible for passwords to be exposed in error, rather than maliciously. In May 2018, [Twitter asked all of its 336 million users to change their passwords](#), after discovering that they had been written in plaintext to an internal log. Without 2FA enabled, users risked their accounts being accessed by anyone with access to the log. With 2FA, they had an extra level of protection.

Common services include:

- Email: everyone should have 2FA on their primary email account.
- Online banking: banks usually require 2FA, but if your bank makes it only optional, definitely turn it on.
- Backup and file sharing services (eg. Dropbox)
- Developer tools (eg. Github, AWS)
- Social media networks (eg. Facebook, Twitter)

Folks should brainstorm other services that they want to prioritize and start setting them up. [Twofactorauth.org](#) is a useful roundup of services that do provide 2FA, while [TurnOn2FA.com](#) has great instructions for many of those services.

**DO:** Demo adding 2FA to a Google or Github account, by setting it up, walking through the process of printing recovery codes, and then using it. Flag for everyone that setting up 2FA can mean they'll be permanently, irrevocably locked out of their account if they lose access to their 2FA device, so everyone should absolutely store backup codes somewhere safe.

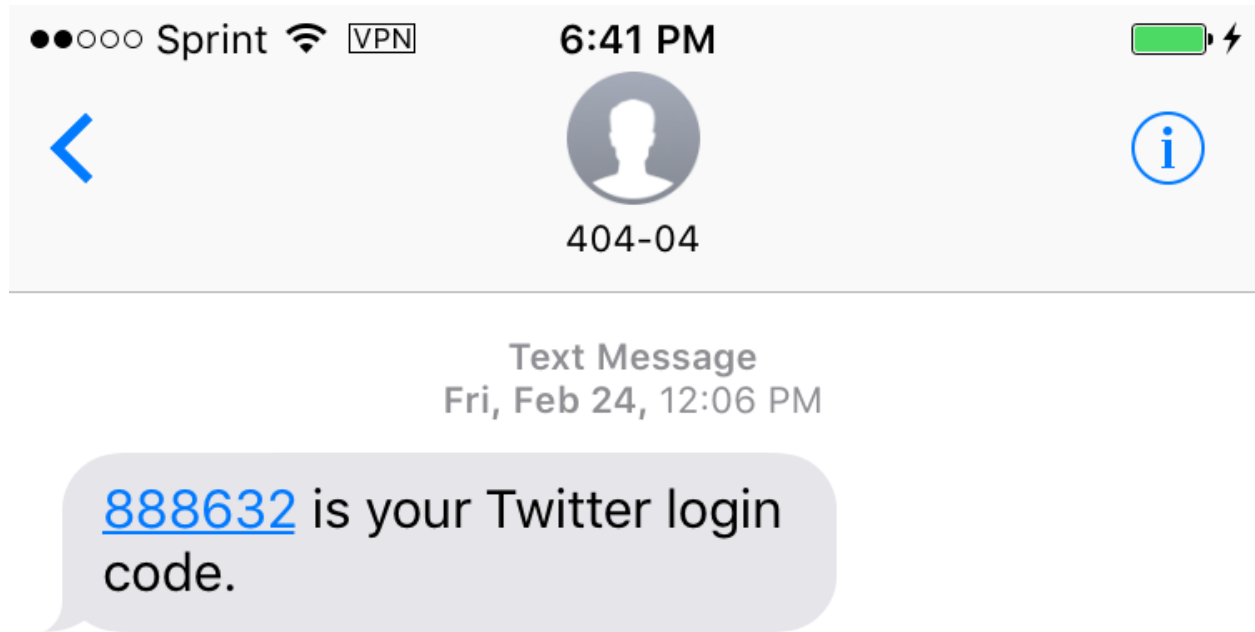
Unless you know everyone is using YubiKeys, have everyone download [Authy](#) or [Google Authenticator](#) now, while you discuss the tradeoffs of the three most common authentication methods.

**DISCUSS:** There are a few easy, widely supported approaches for adding 2FA to your accounts:

- SMS text messages
- Authenticator apps
- Security keys

**Least Great Option - SMS Text Messages:** Most services allow you to receive an authentication code via text message. SMS codes are super convenient but also vulnerable.





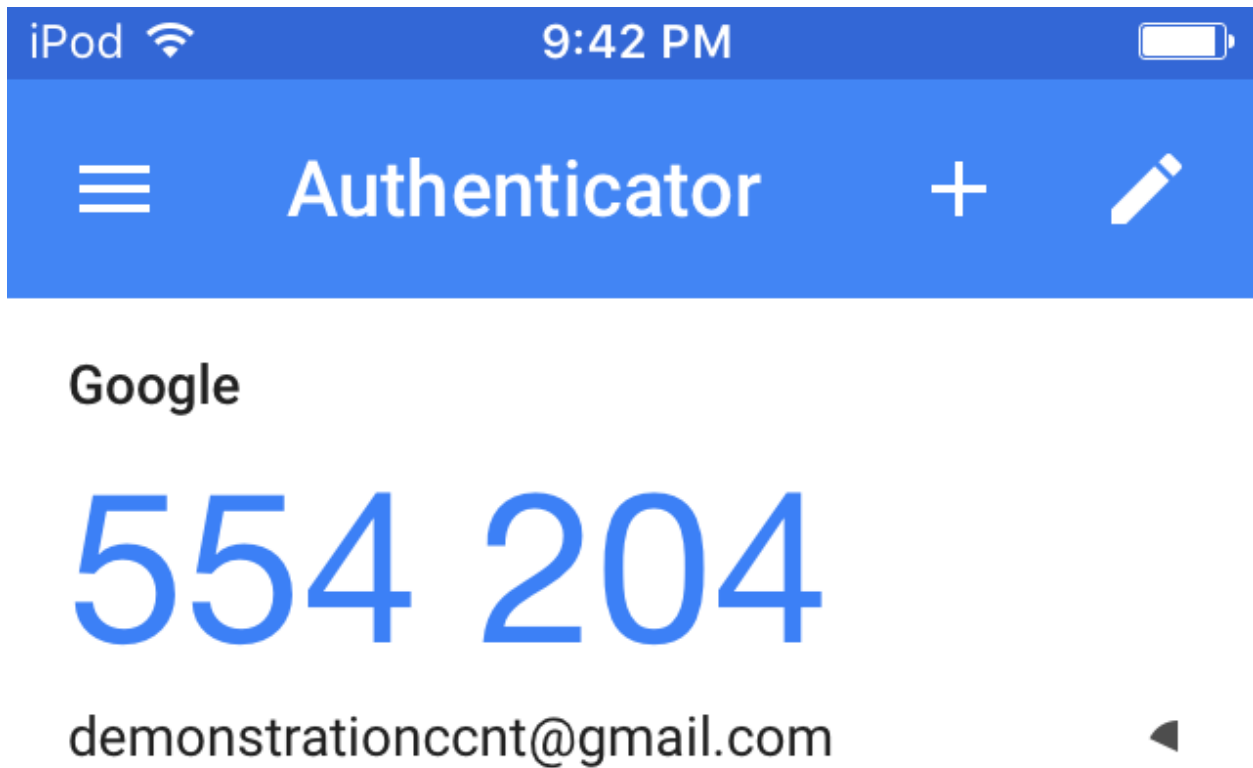
SMS-based 2FA is better than using a password alone, but relying on telephone infrastructure comes with enough trade-offs that the National Institute of Standards and Technology [does not recommend it](#). However, if SMS-based 2FA is your only option, using it is better than not using it.

For example: by convincing Verizon to redirect Deray McKesson's phone messages to a new SIM card, a hacker was able to bypass 2FA. They were able to access the Black Lives Matter activist's email and Twitter records.



SMS-based 2FA is better than nothing, but it isn't a great option.

**Better Option - Authentication Apps:** Some services allow you to receive your 2FA code from a mobile app. There are many options to choose from, including [Google Authenticator](#), [Authy](#), and [Duo Mobile](#).



Some web services let you attach multiple authentication apps to the same account, which can be incredibly helpful when multiple people need access to a single account. Authenticator apps are also great because they work even when you don't have access to your phone network.

Unlike SMS messages, authenticator apps aren't vulnerable to attacks against your mobile network.

**Even Better Option - Security Keys:** A security key is a physical device, usually connected via USB, that you can use to authenticate your account.

They're reasonably cheap — one of the most popular options, a [Yubikey](#) costs \$18.

Using them is easy—you simply insert your security key during login, and physically tap it when prompted.

Security keys are fairly resistant to phishing attacks, making them one of the best options available. Unlike code-based 2FA, phishing sites don't have a great way to intercept information from security keys. Also, Yubikeys generate and store a unique ID for each login on first registration, and check this ID on subsequent logins. If you were to land on a phishing site with an illegitimate URL domain (e.g., [faceboook.com](#) instead of [facebook.com](#)), the ID will not match and the key will not cooperate with the website.

Security keys are not yet as widely supported as authenticator apps, but the standard is getting traction on large websites. Google, Facebook, and Dropbox all support security keys. If you're using Gmail as your email provider, or if you're using any other Google services, security keys are a great option.

Security keys for the Web require [browser support](#). The Yubikey works with [Opera](#) and [Google Chrome](#), and there's a good [workaround](#) for Firefox users.

### Pick One

Encourage your audience to use whichever 2FA method is available and practical. SMS is absolutely better than going without, but you should strongly nudge participants toward hardened options, such as authenticator apps or security

keys. In most cases participants will need to download an authenticator app.

You should have already demonstrated setting up 2FA, but if you didn't, do that now.

Everyone should have downloaded Authy or Google Authenticator by now, but if they haven't, have them do that. Seriously though: it is far preferable to do this during the discussion so you don't overload your bandwidth.

And then have everyone set it up on their primary email account. Have folks look through [TurnOn2FA.com](https://turnon2fa.com) if it isn't obvious how to setup 2FA on their primary email account.

Make sure everyone also sets aside backup codes!

Setting up 2FA should take no more than 10 minutes.

Time to break out the laptops. The instructions below apply to Gmail. If any participants use a different primary email provider, you may need to modify the lesson plan accordingly.

Show everyone how to navigate to the Gmail setup page. From the Account icon (top right) select `My Account > Sign-in & security > Signing in to Google` and look for a `2-Step Verification` option. Click `Get Started`.

**Set up SMS authentication:** First, participants will need to enter their password to verify that they own the account.

Next, participants will have to add a phone number. (Exasperatingly, you can't set up app based authentication without first setting up SMS authentication. At least not on Gmail.)

Once participants have followed the steps on screen to register their phones, they will be able to receive 2FA codes through SMS text messages.

**Set up an authenticator app:** As discussed, we want more security than SMS provides. So once you have enabled SMS based 2FA, have everyone set up app based authentication. They'll have to select "Authenticator App" and then open the authenticator app (probably on their phones) and add an account. They should be looking at a QR code on the screen and a camera on their app.

**Backup Codes:** Now that everybody has 2FA set up, they DEFINITELY need to download backup codes and put them someplace safe. Each backup code can only be used once, but if you lose your phone (or just leave it home one day) and all your authentication is connected to your phone, you're going to be awfully frustrated without backup codes.

**Disable SMS authentication:** After setting up an authenticator app or security keys, participants should remove their phone as a 2FA method.

**Security Keys (optional):** If participants have Yubikeys and want to set them up, they should scroll down to `Security keys` and click `Add security key`. When prompted, they should insert the key into the USB port, and physically tap the gold disk on top.

They'll be prompted to name the newly-registered device. During login, instead of typing in a 2FA code, anyone who sets this up can just insert and tap the key.

Note: Some new computers (e.g., the 2016 Macbook) only have USB Type-C ports. If you can't use a traditional USB 2.0 or 3.0 port, you can still use security keys with a USB Type-C adapter. Here's a short list of [Type-C adapters that are confirmed to work](#). Alternatively, you can purchase a [USB Type-C Yubikey](#).

## 6.8.4 Recommended Reading

- EFF's Security Education Companion has a great [Two Factor Authentication](#) lesson.
- [Two-Factor Authentication for Newsrooms](#)
- [London Calling: Two-Factor Authentication Phishing From Iran](#) from Citizen Lab (Munk School of Global Affairs, University of Toronto) is a good roundup of ways that really good phishing can circumvent 2FA. (August 2015)

- [Phishers rip into two-factor authentication](#), *The Register* also covers some ways that phishing can be used to circumvent 2FA. (July 2006)
- [Text scams: The messages that allow criminals to break into your iPhone, and how to spot them](#), *The Independent*, details another SMS-based phishing attack (June 2016)

## 6.9 Phishing Basics

### 6.9.1 Overview

Many security attacks take advantage of human cognitive bias, using psychological manipulation to trick people into revealing data or acting on behalf of the attacker. These attacks are typically referred to as *social engineering*. *Phishing* is an email-based social engineering tactic that uses misplaced trust to extract information and access. Like other forms of social engineering, its purpose is to trick you (the target) into divulging information that can be used to access to private data, networks or resources. *Spear-phishing* is a form of phishing targeted at a particular individual or group. This sort of attack is widespread, common, and responsible for many [notorious examples](#) of data loss or leakage.

Defending against phishing begins with *awareness* of particular risks and some basic safety *techniques* and can be aided by the use of certain *tools*.

Participants will consider phishing in the context of *trust decisions* and develop awareness and techniques to make these decisions when interacting on the web. Participants will learn the basic mechanics of phishing and spear-phishing, the techniques attackers may use, how to approach online trust decisions, and important, basic techniques and tools.

### 6.9.2 About This Lesson Plan

**Review date:** June 2017 **Lesson duration:** 45 minutes **Level:** Introductory

**What materials will participants need?** Access to the internet.

**How should participants prepare?** Read the introductory articles in the intro email.

**What materials will the instructor need?** Presentation software, sticky notes, pens. A pair of index cards per participant, numbered 1 and 2.

**How should the instructor prepare?** Use outline below to prepare presentation, send intro email.

### 6.9.3 Lesson Plan

#### Part A: A Trust Game

Each participant is given two cards, numbered 1 and 2. On each card, participants should write down a statement about themselves, one true and one false. The statements should not be things other participants already know and should not be immediately verifiable (“I have brown hair” is immediately verifiable; “When I was 12 my hair was purple” is not, unless the group has a very long history together.) The false statement shouldn’t be implausible.

