The Minimum Viable Teaching—When You Have No Time To Teach or They Have No Time to Listen

Sometimes there's no time for a full digital security walk-through. Your audience is suddenly about to face an unexpected set of risks. They could get overwhelmed or intimidated with too much information. They're short on time. You might have only one brief moment to make a difference, and you want to take full advantage of it.

Some security is always better than no security. You can do a lot to improve someone's basic security by walking them through some basic steps, and giving them some general advice.

At EFF, we're often asked to give advice in an incredibly short period of time: a TV or radio interview, or someone asking for help at one of our booths. Here's what we try to say in one minute or less. It's a concentrated form of advice. You could easily expand it into a half-day of teaching.

> "You can turn on encryption on your Android, iPhone, iPad or Mac. Pick a long password made up of six or more random words to lock your computer, or six or more numbers as a PIN to lock your phone. Don't reuse passwords! Use a password manager, or write down your passwords on paper and store it in your wallet instead. Turn on "two-factor" or "two-step" authentication on your Google, Facebook or other online accounts: this will help stop those logins from being hacked. Avoid clicking on strange links or email attachments. To send messages safely and securely, use an end-to-end encrypted messenger app like Signal or WhatsApp. If you want to be anonymous online, try using the Tor Browser."

Here's our thinking about each of those pieces of advice, and how you might expand on them, given more time.

Turn on encryption.

We say “turn on encryption” because that phrase typed into a search engine gives you good links to general instructions on encryption. (Unfortunately we can’t say “turn on encryption” on Windows, because only Windows Professional offers full disk encryption.)

Pick a long password.

“Long” is more understandable than “strong.” PIN is understood as the number that locks your phone, so you can extend this by including it in the same sentence to include desktop PC or laptop device logins. “Random” is a bit technical, but gets across the idea that it shouldn’t just be a familiar sentence. We spend a lot of time arguing internally about whether we should say “six” or “seven” words or digits!

Don’t reuse your passwords!

Reusing passwords is one of the top ways that accounts can be compromised, but it’s hard to stop people from doing it. Take this opportunity to introduce people to password managers. The phrase “password manager” may be new to people. You can introduce them to a number of password manager guides, such as the ones on SSD. Additionally, the surprising advice that one can write down passwords and keep them in their wallet often sticks in people’s minds, and gets across how bad password reuse is.

If people have questions about why passwords matter, you can show websites like https://www.HaveIBeenPwned.com/ and explain how password dumps can affect regular people.

Turn on two-factor authentication.

In an attempt to “avoid jargon,” almost every service uses a different term for two-factor authentication. We say “two-factor or two-step” to imply that it might be called a number of different things. We also give the basic reason why you should turn on two-factor authentication. Understanding why two-factor might protect you is difficult to understand, but the benefit is not.

If people have questions about how to tell what accounts offer two-factor authentication, direct them to websites like https://www.twofactorauth.org/.

Avoid clicking on strange links or email attachments.

We say this to reinforce the idea that you are most vulnerable to phishing when presented with links or attachments, but we have long internal debates about this advice too. Can anyone really go through life not clicking on any links or email attachments? Can anyone confidently tell when a link or attachment is “strange” (i.e. a fraudulent attempt to trick you into accepting malware onto your computer?). When given the opportunity to go into more detail, we often suggest that the recipients of strange attachments or links verify the weird email with the supposed sender in person or over the phone.

If you have better suggestions, let us know!

Use an end-to-end encrypted messenger app like Signal or WhatsApp.

Our first product mention! Break out the ™ symbols! As we explain in How to Recommend Tools, recommending specific software or hardware is complicated, but everyone in a training wants a concrete suggestion. Signal was one of the first audited, open source, messaging devices with a strong theoretical cryptographic foundation, backed by an organization specifically dedicated to providing secure end-to-end encryption. It suffers from some of the problems of a small and underfunded software project, but it is reasonably safe from compromise and has a broad user base.

WhatsApp’s parent company, Facebook, is not trusted by everyone, but the client itself is end-to-end encrypted, and (we believe) is unlikely to be undermined without a large and highly critical expert audience spotting the problem.

By offering two alternatives, we try to imply that the important thing here is “secure messaging app” rather than a particular secure messaging app. We put this advice at the end of our list, because at this point no one will remember much beyond the brand names.

To be anonymous online, use the Tor Browser.

People are often more curious about anonymity than fighting surveillance (they are more concerned about being generally exposed online than specifically monitored by the authorities).

Staying anonymous online involves more than just using Tor, but the Tor project does a good job of warning people who download their software about this. We try to convey that Tor is a solution for anonymity, and not one for defending against surveillance or other side-effects.

“Use Tor; Use Signal” is not always the best advice, but if you start searching for advice on Tor and Signal, there’s a good chance you will be directed to more detailed guidance by experts who know what they’re talking about.

Some other short resources:

EFF’s one pager on Surveillance Self-Defense:

https://www.eff.org/files/2017/06/19/ssd-one-sheet.pdf

Slightly longer advice with links.

Access Now’s First look at Digital Security.

https://www.accessnow.org/a-first-look-at-digital-security/

https://www.accessnow.org/cms/assets/uploads/2017/05/A-first-look-at-digital-security_DigitalCopy.pdf

Not specific advice, but an excellent, graphically-friendly way of getting someone quickly thinking about what they want to protect.

Seven Steps to Digital Security

https://ssd.eff.org/en/module/seven-steps-digital-security

A general guide from us that summarizes some general digital security principles.

Tech Solidarity Basic Security Precautions

https://techsolidarity.org/resources/basic_security.htm

A straightforward set of instructions that concentrates on U.S.-based activists and journalists.