- Post each participant’s sticky-notes a visible place under their name.
- When everyone is done writing down cards, begin the *interrogation* phase. For each participant:
  - The facilitator reads both cards
  - The facilitator starts a 1-minute timer. During the one-minute session, group members ask the participant **yes or no** questions about the facts represented on the cards.

- At the one minute mark, facilitator asks each member of the group to record which card #1 or #2 they think is true.
- *Debrief*: when each participant has been interrogated, the facilitator conducts a debrief. For each participant, the group indicates (by show of hands) which card #1 or #2 they thought contained the true statement.
- *Reflection*: The facilitator may ask the group to reflect how the information obtained during the interrogation affected how they voted:
  - What sorts of questions were useful in making a true/false determination?
  - What kind of context aided in the decision?
  - What kinds of questions were the most revealing?

### Part B: Awareness

Social engineering - the use of psychological manipulation to trick people into revealing data or acting on behalf of an attacker - always involves the manipulation of trust, aided by deception. As the trust game illustrates, we are frequently required to make trust decisions with limited context and limited time. Attackers know this, and take advantage. Social engineering attacks are possible across all methods of communication, including:

- **In-person** impersonation fraud (door-to-door sales people misrepresenting themselves, fraudulent personal identification)
- **Telephone** impersonation fraud: (calling a help-desk phone number to request unauthorized account details or a password reset)
- **Phishing**: impersonation fraud using email

A definition of phishing: an email-based social-engineering attack that uses deception to extract information and access.

#### Basic components of a phishing attack:

- **An email**: the deception begins with an email (or sometimes another message such as an SMS message) containing a call to action. The email will very frequently be disguised so that it appears to be from a legitimate source, with which the subject already has a relationship.
- **A call to action**: the email will always contain a call to action. Typically this is in the form of a link to click on to complete a task or view a document. The call to action is typically designed to appear both urgent and legitimate, and possibly enticing in some way.
- **A harvesting interaction**: clicking on the call to action/link contained in the email will open an interaction—usually but not always a login screen. Like the email, this is generally disguised to appear legitimate, and may attempt to extend the sense of urgency and legitimacy.

#### Example: an urgent alert!

- Urgent subject matter designed to distract from a trust decision. Use of emergency or urgent language is frequent in phishing attacks because it is emotionally distracting.
- Call to action (click here) will require a login. The login form will appear to be legitimate, but instead will harvest the username and password for the attacker's purposes.

Re: Urgent-Important Campus Alert! (Lehigh.Edu) Inbox x



Elizabeth Birks <ebirks@uoguelph.ca>

to ▾

Re: Urgent-Important Campus Alert! (Lehigh.Edu)

Hello,

There's a police situation on campus, we encourage everyone to read and follow protocol.

This message is sent via secured HTML [Click Here](#) to view.

Thanks,  
Richard Nixon,  
Lehigh University

provides a leading-edge library and technology environment that enables flexibility, innovat  
experience, research, administration, community-building and outreach.

Contact Information  
Library & Technology Services  
EWEM Library

---

**Example: a document from a trusted source**

- This email appears to be from the government (a legitimate-looking source).
- In order to open the document, some kind of information or authentication is required, which is the exploit. The document itself may also contain malware.
- Taxes or other financial interactions are frequently exploited by phishers because they may be perceived by their targets as urgent. Freely-available personal data may be included, to increase the chance of deceiving the target.

Your Federal Tax remittance (ID: 57378473347676), recently sent  
from your checking account was returned by The Electronic Federal Tax  
Payment System.

Rejected Tax transaction	
Tax Transaction ID:	57378473347676
Reason	See details in the report below
Income Tax Transaction Report	<a href="#">tax_report_57378473347676.doc</a> (Microsoft Word Document)

Internal Revenue Service P.O. Box 996 Augusta 38914 NY

**Example: brand impersonation**

- What? You didn't just spend \$711 on Amazon? Better click to find out what this is all about ... whoops.
- False transaction reports, when combined with convincing branding, are frequent vectors.





[Your Orders](#) | [Your Account](#) | [Amazon.com](#)

## Order Processing Confirmation

Order #002-5250057-88100666

Greetings @lehigh.edu,

Thank you for shopping with us. We have to inform yo that secondipity shipped your item, and that this completes your order.. If you need to return an good from this shipment or manage other orders, please visit [Your Orders](#) on Amazon.com.

Your estimated shipment delivery date is:  
**Friday, September 21, 2012**

[Why tracking information may be not available?](#)

Your order was delivered to:

539 S Louis Dr , App. 8B  
S Maria, KY  
United States

This shipment have no an associated delivery number of tracking.

### Conveyance Information



Samsung XVT3D23, SV 46-Inch 720p 100 Hz  
Cinema 3D LED-LCD HDTV with 3D Blu-ray  
Player and Three Pairs of 3D Glasses

Sold by onner

Condition: used - acceptable

**\$771.69**

Item Subtotal:	\$771.69
Shipping & Handling:	\$23.99
Total Before Tax:	\$771.69
<b>Shipment Total:</b>	<b>\$771.69</b>
Paid by Check:	\$771.69

Returns are easy. Visit our [Online Return Center](#).

If you need further assistance with your order, please visit [Merchant Contact Form](#).

We hope to see you again soon!

**Amazon.com**

Unless otherwise noted, items are sold by Amazon LLC. Learn more about [tax and good provider information](#).

This email was sent from a notification-only address that cannot accept incoming email. Please don't reply to this message.

**Spear Phishing** The phishing examples so far are cases of general-purpose or mass-market phishing. In contrast, **spear phishing** is a highly targeted variant of phishing that leverages details about the target's life and social connections to intensify the deception. Emails may contain personal messages that **appear to be from friends or colleagues**, and

may even relate to **real events**, issues or other plausible subject matter.

Those who have access to particular information or access that a sophisticated attacker wants are most likely to be spear-phished. Journalists are particularly vulnerable.

*(End Slides/Topics for part B)*

### Part C: Group Sharing

*[Facilitator can pause to offer a chance for participants to ask questions, and to share examples of phishing attempts they've experienced in the past.]*

### Part D: Presentation: Making trust decisions online

**Trust decisions.** When we disclose information, we are making a **trust decision** about the legitimacy, safety and intentions of the party to which we disclose. Defending against phishing requires the development of one **habit** and a set of **techniques**.

**Habit: Every trust decision should be a conscious one** Every time we disclose information online, we grant trust to whoever receives our data; it's better to make these decisions on purpose rather than subconsciously. Developing the mental habit to evaluate the trustworthiness of the recipient of our data is critical to protect against phishing attacks.

**\*\* Activities that imply trust:\*\***

- Submitting an online form
- Clicking on an email attachment
- Replying to an email

**Exercise:** What other activities online imply trust? What would help you to remember to make a conscious trust decision when divulging information online?

**Techniques: Evaluating emails: slowing down, context** Urgency is the enemy of careful decision-making. Even (and especially) when confronted by an urgent email, it is important to **slow down**, and take the time to evaluate the legitimacy of the email.

Another reason to slow down is to avoid clicking on anything (links, attachments, etc.) in an untrusted email until a trust decision has been made.

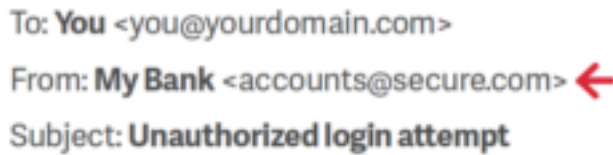
**Sanity check: context.** A first, though not at all sufficient, check on any email is to evaluate whether it is expected or plausible. Is it the result of an activity that we ourselves initiated – for example a transaction that we initiated or expected? Anything that comes as a surprise or out of the blue should be automatically suspect.

**Techniques: Evaluating emails: implicit factors** Answering “yes” to any of the following questions may suggest that the email is not legitimate:

- The email has an unusual “from” address whose domain is not associated with the organization
- The email body contains non-standard or odd-looking formatting
- The email body contains spelling mistakes or unusual grammar
- The formatting of the email differs from other email received from the same organization
- The email contains threatening, overly-urgent or very enthusiastic language

While any of these factors suggest illegitimacy, their absence does not guarantee trustworthiness.

**Techniques: checking the “from” domain** A strong indicator of a phishing email is an unexpected domain in the email's **from** header.



To: You <you@yourdomain.com>  
From: My Bank <accounts@secure.com> ←  
Subject: Unauthorized login attempt

In the above example, the bank has sent an email from an unexpected domain. This is highly suggestive of phishing. Note that you must check the *domain*, and not the display name when checking this.

*Note: “From:” domains are easy to spoof*, and therefore a correct-looking address here doesn’t prove that an email is legitimate. However, an obviously bad address in this space strongly suggests that an email is probably illegitimate.

**Techniques: checking the domain of any links or downloads** The closest thing to a conclusive test for a phishing email is to examine the **domain** of any link it contains. This will likely require checking the HTML markup of the email or otherwise determining what domain the email is attempting to link you to.

Some tips:

- Do not click on untrusted domains
- Look for tricky domains. Sometimes attackers use special, confusingly-similar domains. The domain may only differ from the legitimate one by a single character.
- If unsure, consult the WHOIS record of the domain (you can use the free service at <https://whois.icann.org/en> for instance). Legitimate companies will use public WHOIS records to confirm their actual ownership of a domain.

### Group Exercise: phishing quiz

There are several online quizzes designed to test people on their ability to spot phishing emails. These can be useful for participants as a way to reinforce what they’ve learned so far. Using the techniques described above, take the phishing quiz at: <https://www.sonicwall.com/phishing/>. Take some time to discuss the results as a group.

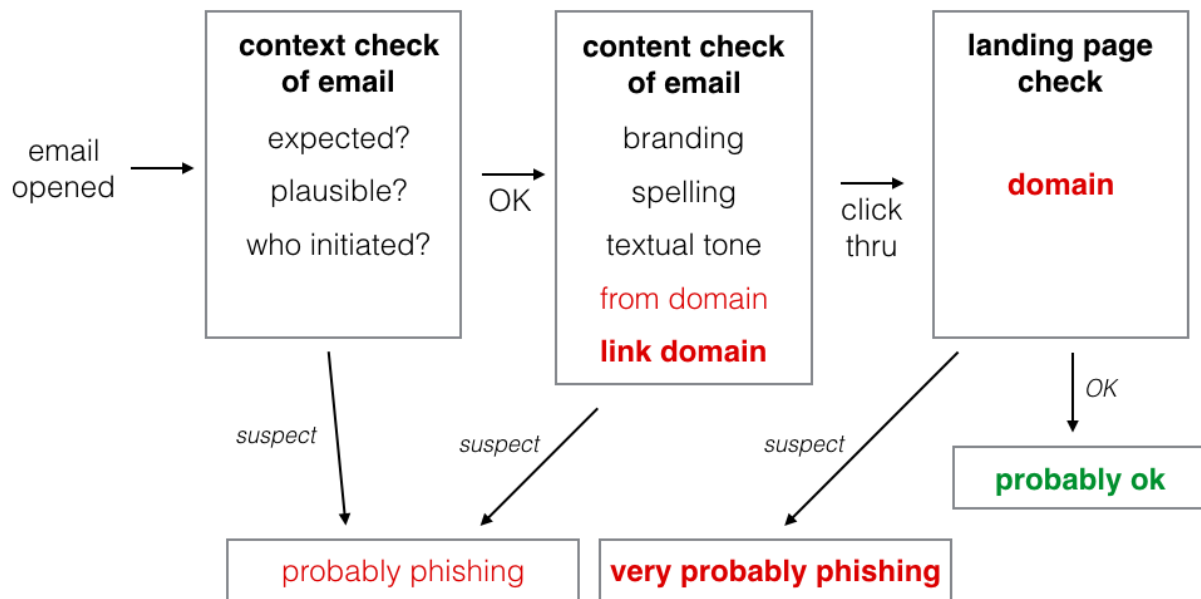
**Techniques: after the click-through: context check** After deciding to click on a link in an email, we have the opportunity to evaluate context again. Questions to ask:

- Was the result of the click what I expected?
- Did the click take me result in an unexpected redirect? Ie: The link appeared to be sending me to domain X but I suddenly find I’m on domain Y.
- Does the state of the page (logged in or not) appear correct? For example, if I’m already logged in to Google in my browser, is the page I’m on asking me to authenticate again?
- Does the link I clicked on ask for any sensitive information? If so, can I verify the request in some way other than email?

**Techniques: after the click-through, check the domain again** Now that we’re on the destination page, we may be confronted by an additional call to action. It’s time to make a second trust decision. Before submitting information, evaluate the domain of the page again according to the same criteria used to evaluate it in the email.

**Summary:** *flow of trust [Instructor can use examples from section B, as well as examples mentioned by participants, to work through the flow diagram below:]*

## trust decisions for phishing



### Recommended reading

#### Links in the news:

- <https://twitter.com/ericgeller/status/944205900138430464> - “Journalists were Fancy Bear’s #3 target, after diplomats and Democrats...”
- <https://gizmodo.com/heres-how-easy-it-is-to-get-trump-officials-to-click-on-1794963635> - Gizmodo sent test spearphishing emails to senior Trump administration officials, and almost half of them fell for it.
- <https://www.buzzfeed.com/sheerafrenkel/russian-hackers-faked-gmail-password-form-to-invade-dnc-email> - Fancy Bear used a fake domain, accounts-google.com, in a spearphishing attack against DNC officials.
- [https://en.wikipedia.org/wiki/Podesta\\_emails](https://en.wikipedia.org/wiki/Podesta_emails) and [https://en.wikipedia.org/wiki/2016\\_Democratic\\_National\\_Committee\\_email\\_leak](https://en.wikipedia.org/wiki/2016_Democratic_National_Committee_email_leak) - Wikipedia’s pages on the 2016 DNC hacks.
- <https://www.welivesecurity.com/2016/04/23/sms-phishing-attackers-continue-pursue-apple-users/> - Social engineering via SMS - attackers used texts to phish for targets’ Apple iCloud credentials.

#### Other resources:

- <https://freedom.press/training/email-security-tips/> - Freedom Of The Press Foundation’s phishing training.

## 6.10 Physical Custody of Electronics

### 6.10.1 Overview

What happens to your data if your device is seized or stolen? How should you prepare to cross international borders safely? This session will talk about ways to approach border crossings, as well as walk through the process of enabling full disk encryption, which can help ensure that someone who has your physical device doesn't necessarily have all your data.

This module makes a few assumptions about your threat model. It is written with American journalists in mind – if your work puts you in conflict with hostile state actors, you should seek out more specialized training.

### 6.10.2 About This Lesson Plan

**Review date:** June 5, 2017 **Lesson duration:** 30 minutes **Level:** Intermediate **Preconditions:** Participants should know how to back up their devices and how to choose a strong passphrase.

#### What materials will participants need?

They should bring their Android / iPhone and laptop.

#### How should participants prepare?

Participants will need administrator access to their machines.

Everyone should read [Digital Privacy at the U.S. Border: Protecting the Data On Your Devices \(EFF 217\)](#).

#### How should the instructor prepare?

Touch base with IT staff to talk through your plans for the workshop – you may need their support in actually enabling disk encryption.

Read through the material carefully and think about what will work for you, as a facilitator and instructor.

Assume that no more than 50% of participants will actually read the EFF guide that you sent around.

#### Follow up

Because most participants will not actually turn on full disk encryption during the session, set a deadline for everyone to do it and then be sure to follow up.

### 6.10.3 Lesson Plan

#### Groundwork

Digital security isn't just about encryption and data and metadata. The physical security of data and devices is also paramount: What happens to your data if your device is stolen? What's at risk if a border agent or other adversary takes your laptop for 30 minutes?

Physical custody issues generally boil down to two categories: permanent loss of your device, and temporary custody.

**Theft or Permanent Loss** You leave your backpack in a taxi. Your laptop disappears from your hotel room. A thief swipes your phone when you're standing on the sidewalk. What are the risks:

*Activity: Have participants spell out their concerns. Capture them on a white board or sticky notes. If someone malicious takes your laptop, what do you need to worry about?*

You're looking for things like:

- Someone else has your documents, password, address book, calendar.

- You don't have them anymore, unless they're backed up.
- Sensitive work information, including documents, e-mails, communication about your reporting, communications from anonymous sources could be compromised.
- You can't do your work because your hardware is gone.

**Seizure or Temporary Custody** Border agents seize your computer, but eventually return it to you. Your laptop is seized in a police or FBI investigation, and subsequently returned to you. You leave your laptop unattended – in a hotel room, or office – and someone tampers with it.

*Activity:* Again, have participants spell out their concerns. Capture them on a white board or sticky notes. If someone malicious takes your laptop, what do you need to worry about?

You're looking for most things from the first list, as well as things like:

- someone can make a complete copy of the disk.
- they can tamper with your device or install malware on it

**So what can you do?** You can mitigate what is available without your permission. But “mitigation” is a key word. You don't know, not really, that it can't be decrypted. The strategies that make sense vary a lot with your threat model. The EFF's [Border Privacy Guide](#) is a great resource – encourage folks to lean hard on it.

- Reduce the amount of data you carry across the border, or don't carry sensitive data across borders at all. This is in some ways the easiest solution, at least as far as border search is concerned. It is also, obviously the hardest.
  - If you have access to a secondary laptop and you're planning a trip, consider taking something other than your primary laptop to use. If you do use an alternate “travel device” and make sure that it doesn't contain your password manager, SSH keys or e-mail client.
  - Do you need a smart phone on your trip? Or would a feature phone with longer battery life meet your needs?
  - Consider backing up, and completely wiping your phone before you leave on a trip. You can restore your device either after crossing or when you're back home.
  - Government authorities in particular, may be able to modify the physical hardware of your device. Restoring software from a backup won't protect against hardware modifications.
- Use a “travel mode”: 1Password offers a [travel mode](#) that won't allow you to access your passwords while traveling.
- Minimize the data available without your permission with full disk encryption, but know that you may not always be able to cross international borders without unlocking a device. The EFF has a good overview of [your rights at the US border](#). *Trainer Note: it is easy to slip into a debate about what the border patrol is likely to do, or a story swapping session about horrible things that have happened. Try to “park” those stories in a “parking lot” for discussion another time.*
- Call a lawyer. If your newsroom has staff attorneys, touch base with them before you travel.
  - Some attorneys recommend telling the border agents that your device contains trade secrets and you're not authorized to authorize a search. That obviously only applies if it is true, but if you have company correspondence or documents on your phone it probably is true.
  - Carry key phone numbers outside your phone: if you find yourself in a situation where you are able to contact an attorney but don't want to power up your phone, make sure you have their number written down somewhere. Business cards are excellent for this purpose.
  - Even if you don't have a staff attorney, do make sure you have someone you can contact if you get into a stand off over your electronics at the border. And make sure that you have their number somewhere analog.

## Walkthrough: Full Disk Encryption

What does full disk encryption protect: disk encryption protects data against being read when your computer is off, or newly powered on.

What does it not protect: if your device is already powered up, the drive is decrypted, even if the screen is locked. Once you enter your passphrase, the disk is decrypted. If someone has your passphrase, either because it was guessable or because you gave it to them, full disk encryption won't protect you.

**Important:** the process of enabling FDE can take many hours, and if you interrupt it you will lose access to everything that was on the disk. So show participants how it works, but **do not have them start the process** until they're sure that a) they have backed up the machine and b) they can live without it for 10-12 hours. Generally that means leaving it over night.

Make sure everyone knows where to find the disk encryption settings on their devices and has a plan to actually enable it when they can do so safely.

### MacOS:

Use [FileVault](#).

In `system preferences > Security > FileVault` you should see a toggle labeled `Enable FileVault`. When you are ready to actually encrypt the disk always write down the recovery key on a piece of paper and store it somewhere safe.

Depending on your threat model, you might want to decline the Apple iCloud recovery method, as it may leave your data vulnerable to state actors.

### Windows (Pro, Ultimate, or Enterprise editions):

Use [BitLocker] [https://technet.microsoft.com/en-us/library/cc731549\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc731549(v=ws.10).aspx).

Users that only have Windows "Home edition" can look into Veracrypt.

### iOS:

iOS has built-in device encryption ([see page 10](#)) – but it is only as good as your passphrase.

### Android:

Options will depend on the Android device. Nexus/Pixel devices have full disk encryption enabled by default, but you can double-check by going to `Device Settings > Security > Encryption` – select `Encrypt phone` to start the process, and be sure to set a strong passphrase.

## Recommended Reading

### Links in the news

- U.S. border agents stopped journalist from entry and took his phones (Washington Post, Nov 2016)
- Department of Homeland Security detains journalist returning from Beirut (The Guardian, July 2016)
- A US-born NASA scientist was detained at the border until he unlocked his phone (The Verge, Feb 2017)



- Secret Service laptop containing Trump Tower evacuation and floor plans stolen (CNN, Mar 2017)
- Privacy Complaints Mount Over Phone Searches at U.S. Border Since 2011
- “Dehumanized” at the Border, Travelers Push Back (Just Security, Feb 2018)
- Digital Privacy at the U.S. Border: Protecting the Data On Your Devices (EFF 217)

### More training resources

- Digital Privacy at the U.S. Border: Protecting the Data On Your Devices (EFF 217)

## 6.11 Scrubbing Metadata from Files- A low-fi approach

### 6.11.1 Overview

Files such as Word documents and JPEG images usually contain information about the systems used to create them. This information, commonly referred to as metadata, could inadvertently reveal personally identifiable details about your sources to anyone given access to the files. Removing metadata from files provided by sources before sharing or publishing them is critical for anonymous source protection.

This lesson plan covers what you’ll need to know to find file metadata in Word documents and JPEG files, and how you can share or publish content from these files without exposing metadata.

### 6.11.2 About This Lesson Plan

**Review date:** June 5 2017 **Lesson duration:** 45 minutes **What will participants learn?** Basic understanding of what metadata is and basic techniques to “clean” common file formats before publishing or sharing. This session does \*not\* cover myriad other types of metadata, most notably the metadata created by journalists and sources when they browse the web, use their mobile phones, or communicate using VoIP, chat, email, etc.

**What materials will participants need?** Email access, a laptop with MS Word installed, access to printer and scanner

**What materials will the instructor need?** Sample document (like a PDF or Word document) and sample image (JPEG or similar format), both with identifying metadata included—such as the name of the Microsoft license-holder, geotag/location data, etc.

**How should the instructor prepare?** Review lesson plan, and share example documents from ScrubbingMetadata folder with participants.

### 6.11.3 Lesson Plan

#### Icebreakers/discussion

Did you know that sharing and publishing files can burn your sources?

Example: Vice and John McAfee: [https://www.vice.com/en\\_us/article/john-mcafee-bath-salts-belize-murder-fugitive-gregory-faull](https://www.vice.com/en_us/article/john-mcafee-bath-salts-belize-murder-fugitive-gregory-faull) - When Vice published the story, the photos still had location data included and basically burned their source.

Example: *How The Intercept Outed Reality Winner* - Reality Winner used traditional mail, not the Internet, to share documents with the Intercept, but was caught due to both operational security mistakes and metadata included in the printed files she shared.

Example: *BBC: Why printers add secret tracking dots* - One mistake that Reality Winner made was to use a color printer to print the documents she leaked. Most color printers add a pattern of yellow dots to any printout, encoding



a unique serial number and the date and time that the printout was made. This is ostensibly an anti-counterfeiting measure, originally used by the US Secret Service to identify the source of fake banknotes, but it's also pretty handy for tracking down whistleblowers who don't take proper precautions.

*[Discussion point: Instructor should ask participants how and when they share documents that they obtained from a source, and what the potential risks are in doing so. Then, if they didn't come up, the instructor should cover the 3 points below. ]*

**Sharing outside the newsroom** When you share or publish information obtained from a source, a good rule of thumb is to only share the minimum amount of information necessary to tell a story. In the most extreme case, for example, simply cutting and pasting document text into a plaintext file effectively removes all digital metadata. There may be cases where this isn't feasible, for example, when you're sharing a document with a third party to verify its authenticity. Even then, simply sharing the original document may expose your source, so it's important to remove any file metadata that you can.

**Sharing within the newsroom** Even for documents not shared outside the newsroom, removing metadata before sharing with colleagues reduces the risk of an accidental or malicious leak of source information.

**Publishing documents with a story** Redaction of information within documents may be necessary before distribution, and it's important that this be done irreversibly. Some document formats include revision histories, others may still contain text that has been graphically obscured. Metadata scrubbing techniques work well here too. More sophisticated methods of watermarking documents, such as graphical watermarks or typographical variations, may also require a reconstruction of the document be made for publication, as the risk of publishing even the redacted original would be too great.

**Removing Metadata** Metadata-removal software exists, but a simpler approach is to print out a sensitive document, scan it back into your computer and rename the file. Similarly, you can remove metadata from an image or photograph by screenshotting the original and sharing the copy only. (Note that color printers may add nearly-invisible metadata to printed pages as an anti-counterfeiting measure. Printing documents in black and white reduces the chance of exposure.)

(Bonus! Being aware of what kind of metadata exists—and how to find it—also gives you a leg up as a reporter when researching and developing evidence and leads for stories.)

## Active Lesson: Removing metadata from a Word doc and a JPEG image

*[Trainer should begin by introducing participants to the concept of document metadata by showing examples of Word documents and JPEG images, showing where to find the metadata and what types of information may be “hidden” in a document's guts.]*

**Finding Microsoft Word metadata** The easiest way to view a Word document's metadata is to open it in Word and open the Properties dialog:

- In MS Word for OS X, choose **File > Properties** and select the summary tab.
- In MS Word 2010 and later for Windows, select the **File** tab, click **Info**, and select **Properties > Advanced Properties** on the right-hand side of the pane.

*[The instructor should take a moment to review the information included under each tab in the Properties dialog box with participants]*

The screenshot shows a macOS-style dialog box titled "SOOPERSEKRIT.docx Properties". It has five tabs: "General", "Summary" (which is selected and highlighted), "Statistics", "Contents", and "Custom". The "Summary" tab contains several text input fields and a checkbox. The fields are labeled as follows: "Title:" with the value "PLANS FOR THE INTERSTELLAR DEATH RAY"; "Subject:" with the value "DO NOT SHARE ESPECIALLY WITH THE HUMANS"; "Author:" with the value "O'Gorman, Kevin"; "Manager:" which is empty; "Company:" with the value "The Globe and Mail"; "Category:" which is empty; "Keywords:" which is empty; "Comments:" with the value "Hi Mom!"; and "Hyperlink base:" which is empty. Below these fields is a "Template:" label with the value "Normal.dotm". At the bottom of the form area is a checkbox labeled "Save preview picture with this document" which is checked. At the bottom right of the dialog are two buttons: "Cancel" and "OK".

SOOPERSEKRIT.docx Properties

General Summary Statistics Contents Custom

Title: PLANS FOR THE INTERSTELLAR DEATH RAY

Subject: DO NOT SHARE ESPECIALLY WITH THE HUMANS

Author: O'Gorman, Kevin

Manager:

Company: The Globe and Mail

Category:

Keywords:

Comments: Hi Mom!

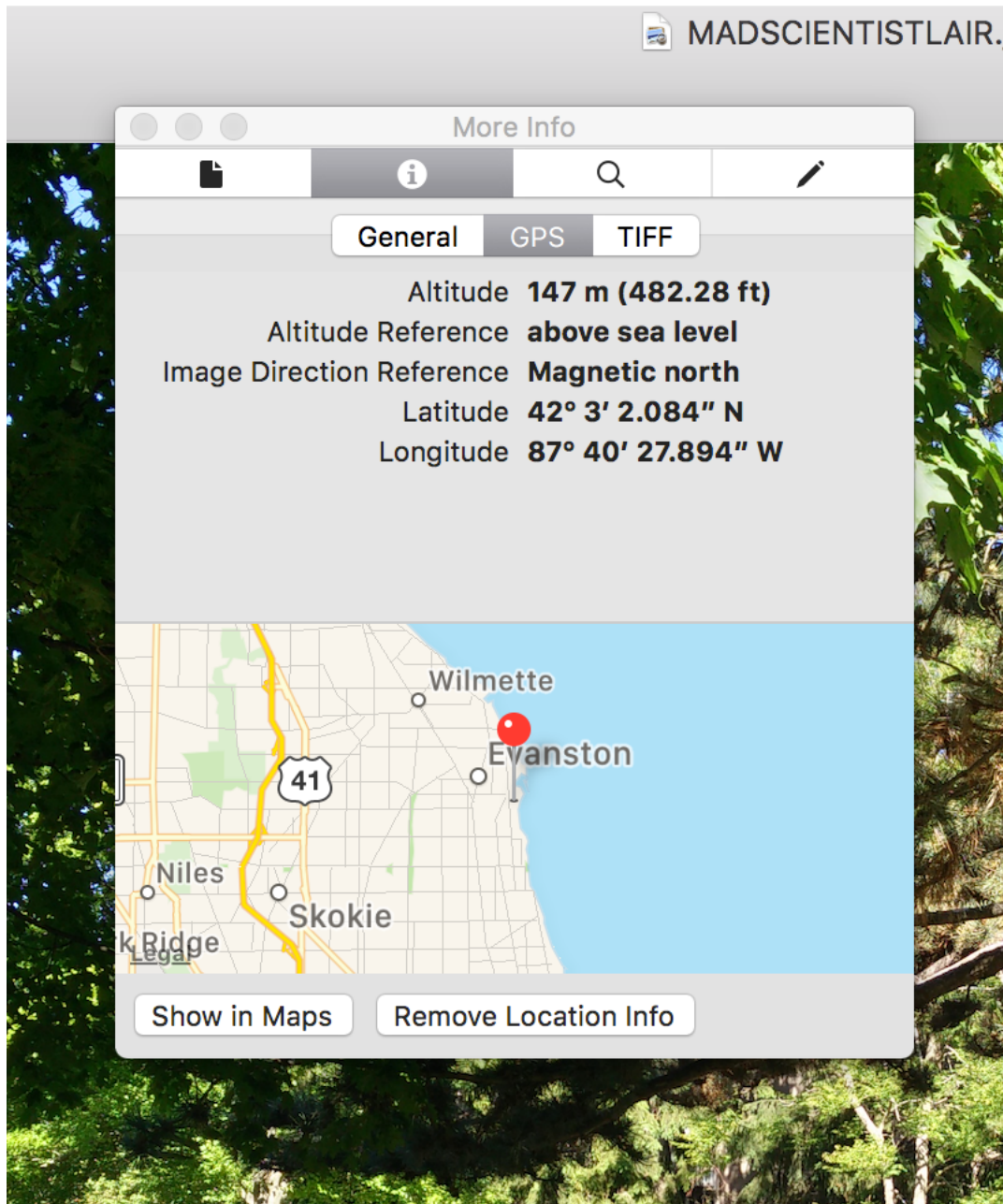
Hyperlink base:

Template: Normal.dotm

☒ Save preview picture with this document

Cancel OK

**Finding image metadata (EXIF data)** Most digital cameras, including smartphone cameras, add metadata to photographs, typically including information about camera settings and the time and location of the shot. You can find this metadata by opening the image information in an image viewing application. For example, in OS X, you can use the built-in Preview App, by opening the image and choosing **Tools > Show Location Info**.



**Scenario: scrubbing metadata** How do you share SOOPERSEKRIT.docx with a third party without exposing the information in the document properties? How do you share MADSCIENTISTLAIR.jpg without giving away the GPS coordinates embedded in the image EXIF data?

*[5-10 minute small group discussion:\** Instructor should ask participants to brainstorm ways they could share or publish the sensitive information. Have each small group report back and see if anyone came up with the idea to retype a document, print and scan, or utilize screenshots. (Spend some time talking about other solutions that came up.)]\*

*[10 minute activity:\** Instructor should provide an image file that has location data ([link](#)) and a Word document with ownership metadata ([link](#)).]\*

Now, split up into pairs, one person pretending to be the journalist with sensitive documents, the other pretending to be a third-party expert in the subject area who is going to review them.

- The “journalist” should print out the document and use a scanner or mobile application to ingest the document (If the “journalist” uses a color printer, the instructor should verify that they printed the document in monochrome.)
- The “journalist” should share the scanned image with the “expert”—for this exercise it doesn’t matter how, but in a real-world scenario the image should be shared securely.

Now, change roles: One person should be a sensitive source with a photo to leak, and the other should be a journalist who is going to receive a “scrubbed” image.

- The “source” should make a screenshot of the original file and send the scrubbed version to the “journalist.”
- The instructor should verify with the “journalist” that the new file’s EXIF data does not contain location info.

### 6.11.4 Recommended Reading

- *Protecting Your Sources When Releasing Sensitive Documents* - a checklist for handling and releasing leaked documents.
- <https://exifdata.com/> - an online tool for examining EXIF data in images. (But note that uploading sensitive images to a third-party site is not recommended.)
- *Simple questions: What is a file’s metadata and how to edit it in Windows?* - a guide to removing file metadata under Windows.
- *The Metadata Anonymisation Toolkit* - a CLI-based metadata removal toolkit. Some familiarity with UNIX shell commands is a requirement, and the project is not under active maintenance.

## 6.12 Using SecureDrop Safely

### 6.12.1 Overview

SecureDrop is an anonymous whistleblowing tool, built on well-tested cryptographic technologies, and designed to provide its users with a high degree of protection from detection through Internet-based surveillance. This lesson plan covers what you’ll need to know to use SecureDrop effectively: establishing a culture of security, setting up SecureDrop securely, and making sure your sources know how to use it safely.

### 6.12.2 About This Lesson Plan

**Review date:** 29 Sep 2017 **Lesson duration:** 1 hour (or 90 minutes with the optional demo section) **Level** (advanced)

**What will participants learn?** At the end of this session, participants will have a general understanding of how SecureDrop works, what is required to install it, and its strengths and limitations.

**What materials will participants need?** A laptop, pen, paper.

**How should participants prepare?** Participants should visit <https://securedrop.org/> and review information about the system available there.

**What materials will the instructor need?** Laptop, projector, Android or iOS phone

**How should the instructor prepare?** Review current SecureDrop documentation at <https://docs.securedrop.org/en/stable/index.html>

Optional: Set up journalist access to Securedrop Demo instance at <https://securedrop.org/demo>:

- add journalist username and password to password manager (or write them on a Post-it!)
- scan QR-code with Google Authenticator app to set up 2FA

- save the private key for the demo instance to their GPG keyring

**Preconditions** Lesson plans covering basic digital security topics: disk encryption, password management, 2-factor authentication.

### 6.12.3 Lesson Plan

**Icebreakers/activities - Discussion** General: how do you communicate with anonymous sources? How many third parties are involved in those communications?

Journalists - how do you get in touch and maintain contact? Email? Text messages? Postal service? In-person only?

Editors - what are policies around use and confirmation of anons? Can you use verified information, information that's unverified but highly credible? What about anonymous quotes?

Publishing - what are policies around how stories with anonymous sources get published?

When leaking goes wrong - [https://en.wikipedia.org/wiki/Reality\\_Winner](https://en.wikipedia.org/wiki/Reality_Winner) [other examples]

**Overview** SecureDrop started off as DeadDrop, a whistleblowing system developed by Aaron Swartz in collaboration with Kevin Poulsen. The system was later renamed SecureDrop, and is now maintained as an open-source project by the Freedom Of The Press Foundation. It's intended to help journalists and anonymous sources communicate securely over the open Internet, and it does so in three ways:

1. it reduces the number of 3rd parties involved in communication,
2. it uses tried-and-true cryptographic technologies,
3. and it isolates critical components from any networks.

These features make SecureDrop a powerful tool, but they also impose strict requirements on how the system is implemented and used. If basic digital security practices are not already being followed in your newsroom, the safety of leaked documents can't be guaranteed to any reasonable level. You'll need to make sure that people have the tools and knowledge to protect their devices and data, by creating a culture of security that emphasizes best practices and includes everybody working with leaked documents. You'll need to set SecureDrop up securely, to reduce the risk of an implementation flaw compromising your sources. Finally, you'll need to provide information to your sources to help them use it safely..

#### A culture of security

In order to use SecureDrop, and provide a reasonable guarantee of security for high-risk sources, you should already have some digital-security tools and policies in place.

*[Discussion: Instructor could ask why this would be important - a good answer would be because leaked documents need to be secured and handled safely within the newsroom, no matter what the source.]*

At a minimum:

- The system's users should keep their electronic devices up-to-date with any OS updates and security patches.
- Full Disk Encryption should be turned on for any related computers, smartphones, and storage devices.
- Strong safe password policies should be mandated and enforced.
- Users should enable 2-factor authentication for any accounts that support it.

Your organization should have existing policies for the sharing and storage of sensitive information (and if it doesn't, you need to create them). These should be reviewed and updated as necessary to cover digital documents. One important thing to consider in this updated policy is whether to reveal the use of SecureDrop in a story. In general, this is not recommended, as it may provide correlating information for someone trying to uncover an anonymous source, but every story is different.

SecureDrop is built on TOR and Onion services - you'll need to make sure that people who will be using the system know how to use the TOR Browser safely. For more information, see the Tor Project's documentation, starting here: <https://www.torproject.org/about/overview.html.en>.

### Setting up SecureDrop

The FPF provides full instructions and hardware requirements for setting up SecureDrop at <https://securedrop.org>, and it is possible for a competent Linux administrator to set it up themselves. However, given the many ways in which even simple setup mistakes could cripple its security, it's highly recommended that you reach out to the FPF for support and assistance with the initial setup.

A SecureDrop installation has two major components:

- the public-facing TOR hidden services (the TOR network's equivalent of websites) used by sources and journalists, delivered by two servers behind a hardware firewall.
- the secure viewing station (SVS) - an air-gapped computer used by journalists to decrypt messages and files from sources.

*[Discussion: Instructor could ask what kind of challenges participants might face setting up and protecting these servers, both from physical access and from attacks over the Internet, and compare with existing server infrastructure, if they know how and where it's currently hosted.]*

During setup, an encryption keypair is generated for use by the SecureDrop installation - the public key is used by the hidden services to encrypt submissions, while the private key is stored on the SVS and is used by journalists to decrypt the same files. Because the SVS contains the only copy of the private key, it is critical to keep it secure and limit access. As such, the two system components have stringent physical security requirements.

**Public-facing services** The public-facing services component includes two servers (typically consumer-grade micro-PCs), a network switch/firewall, and a dedicated Internet connection. Sources use it to upload documents, journalists use it to download uploaded files. You should keep these servers somewhere you can control and monitor, preferably on-site. If they're kept off-site, for example in your datacenter, your hosting company may be legally compelled to give 3rd parties access to them without your knowledge. If a 3rd party has access to these servers, they'll be able to monitor incoming communications, which may compromise your sources.

**Secure viewing station** The SVS is an airgapped computer. It's not connected to any network, and ideally has no network or wifi hardware at all. It must be kept in a secure location, and access to it must be strictly limited to the people tasked with downloading and decrypting submissions. When it comes to the SVS, you should be as paranoid as your budget allows. If the SVS is compromised and the private key copied, all your SecureDrop submissions, past and future, can be decrypted.

**Roles and responsibilities** To maintain and use SecureDrop safely, you'll need to find people in your organization to fulfil the roles below:

- System administrator - they'll need some familiarity with Linux, and will be responsible for updates and backups. They should have access to the public-facing servers, but should not need unsupervised access to the SVS.
- User admin - they'll be responsible for managing journalist access to the system. They should not have unsupervised access to the servers or SVS.
- Journalist - they'll be responsible for checking for submissions and decrypting them via the SVS. They should have access to the SVS but do not need access to the public-facing servers.

There is no technical restriction on the number of journalists that can be given access to the system, but you should decide how you want to manage access. The more people who have access, the harder it is to secure the SVS. Typically, most organizations will designate a small team of journalists to check the system periodically, relying on them and their editors to pass along any submissions to the appropriate destination in the newsroom.



## Help your sources use SecureDrop safely

Used properly, SecureDrop makes it difficult to intercept communications between you and your sources, but it doesn't work in a vacuum. If your newsroom network or personal computers are compromised, this puts submitted documents at risk. Similarly, if your sources don't take precautions on their end, they may compromise themselves by contacting you. When you provide a link to your SecureDrop instance, whether publicly or privately, you should also provide instructions for sources on using it safely.

*[Discussion: Instructor should ask participants, given what they know already, what kind of risks a source might face while submitting documents to SecureDrop.]*

At a minimum, sources need to be aware of these basic points:

- Sources should use a computer they control, that is free of malware and monitoring software. Their employer-issued computer should not be used, as it doesn't meet this requirement. Using a self-contained secure OS like Tails (<https://tails.boum.org/>) adds an extra level of security here.
- Sources should connect to SecureDrop from a network that isn't associated with them in any way. For example, they should definitely not use their home network, or a coffeeshop network that they use often. Ideally they should find a network connection they've never used before, located somewhere they don't usually go.
- Sources should not contact you via any other method - email, Twitter DMs, or any other social networks. This will reduce the chance of them being exposed by correlating those communications with the content of future stories and the activities of your journalists.

High-risk sources need to take more precautions. The SecureDrop Source Guide (<https://docs.securedrop.org/en/stable/source.html>) provides a comprehensive guide for sources looking to protect themselves against surveillance by state-level actors.

## Alternatives

SecureDrop's requirements might make it not the best fit for your newsroom. In particular, if you can't guarantee the physical security of the public-facing servers or the air-gapped SVS, you should consider other options to support anonymous sources. Traditional methods such as postal mail still work, if sources take the appropriate precautions. One option worth considering is a newsroom dropbox using Signal, the encrypted messaging platform written and maintained by Open Whisper Systems. Barton Gellmann has written a guide on using Signal as a newsroom dropbox, which you can find here: <https://github.com/b4rton/signal-newsroom/blob/master/README.md>. For more information on the risks and benefits of alternative whistleblowing methods, see [Opening Secure Channels for Confidential Tips](#).

## (Optional) SecureDrop Demo

*[Practical: Instructor should guide participants through the process of submitting to SecureDrop, using the FPF demo instance at <https://securedrop.org/demo>. Participants should play the role of sources, using the source interface to send one or more messages. The instructor should have already configured their access to the demo instance's Journalist interface and be able to decrypt submissions.]*

## 6.12.4 Recommended Reading

**Links in the news** <https://securedrop.org/directory> - the Freedom Of The Press Foundation's directory listing media organizations offering SecureDrop.

<https://www.wired.com/2015/11/securedrop-leak-tool-produces-a-massive-trove-of-prison-docs/> - the Intercept confirms use of SecureDrop in a story for the first time.

<https://twitter.com/fahrenthold/status/785195210347163648?lang=en> - David Fahrenthold of the Washington Post heavily hints at its use during the 2016 US Presidential election.

**More Training Resources** <https://docs.securedrop.org/> - The official documentation site for SecureDrop, maintained by the Freedom Of The Press Foundation.

## 6.13 Security in the Newsroom: Who are you?

This is a living document and the most recent version can be found at: <https://goo.gl/7ojKpw>. This lesson plan, which covers Passwords and Two Factor Authentication is a great hour long brown-bag session that was shared with us by Alan Palazzolo at the Minneapolis Star Tribune. For other great overview lesson plans, take a look at:

NICAR18: Digital Security Tip Sheet for Journalists, March 2018 by @mshelton, @geminimatt, @mtigas, Sequoia McDowell and @camfassett.

Or, there are more great resources in [the resource roundup](#).

### 6.13.1 Logging in and authentication

There's a login for everything these days. The default way to prove to computers that you are you is with a username and password. We all have hundreds of different websites, computers, and other digital things that require passwords. That's a lot of opportunity for attackers to try to steal your identity or your personal information. So, how can we make sure we are being safe when we log into things? Let's talk about strong passwords, password managers, two-factor authentication, digital keys, HTTPS and more.

### 6.13.2 Security

A quick step back. Security comes in many forms, not just digital. There are lots of aspects to consider when it comes to your personal security, and many things to focus in on when talking about security in the newsroom. A few things to keep in mind about security in general:

- It's unfortunate, but more often than not, good security takes a bit of effort. And in practice, there is often a trade-off of what is easy and what is most secure.
- Good security does not rely on trust, though in practice it requires some.
- Though there are good general security practices, thinking about your security in terms of threat modeling (who will reasonably attack me, and what specifically do you need to defend against) will help focus your efforts.
- Attacks are always changing, it's good to stay up to date if just on a high level.
- Talk to experts. Unless you are totally confident of what you are doing, take a moment to double check with someone how to practice good security.
- You are never 100% secure. Understand what you are risking.
- Even if you don't think you are at risk, we are all avenues to other people who may be targets. *You are worthy of a data breach.*

### 6.13.3 Some terminology

Just to make sure we are all on the same page, here are some top-level words and concepts:

- **Authentication:** A mechanism used to identify someone. The most common mechanism is a username and password, but there are others, such as PIN codes, fingerprints, and more.



- **Authorization:** The ability to access a particular resource. For instance, your user on your computer has access to edit certain files, but not core, system files.
- **Password:** Usually a single word or short random set of characters used for authentication.
- **Passphrase:** A phrase used for authentication, usually at least a few words or a whole sentence. Note, that when we refer to good, secure “passwords”, we usually mean a passphrase.



– this icon indicates that you should customize the section to your newsroom.



– If you see this icon, this is important.

### 6.13.4 What’s at stake?

Though fairly simple, authentication, i.e. logging in, is a huge, far-reaching topic. Almost anything important these days has some sort of authentication. Your email, your bank account, your bills, your medical history, and so much more all are just a username and password away from being accessed.

**One compromise can lead to many.** Huge companies such as Target, Equifax, Yahoo, and *many others* have had huge amounts of their user’s data compromised. If you have use the same password or a pattern of passwords, once one site is compromised, your other accounts are much more likely to get compromised.

It is very possible that you have had an account compromised. The site “*Have I Been Pwned*” will give you some insight into that possibility. Note that “pwned” is a term used to describe getting “owned” by someone.

*Mat Honan had his digital life erased* and hijacked because of a series breaches chained together.

**Your identity.** If someone has access to your account, they can do things as you, such as post things to Twitter, reset accounts, or access sensitive information.

The Twitter account of CNN’s host, Anderson Cooper, was *compromised* just as recently as December. Deray Mckesson (@deray), a prominent figure in the Black Lives Matter organization and movement, had his account hacked into, even with second-factor authentication enabled. This is a good instance where one thought a security practice was solid, but in reality, it had holes.

**Specifically your email.** Your email is very strongly tied to your identity. In fact, most online accounts allow you to reset authentication with email, so, if your email gets compromised, many other accounts can be compromised. Your email is also often a trusted contact for the inbox of the people you know, so an attacker can more easily become a trusted contact if your email is compromised.

## Passwords

Passwords (and usernames) are probably the most common way to authenticate someone to access a service and one of the most important security concerns.

## Password managers

Most of us have hundreds of services that require a username and password. Most of us can’t remember hundreds of passwords. This is where a password manager comes in; they create a secure way to store all the username and

passwords you need. And most have the ability to integrate with your web browser so it makes it easy to login to a service.



**Installing and using a password manager is possibly the biggest step you can take in making your life more secure, and it's one of the easiest.**

There are two popular password manager products that you should consider using: LastPass and 1Password. Both have similar features, but **LastPass** has a free tier with all the main features, and it can be used/installed without installing an application on your computer, so it is suggested for most users.

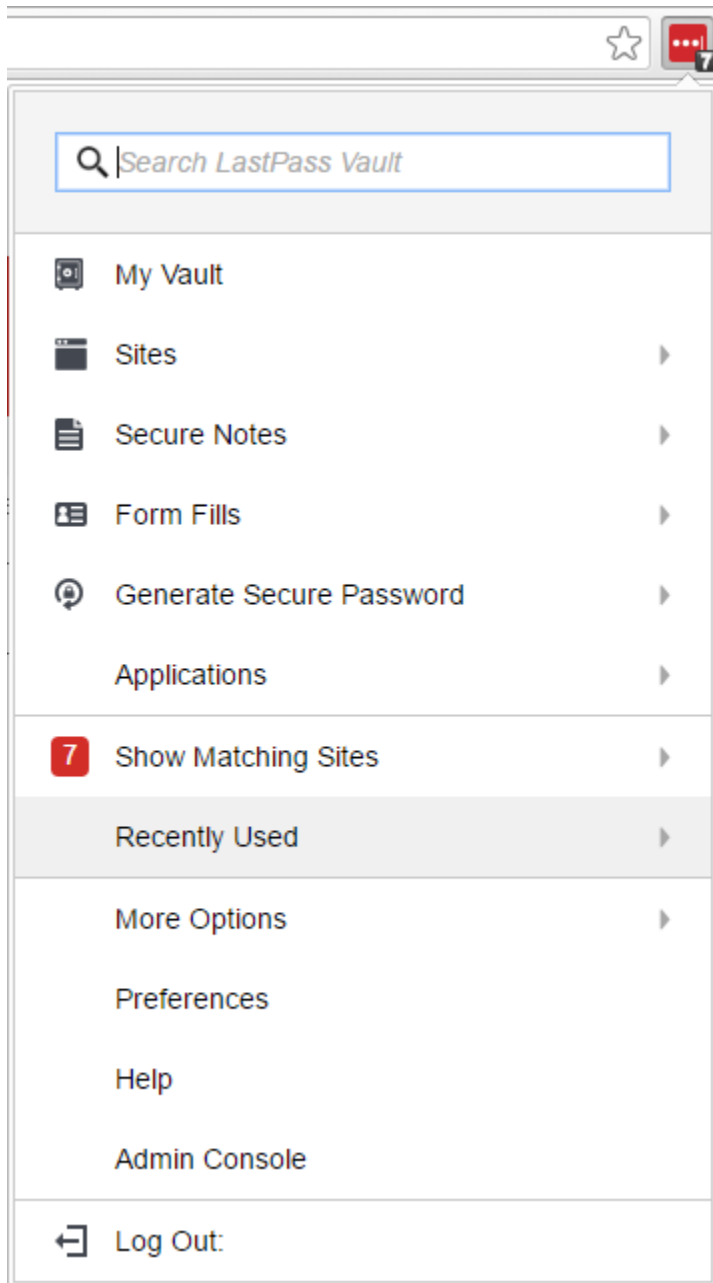
To see other options and features, see this [Wirecutter review](#).

It's important to note that you are putting a lot of trust into your password manager and the company that makes it and stores your data. Though it is not in their interest to compromise anyone's security, you cannot be 100% sure that it won't happen, and access to all your passwords is a lot of important information. But, it is still better than most alternatives.

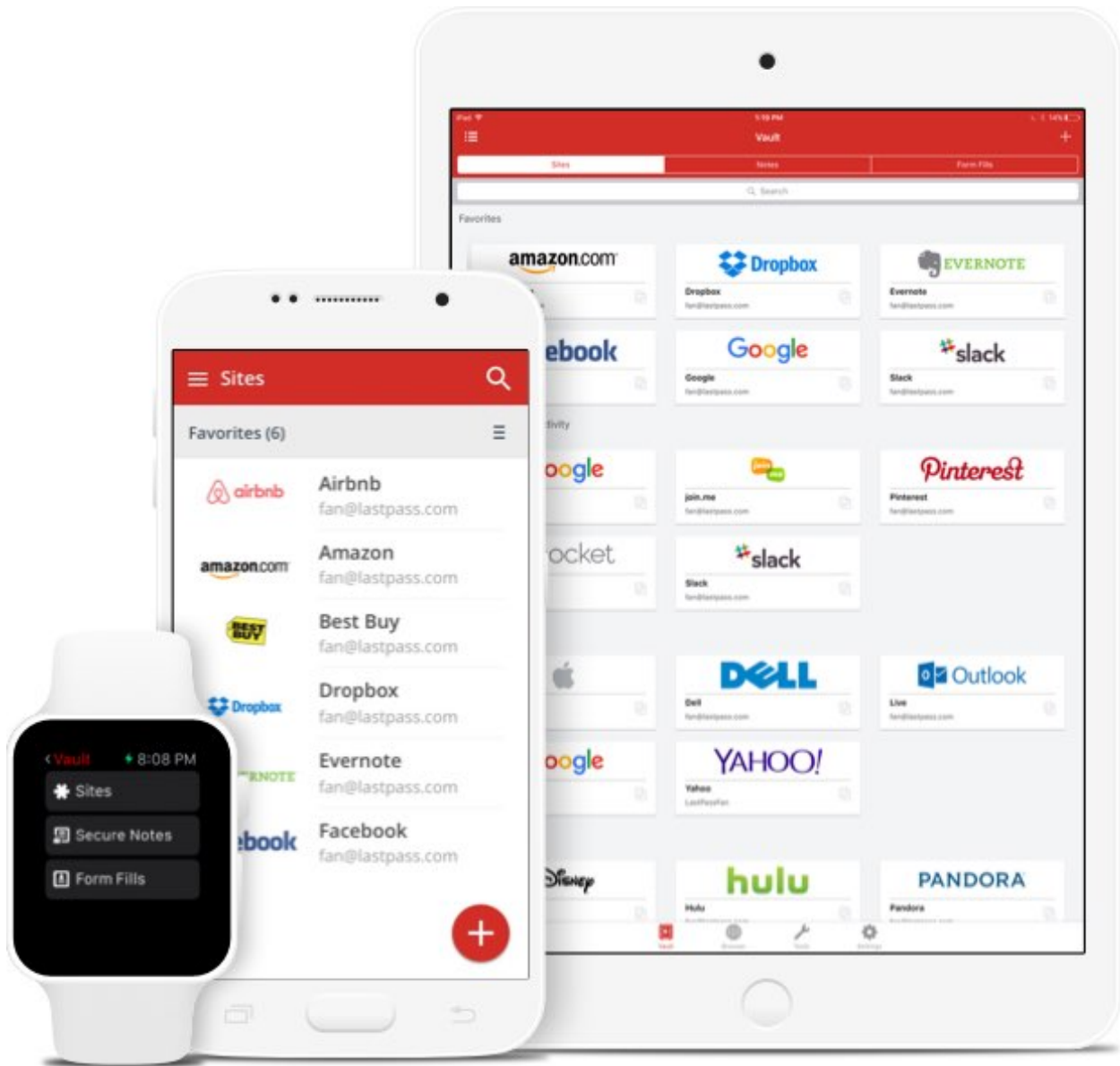
### LastPass

There are many ways to use and access LastPass.

One of the main ways is to use their [browser extensions](#). These are particularly great because they make it very easy to log into websites.



Another useful way to get access to your LastPass account is with their mobile applications, both for *Android* and *iOS*.



You can also install *stand-alone desktop applications* for LastPass.



Does your newsroom have a policy that prevents users from installing software or plugins? How should users in your newsroom install?

## Unique passwords

So, now that you have a password manager, you can practice some other good security more easily.



Use unique passwords for everything.

Unique passwords are important because you never know what site or service may be compromised. If you share passwords among services, the password is only as strong as the weakest security of all the services.

Unique passwords are hard to do without a password manager. Some people use a specific pattern that makes a unique password for each service, but more than likely, this pattern is easily discerned by an attacker.

Since Strib account passwords must be changed regularly, it's tempting to have your password include a number that you just increment at each change, e.g. "fiddler111" followed by "fiddler112". This is easy to remember but leaves a trail of breadcrumbs for any adversary who discovers an old password.

With a password manager, it is trivial to use a unique, unrelated password for every service.

### Strong passwords

The strength of a password refers to the ability for it to be determined or guessed by trying many combinations of words, letters, numbers, and symbols. The password "password" is both very short and extremely common and might be the first attempt someone uses when guessing your password; therefore it is very weak.



#### Use strong passwords.

In fact, just use long, random passwords. Most password managers will provide a way to generate passwords.

In some cases, you have accounts that you log into often where you need a password that you can remember. Overall, length is more secure than the variation (i.e. using symbols or uppercase letters). So, create a phrase that is memorable, but not easily guessable, and maybe add some easily rememberable variation. Some examples:

```
security-sure-is-gr8-for-us-all!  
is it snowing outside today in minneSNOWta?
```

Note, that once you start using really long passwords, you may notice that some services limit the length of your password. This is bad security on their part but not something that you will be able to change. This can be particularly annoying if you paste in passwords where the input has a maximum length.

### While we're at it...

Use unique, random usernames too. Many times your username is an email, but when it's not, why not use a unique username. This adds more security as it is less guessable, and if compromised less likely to be associated with another account.

### Shared passwords

It's a sad fact, but we often use shared passwords in the office; sometimes this is out of necessity and sometimes it's just a lack of effort.

Until our organization has a common, shared password solution that makes shared passwords easy and secure, here are a few tips for handling shared passwords. Basically, follow the same advice for non-shared passwords.

- Don't use easily guessable passwords like `startribune`. Use strong passwords.
- Don't use the same password over and over again. Use unique passwords.
- Don't write them down, or if you must, dispose of them in a shredder or other secure way.

- Put your shared passwords in your password manager.

*To explore:* It has been suggested that some services will allow multiple authenticator applications to be tied to one account, thus allowing 2FA for a shared account.

### More about passwords

There is plenty written about passwords; here are some good resources if you want to dive deeper.

- *Security in a Box's article on passwords*
- *Wirecutter's review of password managers*
- *OpenNews security training on passwords*

### 6.13.5 Two-factor authentication

A password is often referred to as a knowledge factor when authenticating. To make accounts more secure, more factors can be introduced if the service allows it. Common examples are possession factors (keys, phones, etc) and inherence factors (fingerprints, iris, etc).

Many services these days offer 2FA (two-factor authentication), allowing you to add a factor on top of the main mechanism which is most often a username and password. Some of the common ones are:

- A text or call sent to your phone with a specific code.
- A custom or 3rd-party application that provides a code (usually installed on your phone).
- A USB key
- A physical device that generates a code.
- Fingerprint.

Note that two-factor authentication may be referred to in other ways such as “two step verification” or “multi-factor authentication”.



**Enable two-factor authentication wherever you can.**

2FA makes your accounts much more secure (note nothing is 100% secure). If for some reason an attacker gets your password, or finds some way to reset your account, they still need some access to your second factor which makes it much harder to compromise your account.

Common services that have the ability to turn on 2FA:

- Google (GMail)
- Dropbox
- Twitter
- LastPass
- and *more*



**If your newsroom has a two factor policy, include it here.**

## Choosing your second factor

Some services allow you to choose different methods for your second factor. We'll go over a couple different ones. Though some are better than others, they are all better than nothing. If a choice is available, the preferred factor for most people is the **authenticator application**.

### Texting (SMS) or phone call

Probably the most popular, this is where the service will send you a code via SMS and then you enter that code into the service.

The main downsides of this is that you need to have phone reception, and your text and phone access is actually tied to your SIM card and not the actual phone; and there has been cases where a SIM has been transferred and an *account compromised*.

### Authenticator application

Another popular option, if available, is to use an authenticator application, often on your phone. This works similarly to SMS by generating a code that is tied to your account.

This is beneficial over the SMS approach, since it does not require network access, and does not lend itself to the SIM attacks described above.

There are a number of authenticator applications. Most services will let you use the one you want, but some are more forceful in their requirements. Some popular authenticator applications are *Google's Authenticator for Android* and *iOS* and *Authy*.

## Security keys

Though only really supported by some of the major services at this point, another option is a physical security key (usually via USB). These are much harder to compromise, but they are not free. A very popular option is *Yubikey*, and they offer a basic key for as little as *\$18*.

## You have a password manager now...

When setting up a 2FA, you will usually get some set of recovery codes that can be used if you lose your phone or authentication method. Put these in your password manager.

## More about 2FA

Enabling two-factor authentication is one of the best security practices that you can do and there's lots more to read up about it if you want.

- *OpenNews article on 2FA*
- *TwoFactorAuth.org*, a place to see what services offer two-factor authentication and what kind
- *EFF's guide to enabling 2FA on common services*
- *TurnOn1FA.com* has lots of specific tutorials on how to turn on 2FA for many services.
- *OpenNews security training chapter on 2FA*

### 6.13.6 Biometric authentication

Often used in place of a password, biometric authentication is using something that is unique to your physical body to prove that you are you. The most common is fingerprint scanning on our phones, as well as the face recognition that Apple has recently introduced.

Biometric authentication has its pros and cons (need reference). If you want to use biometric authentication, it is suggested to enhance it with a password or PIN; for instance, on Android, you can require the password every few days. If you are at a higher risk than most, such as working on very sensitive materials, use both a password and biometrics every time.

The use of biometric authentication is not new, but its consumer use is relatively new, and it really isn't known what the *practical* or *legal* consequences of it are.

### 6.13.7 Enhancements when authenticating

Some services will use different techniques or data points to “enhance” the authentication process. It can be argued whether these actually produce better security, but either way, these things should not be taken lightly, as they could be ways for attackers to access your account.

#### Security questions

“Security questions” are often used to enhance authentication. The idea is that by using some simple, easy-to-remember questions and answers, the service can be more certain you are who you are.

In practice, these should just be viewed as another password. So, treat it like one. Use unique answers, and write them down in your password manager. It is suggested to use simpler answer for these, as they may be used to confirm your account verbally over the phone (though hopefully not).

#### PIN

A PIN (personal identification number) is sometimes used to enhance a username and login, and sometimes it is the main method of authentication.

Again, these should be considered the same as passwords. Make them as long as possible, don't use the same one twice, and store in your password manager.

For things like a debit card, you're authenticating with the card itself and the PIN. In practice, you will probably want to use a number that you can remember. Make sure not to use a number that is easily associated with you, such as your house number.

#### Login images

These are not technically about authenticating who you are, but in actuality an anti-phishing technique; it is a mechanism for you to be (more) sure that the service is the correct service and not an attacker faking the service. It is suggested to make note of the image you set when creating an account in your password manager.

Note that we will talk about phishing in another session.

### 6.13.8 Email address

Your email address is very often your username for a service. Often, a service will have you “verify” your email address by sending you an email with some sort of verification link or something similar.



This is a sort of second form of authentication, as your email is assumed to be associated with you personally.

Your email becomes a gateway to many other accounts, as it is the username, and it is the main mechanism for services to reset your account. Make sure you use a very strong, unique password for you email and turn on two-factor authentication.

Note that Google Mail allows you to use *different forms* of your email address. This helps obfuscate your address, making it slightly harder to associate accounts.



**At the very least, make sure you use strong passwords and 2FA for your email addresses.**

### Temporary emails

For serious, though a bit risky, security, you can use temporary or throw-away email services to verify accounts. This is a good idea to ensure that your own email is not compromised, but it means that you won't be able to recover access if needed.

This list has not been reviewed, but here is a list of *disposable email services*. If “temporary” is not super important, consider using *ProtonMail*, a secure mail service that stores emails on an encrypted server and encrypts any messages sent to other ProtonMail users (but not outside email addresses).

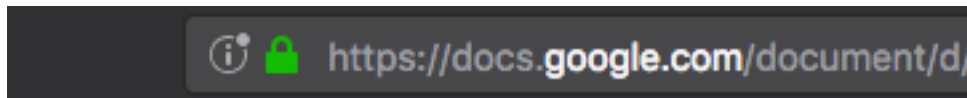
### 6.13.9 Make sure the site is secure

When actually logging into a site, you should consider a couple things. First, you should make sure it's the correct site and you are not being phished, but this will be covered in another session.

#### HTTPS

Just as importantly, you should make sure the browser is communicating securely with the server via HTTPS. The default of the web is to use HTTP (hypertext transfer protocol); the thing to know about HTTP is that information is transferred as is. So, if you send your password to the website, someone who has access to the network itself can see that password. That's where HTTPS (“s” is for secure); it creates an encrypted channel between your computer and the website. So, it's important to use HTTPS when logging in. Your browser should make it fairly easy to know if the site is secure.

Look for a lock icon near the website address. Similar to the following:



### 6.13.10 In the newsroom

What are specific considerations in the newsroom. Indirectly, any information or communications that can be accessed by a login is at stake; this may include a source's identity, communication to colleagues, sensitive documents, etc.

## **Research**

While researching online, and obviously depending on the nature of the research, it may be beneficial to use a temporary email so that your identity is not tied to any research you may be doing.

---

## Chapter 3 - Resources

---

Chapter 3 aggregates links to the best existing resources, to help new trainers deepen their own expertise. It also includes a glossary of common terms.

### 7.1 Resources for building further expertise

What follows is a curated list of links to guides, curricula, how-to's and in-depth resources suitable for those who wish to build further expertise.

#### 7.1.1 COMMUNITIES, LEARNING AND GUIDES

Comprehensive resources addressing digital security in general, and online communities where digital security is discussed.

**PEN America's Online Harassment Field Manual** <https://onlineharassmentfieldmanual.pen.org/> *Pen America* A resource containing effective strategies and resources that writers, journalists, their allies, and their employers can use to defend against cyber hate and fight online abuse. **Published:** April 2018 **Added:** May 2018

**EFF's Security Education Companion** <https://sec.eff.org> *Electronic Frontier Foundation* A resource for people teaching digital security to their friends and neighbors. **Published:** November 2017 **Added:** December 2017 **Tags:** curriculum, train-the-trainer

**Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communication** <https://ssd.eff.org/> *Electronic Frontier Foundation* A guide to protection against surveillance, this guide also includes great material on personal digital security. Organized into overviews, tutorials, briefings, playlists. **Published:** October, 2014, updated frequently (timestamp at the bottom of each guide.) **Added:** June 2017 **Tags:** guides, surveillance

**A First Look at Digital Security** <https://www.accessnow.org/a-first-look-at-digital-security/> *Access Now* A primer booklet for those beginning to think about digital security and threat modeling. Based around a series of useful personas. [Open on github](#). **Published:** last updated May 2017 **Added:** June 2017 **Tags:** guides, beginners

**Introduction to Digital Security for Journalists Handout (NICAR 2018)**

@mshelton, @gemiimatt, @mtigas, Sequoia McDowell, @camfasset A thorough roundup of tools and best practices from NICAR 2018 **Published:** March 2018 **Added:** March 2018 **Tags:** guides, intros

**11 tips for protecting your privacy and digital security in the age of Trump** <https://freedom.press/news/11-tips-protecting-your-privacy-and-digital-security-age-trump/> *Olivia Martin, Freedom of the Press Foundation* An introduction to digital security with brief descriptions and links to resources on threat modeling, strong authentication, secure communications, device encryption, browser security. The article also includes guidance on update hygiene, VPNs, and phishing. **Published:** January, 2017 **Added:** June 2017 **Tags:** intros, lists, beginners

**A DIY Guide to Feminist Cybersecurity** <https://hackblossom.org/cybersecurity/> *Noah Kelley, HACKBLOSSOM* This fairly guide covers basic explainers and links to tools for blocking online tracking, circumvention and anonymity tools, defending against malware, strong authentication practices, privacy on social media, as well as device and communication encryption. It does *not* include hands-on guides that walk users through use/installation of various tools. **Published:** ? **Added:** June 2017 **Tags:** guides

**Journalists in Distress: Securing Your Digital Life** [http://www.cjfe.org/journalists\\_in\\_distress\\_securing\\_your\\_digital\\_life](http://www.cjfe.org/journalists_in_distress_securing_your_digital_life) *Canadian Journalists for Free Expression* The guide includes background information describing how data flows online and in mobile networks, as well as information on browser privacy and security, encrypted communications, social media privacy, internet cafe concerns, strong authentication, and information about technical threats from authorities. **Published:** January 2017 **Added:** June 2017 **Tags:** guides

**Security Training Resources for Security Trainers (Spring 2017 edition)** <https://medium.com/cryptofriends/digital-security-training-resources-for-security-trainers-spring-2017-edition-e95d9e50065e> LINKS TO GUIDES/ARTICLES *Rachel Weidinger, Cooper Quintin, Martin Shelton, Matt Mitchell* A “meta-guide” for finding information on the current state of U.S. digital security training. **Published:** Spring 2017 **Added:** June 2017

**Digital Security and Source Protection for Journalists** <https://susanemcg.gitbooks.io/digital-security-for-journalists/content/index.html> GUIDE (BORDERING ON A TEXTBOOK) *Susan E McGregor* A comprehensive and well-written paper on digital security for Journalists. Written in 2014, most of the content is still relevant. **Published:** 2014 **Added:** June 2017

**Committee to Protect Journalists Security Guide: Technological Security** <https://cpj.org/reports/2012/04/technology-security.php> GUIDE *CPJ staff* Part of CPJ’s comprehensive Journalism security guide. **Published:** 2012, updated since (note: asked for update policy) **Added:** June 2017

**Tinfoil Press** <https://mshelt.onl/tinfoil.press/> COMMUNITY *An online community space founded by Martin Shelton* A tinfoil-hat free zone to discuss digital security and Journalism with others in the field. Now inactive, but available as an archive. **Published:** ? **Added:** May 2018

**LevelUP** [https://level-up.cc/CURRICULUM/GENERAL TRAINING GUIDANCE](https://level-up.cc/CURRICULUM/GENERAL%20TRAINING%20GUIDANCE) A pedagogical resource for those providing digital safety and security training. **Published:** June 2016 **Added:** June 2017

**Digital Security Resources for Media Trainers** [http://saferjournointernews.org/pdf/SaferJourno\\_Guide.pdf](http://saferjournointernews.org/pdf/SaferJourno_Guide.pdf) CURRICULUM/GENERAL TRAINING GUIDANCE *Manisha Aryal, Dylan Jones, Internews* An in-depth and still relevant guide to digital security for Journalists. **Published:** 2014 **Added:** June 2017

**Rory Peck Trust Digital Security Resources** <https://rorypecktrust.org/resources/digital-security> GUIDE Links to videos and other resources on secure communication and digital security. (Includes a well-developed risk assessment series for journalists.) **Published:** various **Added:** June 2017

**Information Security for Journalists** <http://www.tcij.org/node/1016> *Silkie Carlo & Arjen Kamphuis, the Center for Investigative Journalism* GUIDE (Advanced) **12/2017:** *This resource is not currently available. Reached out to TCIJ for more info. – abh* This guide focuses on security concerns for investigative journalists, particularly those with sophisticated attackers. This guide examines threat modeling, hardware security, enhancing operating system security (e.g., with TAILS), disk and communications encryption (e.g., PGP and OTR), file data and metadata, browser privacy tools, circumvention software, and strong password practices. (Great advanced guide, but probably not the best guide to give to users who are new to digital security, since they are likely to be overwhelmed and decide that digital security is not for them.) **Published:** 2016 **Added:** June 2017

**How to Lead a Digital Security Workshop** [https://motherboard.vice.com/en\\_us/article/how-to-give-a-digital-security-training](https://motherboard.vice.com/en_us/article/how-to-give-a-digital-security-training) ARTICLE/101 TRAINING ADVICE *Rachel Weidinger, Cooper Quintin, Martin Shelton, Matt Mitchell via Motherboard* How to get started on digital security training for first-timers. The short guide encourages new and would-be security trainers with some considerations for effective training. These considerations include how to think about practical security advice, planning and logistics, building knowledge, focusing on teaching narrowly-scoped mastery, as well as self-presentation and audience engagement in security trainings. **Published:** February 2017 **Added:** June 2017

**My Shadow Training Curriculum (Tactical Tech)** <https://myshadow.org/train> and <https://gitlab.com/ttc/data-privacy-training/tree/master/content> for easier access to .md content CURRICULUM *Tactical Tech* Tactical Tech's training curriculum for their "My Shadow" project focused on privacy. It focuses on privacy and digital security awareness-raising, and includes some easy recommendations for general audiences. You can select lesson modules, workshop information, and print out corresponding PDF handouts. (The gitlab link is currently most accessible than the main website, with the a **Published:** late 2016 **Updated:** June 2017

**SAFETAG** <https://safetag.org/#audit> *Internews, Multiple Human Rights International Training Organizations* These are resources on security support for different types of collectives (usually organizations, but also networks of varying complexities). Includes conducting pentesting audits, training, incident response processes, persuading organizations and leadership to adopt security tool, practices and policies, etc. (When groups and industries fully commit to safe practices and behaviors for staff and users, this is the next step beyond ad hoc "trainings" and peer recommendations, since doing security at a collective level is vastly more effective than doing it in a scattershot manner.) **\*\*Published:** **\*\*2016**, new edition to be published late 2017 **Added:** June 2017 **Tags:** Security for Groups, Security for Networks, Organizational Security

**Organizational Security Wiki** <https://orgsec.community/display/OS> *Internews, Multiple Human Rights International Training Organizations* These are resources on security support for different types of collectives (usually organizations, but also networks of varying complexities). Includes conducting pentesting audits, training, incident response processes, persuading organizations and leadership to adopt security tool, practices and policies, etc. (When groups and industries fully commit to safe practices and behaviors for staff and users, this is the next step beyond ad hoc "trainings" and peer recommendations, since doing security at a collective level is vastly more effective than doing it in a scattershot manner.) **Published:** early 2016, intermittent additions **Added:** June 2017 **Tags:** Security for Groups, Security for Networks, Organizational Security

**WMC Speech Project - Tools and Resources** <http://www.womensmediacenter.com/speech-project/tools-resources/> *Women's Media Center - multiple authors* These are resources and tools to support the The WMC Speech Project, which is dedicated to expanding women's freedom of expression and curbing online harassment and abuse. Included are resources to assist with immediate and ongoing harassment, guides to digital security from the perspective of preventing doxxing and online harassment, and links to organizations with similar goals **Published:** late 2016, ongoing additions **Added:** January 2018 **Tags:** Security for Groups, Online Harassment, Organizational Security, Personal Security

**The Holistic Security Manual - Tactical Tech** <https://holistic-security.tacticaltech.org/> *Tactical Tech - multiple authors* This manual takes a holistic approach to security, treating physical, psycho-social, and digital security as part of a greater whole rather than addressing them separately. It describes a process with Prepare-Explore-Strategize-Act phases to produce security recommendations tailored to specific circumstances. **Published:** September 2016 **Added:** January 2018 **Tags:** Security for Groups, Organizational Security, Personal Security

**CPJ - Emergency Response Team** <https://cpj.org/emergency-response/> *CPJ staff* This team provides safety and security tools and information for journalists, in addition to rapid response assistance for journalists at risk. **Published:** undated **Added:** January 2018 **Tags:** Security For Groups, Personal Security, Emergency Support

**Global Journalist Security** <https://www.journalistsecurity.net/> *Global Journalist Security staff* This organization provides hostile environment training for journalists and other at-risk groups. Their main focus seems to be physical security, but they also have a Digital Security For Newsrooms course. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Personal Security

**Global Investigative Journalism Network - Helpdesk** <https://helpdesk.gijn.org/support/solutions/articles/14000036509-safety-and-security> *Multiple authors* Guides covering physical and digital security for journal-

ists, along with a helpdesk to provide support with queries related to the covered topics. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Personal Security

**Dart Center for Journalism and Trauma** <https://dartcenter.org/> *Multiple authors* Guides and teaching resources to support journalists reporting on traumatic topics and events. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Psychological Support

**International SOS** <https://www.internationalsos.com/> *International SOS staff* Risk management consulting and support for organizations operating in hostile environments. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Risk Management

**Control Risks** <https://www.controlrisks.com/> *Control Risks staff* Risk management consulting and support for organizations operating in hostile environments. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Risk Management

**On Call International** <http://www.oncallinternational.com/> *On Call International staff* Risk management consulting and support for travelers and organizations operating in hostile environments. **Published:** undated **Added:** January 2018 **Tags:** Physical Security, Security for Groups, Risk Management

### 7.1.2 PERSONAL DIGITAL SECURITY

Resources for securing accounts and personal digital integrity.

**Security Planner** <https://securityplanner.org/> *Citizen Lab staff* A resource that provides digital security recommendations based on responses to a few simple questions. It's a good starting-point for basic digital security policies for journalists in low-risk situations. **Published:** December 2017 **Added:** January 2018 **Tags:** Personal Digital Security

**Security for Journalists: Part 1: the Basics** <https://source.opennews.org/articles/security-journalists-part-one-basics/> *Jonathan Stray* A beginner-friendly introduction to threat modeling, strengthening authentication, identifying phishing attacks, as well as device encryption. While this resource came out in 2014, its lessons are still applicable today. **Published:** 2014 **Added:** June 2017

**Defending Accounts Against Common Attacks** <https://source.opennews.org/guides/defending-accounts/> MIX: LINKS TO GUIDES, ARTICLES, TOOLS. *Martin Shelton/OpenNews* A curated list of account security resources and articles from Martin Shelton – a really good overview. **Published:** 2014-2017 **Added:** June 2017

**Securing Your Digital Life Like a Normal Person** <https://medium.com/@mshelton/securing-your-digital-life-like-a-normal-person-a-hasty-and-incomplete-guide-56437f127425> GUIDE (101) *Martin Shelton* A very approachable guide to better security practices for the average user of the internet. **Published:** December 2015, regularly updated **Added:** June 2017

**The Motherboard Guide to Not Getting Hacked** [https://motherboard.vice.com/en\\_us/article/the-motherboard-guide-to-not-getting-hacked](https://motherboard.vice.com/en_us/article/the-motherboard-guide-to-not-getting-hacked) GUIDE (101) *Vice, Joseph Cox and Lorenzo Franceschi-Bicchierai* A basic guide to personal digital security from Motherboard. **Published:** August, 2016 **Added:** June 2017

**Umbrella from Security First** <https://secfirst.org/index.html> MULTIPLE GUIDES (ANDROID, TEXT FILES) *Umbrella* is a huge conglomeration of numerous *other* guides, including EFF's SSD, Security-in-a-Box, humanitarian physical safety guides, and many more – complete list of guides [here](#). *Security First* An open source ([github](#)) app with checklists and details about online and physical security. **Published:** 2015, actively updated **Added:** June 2017

**Digital Privacy at the U.S. Border** <https://www.eff.org/wp/digital-privacy-us-border-2017> GUIDE *Sophia Cope, Amul Kalia, Seth Schoen, Adam Schwartz, Electronic Frontier Foundation* In light of the looming U.S. travel ban targeted at individuals traveling to and from primarily Muslim countries, the Electronic Frontier Foundation Part released this whitepaper to examine travelers' security options at the U.S. border. The paper examines the basics of risk assessment, as well as legal, technical, and practical concerns when you are preparing to leave, arriving at the border, and what to do afterwards. The guide also examines your rights, U.S. border policy, a wide range tools you can use to protect yourself, and their constraints. **Published:** March 2017 **Added:** June 2017



**Anti-phishing and Email Hygiene** <https://freedom.press/training/email-security-tips/> TOOL-SPECIFIC GUIDE Harlo Holmes, *Freedom of the Press Foundation* This guide covers threat modeling, authentication practices, as well as common phishing tactics and how to avoid them. **Published:** December 2016 **Added:** June 2017

**Password Managers for Beginners** <https://medium.com/@mshelton/password-managers-for-beginners-d1f49866f80f> TOOL-SPECIFIC GUIDE Martin Shelton A beginner-friendly guide describing why password managers are useful, branching into three step-by-step guides for getting started with 1Password, LastPass, and KeePass. **Published:** November 2016 **Added:** June 2017

**Two Factor Auth** <https://twofactorauth.org/> TOOL-SPECIFIC GUIDE Josh Davis, *et. al.* Two Factor Auth is a list of popular websites, and information on whether they support two-factor authentication. It offers links with instructions for setting up two-factor authentication on each web service. On [github](#) here. **Published:** June 2017 **Added:** June 2017

**Two-Factor Authentication for Newsrooms** <https://medium.com/@mshelton/two-factor-authentication-for-newsrooms-a873060ea405> TOOL-SPECIFIC GUIDE Martin Shelton This guide examines how to use two-factor authentication by breaking it down into multiple methods, and walking through how to set it up, using Gmail as one example. It also describes some considerations for its use in a team setting. **Updated:** May 2017 **Added:** June 2017

**The Impossible Task of Creating a “Best VPNs” List Today** <https://arstechnica.com/security/2016/06/aiming-for-anonymity-ars-assesses-the-state-of-vpns-in-2016/> TOOL-SPECIFIC GUIDE Yael Grauer This article lays out the many, many issues with choosing a VPN, including logging, using preshared keys, and outdated encryption protocols. **Published:** June 2016 **Added:** June 2017

**The Motherboard Guide to VPNs** [https://motherboard.vice.com/en\\_us/article/the-best-vpns-ranked](https://motherboard.vice.com/en_us/article/the-best-vpns-ranked) TOOL-SPECIFIC GUIDE Lorenzo Franceschi-Bicchierai via *Vice/Motherboard* The basics of choosing a VPN, and a few practical recommendations for specific VPNs. **Published:** March 2017 **Added:** June 2017

**Encrypting your laptop like you mean it** <https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/> TOOL-SPECIFIC GUIDE Micah Lee A detailed resource on disk encryption for Mac devices with FileVault, Windows PCs with BitLocker, and Linux machines at the time of installation. The guide covers several attacks for stealing data from an unencrypted device. **Published:** May 2015 **Added:** June 2017

## 7.1.3 SECURE COMMUNICATION

Resources and tools for secure digital communication.

**Surveillance Self-Defence Against the Trump Administration** <https://theintercept.com/2016/11/12/surveillance-self-defense-against-the-trump-administration/> INTRO ARTICLE/SHORT LIST OF STEPS Micah Lee, *The Intercept* Framed for “activists and other concerned citizens.” Some steps are basic (encrypt your phone), some are more advanced (use Qubes). **Published:** November 2016 **Added:** June 2017

**Surveillance Self-Defence for Journalists** <https://medium.com/the-intercept/surveillance-self-defense-for-journalists-ce627e332db6> INTRO ARTICLE/SHORT 101 CHECKLIST OF STEPS *The Intercept* Checklists for secure digital communications. **Published:** January 2017 **Added:** June 2017

**Edward Snowden on how to Reclaim your Privacy** <https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/> INTRO ARTICLE/SHORT 101 LIST OF STEPS Micah Lee, *The Intercept* Snowden himself on how to regain as much of that sweet sweet privacy as possible. **Published:** November, 2015 **Added:** June 2017

**Signal for Beginners** <https://medium.com/@mshelton/signal-for-beginners-c6b44f76a1f0> TOOL GUIDE Martin Shelton A primer for using Signal for newcomers. Covers setup, using the app, and potential risks. **Published:** November 2016 **Added:** June 2016

**How to Keep Your Chats Truly Private with Signal** <https://theintercept.com/2017/05/01/cybersecurity-for-the-people-how-to-keep-your-chats-truly-private-with-signal/> Micah Lee, *The Intercept* A thorough, step-by-step guide on using Signal as securely as possible. The guide includes a short video overview, and

information on securing your mobile device, hiding lock screen messages, deleting old messages, exchanging video and photos, group chat, voice and video, adding contacts, verification, and using the desktop app. **Published:** May 2017 **Added:** June 2017

**Off the Record Messaging** <https://otr.im/> *Various* For those who want to dive deeper, this is the home of OTR, the encrypted, authenticated and deniable messaging protocol (very similar to what is used by Signal.) **Published:** Unknown (updated continuously) **Added:** June 2017

**Signals, Intelligence** <https://medium.com/@thegrugq/signal-intelligence-free-for-all-5993c2f72f90> *Thegrugq* A useful resource for understanding how Signal's encryption works and the various forms of metadata it exposes in routine use. **Published:** November 2015 **Added:** June 2017

**Upgrading WhatsApp Security** <https://medium.com/@mshelton/upgrading-whatsapp-security-386c8ce496d3> *Martin Shelton* A short guide that walks through improving WhatsApp's security by turning off and removing cloud backups, adjusting privacy settings, encryption key change notifications, and using session verification, as well as information on securing the device itself (e.g., with device encryption). **Published:** February 2017 **Added:** June 2017

**Opening Secure Channels for Confidential Tips** <https://source.opennews.org/articles/opening-secure-channels-confidential-tips/> *Martin Shelton* An overview of securing communications with confidential sources. **Published:** February 2017 **Added:** June 2017

**SecureDrop** <https://docs.securedrop.org/en/stable/index.html> *Various* SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. **Published:** updated regularly **Added:** June 2017

### 7.1.4 EVENTS

**RightsCon** <https://www.rightscon.org/> *n/a* Yearly conference focused on human rights and digital technology. **Published:** n/a **Added:** January 2018

**Global Investigative Journalism Conference** <https://gijc2017.org/> *n/a* Yearly conference hosted by the GIJN and various other institutions. Focuses on issues related to investigative journalism, with some digital security content. **Published:** n/a **Added:** January 2018

### 7.1.5 Contributing

To contribute a link, please open a pull request. This is a community-curated list, so we welcome additions, edits, deletions (in the case of content that no longer exists) and other helpful changes. We attempt to maintain a standard format to make this list more readable by both robots and humans, so please follow the format below when submitting or editing links.

**To add a link please follow this format:**

```
**<title>**<br />
<url><br />
*<authors> (csv)*<br />
<description> (single paragraph, or sentence)<br />
**Published:** <date> (date known to be published or updated) format: [month] [yyyy]
**Added:** <added> (date added to this list) [month] [yyyy]
**Tags:** <tags> (keywords, csv)
```

## 7.2 Concept Glossary

There are many ways to talk about digital-security concepts, and the example that really clicks can be different for every person. This resource is less a glossary than a roundup of great analogies and explanations, offering easier ways



to explain technical concepts for non-technical users.

**Adding your ideas:** We know this list is incomplete, and it probably always will be! It's a great place for contributions from the journalism-security community, so if you have a favorite concept or helpful analogy to share, we'd love to [hear from you](#). Let's make this list a lot longer:

- [Networks](#)
- [HTTPS](#)
- [Certificate Authority](#)
- [Encryption](#)
- [Authentication](#)
- [What is a Computer](#)

And if you're looking to build your own expertise as a security trainer, you'll find a community-driven list of resources to help you in [Chapter 3: Resources](#).

## 7.2.1 Networks

A network is two or more nodes connected physically and informationally over time. For example:

- Electrical grids
- Social graphs
- Road systems
- [John Snow's cholera map](#)
- [Packet-switching diagram](#)

Think about what a network sees when it sees you. On some you look like a billing point, little more than an amount of money owed, with a individual ID number. On some you look like a series of paths: Think about cell phone towers and ATM withdrawals. In a medical network, you look like a series of diagnoses, vital statistics, and a place where medical professional time and drugs vanish. That's what the you-shaped hole in that network looks like. To the electrical grid, your house looks like a point where power vanishes and money comes out. On a smart grid, that portrait is a little more complex. What do you look like on a phone network? You look like data, metadata, and paths from tower to tower. Time stamps, locations, and connections out to nodes on the internet tell the story of your day, and much of your life.

Most surveillance, good or bad, is built on how networks operate on the physical level. They're not nefarious, they're physics.

We live with and in networks every minute of every day. These networks lay over each other and touch all over the place. Once we start thinking about them, what they're shaped like, where we are in them, our contemporary world starts to make more sense.

The net is a packet-switching network. Packet switching is rather like passing notes in class: You hand the note to someone near you, who tries to hand it to someone closer to the person it's intended for. To know where to pass the note, a person has to know who it's going to, and they know who gave it to them. This knowledge is called metadata: the data a network needs to function.

## 7.2.2 HTTPS

- [The US CIO's excellent and thorough explanation](#), and [Chrome's Developer Blog](#) are both excellent explanations of why HTTPS is important.

- [HTTPS as Pigeons](#) via Andrea Zanin on freeCodeCamp walks through the core principles of HTTP and HTTPS with some nice pigeon analogies. (Not helpful, but clever, is the [IP Over Avian Carriers](#) protocol.)
- Wikipedia's [HTTPS entry](#)

### What is a Certificate Authority

- [HTTPS as Pigeons](#) covers CAs as trusted signatories (but doesn't address Let's Encrypt).

### 7.2.3 Encryption

- Wikipedia's [entry on Encryption](#) is a solid overview.

### 7.2.4 Authentication

The [passwords lesson](#) is a great resource for explaining the process of authentication. But at its core, "authentication" is just the process that a system uses to determine that you are who you say you are.

### Key-Based Authentication

Seth Schoen leads a great workshop on key-based authentication, and the analogy he uses is this: If you remember anything about mathematics, you might remember that it's not that hard to multiply two big numbers together. It takes time if you're only using a pencil, but you can do it. Factoring the product of two primes, however, is a lot harder. You can think of key-based encryption as taking advantage of this disparity.

### 7.2.5 What is a Computer (& What is Software)

- As ever, [Wikipedia's entry on Computers](#) is an excellent resource for thinking about definitions.

## 7.3 Best Practices for a Tips Page

This document was adapted from Martin Shelton's [Opening Secure Channels for Confidential Tips](#) (Source, Feb 2017). You should read that for a thorough review of best practices.

You should also read Ted Han and Quinn Norton on [Protecting Your Sources When Releasing Sensitive Documents](#) (Source, June 2017)

Secure tip channels allow sources to come forward with compelling information, while minimizing the risk to their own safety or livelihood. Secure tip channels also signal to sources that you take their confidentiality seriously.

This short guide describes some basics around how to think about security on behalf of your sources before thinking about tools and practices. We'll also describe common communication channels for accepting sensitive tips and tradeoffs when using each channel. When thinking about tradeoffs, consider which channels are right for you.

### 7.3.1 Before We Talk About Tools

Before we even talk about tools for taking confidential tips securely, there are some more basic issues to address.

1. Who is going to maintain the page? If you're reading this, the person maintaining the secure tip page for your newsroom might be you. Make sure you know what that entails, and that there's a plan in place for handing off ownership if you leave the newsroom.
2. The page should easily accessible, and under the newsroom's control.
3. Host secure tip pages with HTTPS, not over an unsecured HTTP connection. This prevents unwanted third parties from snooping on would-be sources' connections to your tip page. If your site doesn't already default to HTTPS, address that first. Two excellent resources to help make the case: [The US CIO's excellent and thorough explanation](#), and [Chrome's Developer Blog](#).
4. HTTPS prevents an eavesdropper from sniffing out anything beyond the domain name, so your tips page should not be served from a dedicated subdomain (eg. <https://tips.example.com>), but on a subdirectory of your primary website (eg. <https://www.example.com/tips>).
5. The newsroom should be prepared to advertise the tips page widely. A good tips page only works if people read it *before* reaching out.

### So what goes on the page?

- Give sources as many ways to reach out as you have, and be clear about the advantages and drawbacks of each channel.

### Don't stop with a tips page.

Whether or not a source uses your confidential tips infrastructure to reach you, you have a responsibility to consider their safety before you continue to communicate with a source.

Think about who would care about this information being made public (such as their employer). What capabilities do they have to investigate the source of the tip? What are the potential consequences for your source if they are discovered? And then guide your source to the communications channels that will best protect them from surveillance.

And when you're ready to publish, make sure you're not inadvertently revealing your source.

[Protecting Your Sources When Releasing Sensitive Documents](#) (Source, June 2017) is an excellent review.

### Content versus metadata

Many of the tools we recommend can protect the contents of your communications, but not the fact that you communicated at all. Even if your phone company isn't monitoring the contents of a phone call, their records will show all the numbers you called, whether the other party answered, and how long you stayed on the line. If you make calls over a service like WhatsApp, your phone history will still show that the call was made.

Most secure communications channels do not protect against metadata surveillance, so make note of these constraints in your documentation.

Similarly, any file on your computer has a bunch of metadata attached to it: the date and time it was created, the time it was last modified, size, and filename. And depending on the software that created the metadata might include the name of the person who created it, or the company the software was licensed to. EXIF data attached to digital images often includes the type of camera the image was captured with, or even the GPS coordinates of the device at the time the photo was taken. In 2012, Vice [outed the location of then-billionaire-in-hiding, John McAfee](#) by posting a photo online: the journalist's iPhone 4 automatically tagged the photo with the phone's GPS data.

The session on [scrubbing metadata from files](#) includes some excellent resources to help ensure that hidden metadata doesn't burn your sources.

### First Contact

If a source reached out over a work phone or email, they have already given their employer a metadata trail. This is sometimes called the "first contact problem," and there is no quick fix. This is why newsrooms have a responsibility to educate sources (and potential sources) before they reach out.

Your tips page is a good place to offer that education.

The best we can do is support the appropriate communication channels, and advertise that we're available to check out tips. Have a page where these channels are clearly organized, and share it with information about the tradeoffs.

It's also important to be clear that if they have reached out over a less-than-ideal channel, such as calling from their work phone or using their work computer, sources may have burned themselves already.

The Intercept has an [excellent guide](#) to reaching out anonymously. They are very clear both about how to reach out, and *what not to do*.

## What not to do if you want to remain anonymous

**Don't** contact us from work. Most corporate and government networks log traffic. Even if you're using Tor, being the only Tor user at work could make you stand out.

**Don't** email us, call us, or contact us on social media. From the standpoint of someone investigating a leak, who you communicate with, and when, is all it takes to make you a prime suspect.

**Don't** tell anyone that you're a source.

### Be clear about risk

Many existing resources fail to give would-be sources enough information about the risks associated with reaching out with sensitive information. News organizations can, and must, do better.

If someone's at risk of going to losing their job, going to jail (or worse) for reaching out to you, you owe them a sober explanation. Only promise the protection you know you can actually provide. Don't scare people unnecessarily, but do make sure they understand what they're getting into.

## 7.3.2 Onto The Tools

Many of us already have a professional email address, desk phone, cell phone, or social media accounts (eg. Twitter, Facebook) to gather information for stories. These are all great channels for less sensitive tips, but what do you do if you need to secure your communications?

### Common secure channels

Some common secure communication channels include [Signal](#), [WhatsApp](#), [Off-the-record messaging](#), and PGP for email encryption. Each has advantages and tradeoffs:

- [Signal](#) is a free and open source secure messaging app for [iPhone](#) and [Android](#), developed by [Open Whisper Systems](#). There is also a [desktop](#) application. Signal supports encrypted text messaging and phone calls. Signal's developers designed the service to retain as little metadata as possible: all they store is a user's phone number, sign-up time, and the time when the user was last active. Signal also allows messages to "self-destruct" automatically after a preset amount of time, leaving behind as little information as possible. For help getting started, read [Signal for Beginners](#).

- Tradeoffs: While Signal’s servers retain [very little metadata](#), the app is not designed to prevent live meta-data surveillance. The users in conversation should not be considered anonymous.
- [WhatsApp](#) has over a billion users on [iPhone](#) and [Android](#) and uses similar encryption to Signal. It’s easy to use, and with the right settings, can be a decent option for routine communications. WhatsApp users can share more types of files than Signal, and it can be a great way to send documents.
  - Tradeoffs: Importantly, some settings must be tweaked to maximize the security of the app, and to make it safer for routine use. Under some circumstances, WhatsApp backs up unencrypted messages to iCloud or Google Drive by default: users may need to confirm that backups are disabled. [Upgrading WhatsApp Security](#) is a good place to get started.
  - Like Signal, WhatsApp stores user phone numbers. They also [store substantially more data](#) – your address book, who you contact most often, and other information about how you use the service. WhatsApp [shares that data with their parent company, Facebook](#). Facebook, and WhatsApp can be forced to share their user data in response to a court order or subpoena.
- [Off-the-record](#), or OTR is a messaging encryption standard. OTR can be installed as a plug-in for messaging clients, such as [Pidgin](#) or [Adium](#), typically using an open messaging standard called [XMPP](#). OTR can encrypt communications on a variety of inter-operable messaging clients. The Electronic Frontier Foundation provides a primer on getting started with OTR for [Windows](#), [Mac](#), and [Linux](#). OTR allows users to accept messages from anyone using an OTR client, including some anonymity-protecting clients such as [Tor Messenger](#). If your contacts have the know-how, this can be an asset for protecting their anonymity.
  - Tradeoffs: Not everyone is familiar with OTR – you’re much more likely to receive an OTR message from a savvy user than anyone else. OTR should not be confused with the “off the record” setting in Google Hangouts.
- [OpenPGP](#) is an email encryption standard, most commonly used to secure email correspondence. Note that PGP (Pretty Good Privacy) and GPG (GNU Privacy Guard) are two implementations of the same standard, so you may see GPG and PGP used interchangeably. PGP uses public key cryptography: messages scrambled with a “public” key can only be unscrambled by the corresponding “private” key. The public key can be shared widely, so anyone can create a scrambled message that can only be read by the user who holds the corresponding private key. Users typically post their public key in an accessible place, such as a personal website, byline, or a [public keyserver](#). The Electronic Frontier Foundation has resources for setting up PGP on [Windows](#), [Mac](#), and [Linux](#).
  - Tradeoffs: PGP is famously tricky to use, even for security geeks. It’s easy to make a mistake that will compromise sensitive communications. And PGP only secures the body of an email: email addresses, timestamps and subject lines are all still sent in plaintext, exposed to eavesdroppers. You are likely to get more “return on investment” with simpler channels, such as Signal.

### Secure Organizational Channels

When done properly, physical mail and [SecureDrop](#) can both be good ways for sources to avoid giving personally identifiable information. The catch is, your sources have to know what to do.

- [Postal mail](#). Regular old-fashioned postal service physical mail is a solid way to receive sensitive tips because sources don’t need to provide a return address. The U.S. postal service does [collect images of the exterior of paper mail](#), so encourage sources to leave off the return address (or put it inside of the envelope). Physical mail can be a great way to send paper documents as well as electronic media, such as SD cards or small USB devices.
  - Tradeoffs: The main drawback is that mail is one-time communication. If you advertise your office address for accepting tips, encourage sources to give you a way to reach them if you have questions. Also, many workplaces are able to see who accessed a particular document, as well as review individual printer usage: a tipster who prints out a sensitive document at work may be caught by their own infrastructure before the document even reaches a newsroom.
- [SecureDrop](#) is an encrypted submission system that can help news organizations receive documents and exchange messages with sources. SecureDrop uses the Tor anonymity network, which encrypts and bounces web

traffic around the globe, making it much more difficult for eavesdroppers to determine the original source of a tip. This is one of the best options available for protecting confidentiality.

- Tradeoffs: Sources using SecureDrop don't have to provide identifying information unless they choose to do so. This added protection for sources can sometimes present challenges for newsrooms that need to verify the legitimacy of an anonymous leak.
- SecureDrop requires dedicated equipment and an administrator familiar with the basics of Linux and Bash shell. The SecureDrop docs provide a good overview of the process of [setting up SecureDrop](#). It isn't a trivial undertaking – this guide includes a whole [session on SecureDrop planning](#). And while some individual reporters have their own SecureDrop instances – [Bart Gellman](#) and [Wired's Kevin Poulsen](#) both do, in general SecureDrop should be an institutional tool.

### 7.3.3 Security is your responsibility

Conversations are only as secure as the least secure devices on your networks. Everyone in the newsroom should be educated about the risks of phishing and poor password hygiene.

Learn more about [how to keep newsroom accounts safe from hijacking](#).

### 7.3.4 Sample Pages

Note that a number of these pages use a customized subdomain that would alert an employer that an individual computer user had accessed the tips page.

- ProPublica: <https://securedrop.propublica.org/> (also: [How to Leak to ProPublica](#))
- The New York Times: <https://www.nytimes.com/tips>
- The Washington Post: <https://www.washingtonpost.com/anonymous-news-tips/> (also: <https://www.washingtonpost.com/securedrop/> and [Here's how to leak government documents to The Post](#))
- BuzzFeed: <https://contact.buzzfeed.com/>
- Associated Press: <https://www.ap.org/tips/>
- The Guardian: <https://securedrop.theguardian.com/>
- The New Yorker: <https://projects.newyorker.com/strongbox/>
- The Intercept: <https://theintercept.com/leak/> (also: [The Intercept Welcomes Whistleblowers](#))
- Vice: <https://news.vice.com/securedrop/>

### Recommended Reading

- [Opening Secure Channels for Confidential Tips](#) (Source, Feb 2017)
- [Protecting Your Sources When Releasing Sensitive Documents](#) (Source, June 2017)
- [Beyond Signal: Secure messaging channels & confidential tip pages](#) (NICAR, March 2018)