Phishing and Malware: beginning

The most common threats your learners are likely to face online are links and files pretending to be something they're not — in other words, phishing and malware. Defending against these sneaky hacking strategies is less about downloading new tools or software, and more about building up learners' awareness and understanding.

Recommended Reading

- How to: Avoid Phishing Attacks
  Comprehensive guide to best practices
- Animated Overview: Protecting Your Device from Hackers
  A short (2.5 minutes) animation explaining malware— what it can do, how you can get malware from emails, USB, and links.
- Malware Handout
  A double-sided informative handout about malware, and protections against contracting malware on devices.
- How to: Protect Yourself Against Malware
  More targeted at preparatory protections from state-level actors. Good examples of phishing of sensitive targets.
- Digital First Aid Kit
  What to do if you suspect you've been targeted for phishing.
- PBS's Cybersecurity game has a phishing recognition quiz and other helpful guides:
  - Social Engineering Challenge
  - Recognizing phishing emails
  - Recognizing phishing sites
  - Recognizing phishy phone calls

Gotchas and Problems You Might Hit

A word of caution: Malware is a scary topic for many learners, and can move participants from an open place of learning new concepts, to feeling frozen by a fear-based mindset. Our recommendation is for facilitators to focus on the more common forms of malware for the communities they are teaching. For example, in the U.S. in 2020, most learners might find information on common malware and phishing attempts, adware, ransomware and stalkerware to be more personally relevant. It's better to avoid diving too deep into some of the more esoteric forms of malware you may have heard about that are relatively uncommon (e.g. state-level APT attacks such as what we cover in our malware handout), and to redirect those questions for 1:1 time after the main workshop has ended. Please be mindful of learners' engagement, and whether learners are too scared or distracted to absorb new information. If someone believes they have malware on their device, encourage them to reach out to you after the workshop for individual help. In many cases, the cause of feeling watched may be tied to needing to configure location and privacy settings in apps or social media, and may not be a malicious application. The facilitator should provide concrete strategies for learners who believe they may have malware on their devices.

Being mindful of resources: An additional challenge you may face is recommending software. In the course of talking about the importance of **software updates**, your participants may disclose or discover that they are using unlicensed or bootlegged software. Many people may have a barrier to acquiring licensed copies of software due to its cost, or not being aware of free software that receives regular updates. It's important to not shame the learner and to adopt a harm reduction approach. If you have time, you can assist learners with finding software that receives updates. For learners who are part of a nonprofit or civil society organization, you can encourage them to reach out to groups like TechSoup which help with discounted licenses for popular software. In addition, the facilitator can point the learners to using free, open source software alternatives that might meet the same need.

Being mindful of antivirus considerations:

Not all antivirus is created equal. Learners may ask the facilitator for advice in choosing antivirus. **In general, the antivirus that comes with the device may be best for most learners in a typical workshop.** However, if helping a learner who is concerned about a sophisticated adversary, such as an attacker with significant resources, the facilitator may want to provide additional guidance on looking at antivirus vendor websites with the learner. Things to look out for include: whether the antivirus software is regularly updated, whether it has good external reviews of its services, and whether the antivirus company website publishes threat research on a specific type of malware or type of adversary.

If someone reaches out to you about backups: Backing up data (or making "backups") is a great practice for being prepared against data loss. If a learner's device gets stolen, damaged, or infected by malware, having backups can be a significant relief to the learner, as the data can be restored to a device. As backups can take significant time, you may want to redirect specific questions about backups to after the workshop has ended. The facilitator can anticipate having to walk through the learner's threat model (e.g. Are they backing up data to an external hard drive or to a third-party cloud service? Are the backups encrypted? Do they have a strong password in place? Is that password memorized, or stored in a safe place like a password manager?).

If someone reaches out to you about wanting to wipe a device: A learner might ask for assistance with wiping their device. This may be best handled as additional follow up after a workshop has ended. Wiping a device is often a time-intensive ask and has additional threat modeling considerations. It requires walking through the learner's device settings (e.g. What led to their decision for wiping the device? Was the device encrypted? What kind of data was stored on there? Do they have the means to obtain a different device, if the problem on the old device persists?), as well as the learner's goals for wiping the device (is the intent to use the device uninfected? Or is it to sell the device after?), and who they might want to defend their data against. If appropriate, the facilitator may then want to share a few tutorials specific to the learner's needs.

If someone reaches out to you about malware after the training: If a learner has a unique malware consideration (falling outside of adware, for example), the facilitator may want to get in touch with a specialist. The facilitator may have to walk through additional information: for example, if a learner has received a phishing email, the facilitator may have to show the participant how to forward email headers.

If the learner is facing challenges that include physical security implications (such as stalkerware and APT attacks), be mindful that there are many ways to share unhelpful advice that have potential to put the learner at more risk. If the learner is concerned their location is being tracked by someone they know (such as in stalkerware and domestic violence situations), the facilitator may need to recommend using a different device (such as at the library, or borrowing the device of a trusted friend) to access specialized information, such as from groups like Operation Safe Escape. If the learner is from a heavily surveilled community and believes they may be the target of

an APT attack, encourage them to safely get in touch with groups like EFF's Threat Lab, The Citizen Lab at the University of Toronto, or CiviCERT.

Anticipated Questions and Answers

Q: What is the best antivirus program to use?

A: We tend to recommend using the manufacturer's own antivirus (AV) software (Windows Defender, Apple's built-in systems). Discussions about how badly-written antivirus software can make things worse can be dispiriting and don't provide solutions that participants can use.

Q: If you think you might be infected, what should you do?

A: You can go to the Digital Defenders' First Aid Guide. It's critical to make regular backups just in case your device gets infected. Wiping (or "factory resetting") your phone or laptop is also important. You can learn more here: https://www.digitaldefenders.org/digitalfirstaid/#section-malware

Q: We use attachments all the time! Are you telling me I can't send or receive documents?

A: Suggest using a shared store for frequent documents, like Dropbox or Google Drive. We talk a little about EFF's own practices here—we send documents, but we digitally sign our own messages, and encourage external groups to upload their files where we can examine them safely. You can also highlight that this is not an all-or-nothing proposal. You can certainly send and receive documents—and while you do, it's good, common-sense practice to be on the lookout for strange things that could indicate phishing and malware.

Q: How can I report phishing?

A: Emphasize the difference between mass phishing (like spam), and spear-phishing. Spear-phishing of a vulnerable group is something that researchers tend to be working on and interested in helping identify and prevent. You can email EFF at info@eff.org, or call Access Now's Digital Security Helpline (help@accessnow.org) for assistance. The U.S. Federal Trade Commission also collects examples of mass phishing, which can be forwarded to spam@uce.gov. The FTC's phishing page explains how to include useful information in that email.

Q: I am worried I am infected with malware. Can you check?

A: There are no consistent or obvious indicators of compromise for malware; slow computers and/or batteries that drain quickly, for example, have many alternative causes. It's very possible that an audience member may be infected with something from opening spam or generic phishing, and you can suggest installing antivirus software to check this possibility. For most communities, it is relatively unlikely that it will be from a targeted attack by a government or other large group. If you want to reassure your questioner, you can talk a little about the labor and research costs of sending targeted phishing emails.

Learning Objectives

Learners will:

- Be able to describe what phishing means.
- Understand why they may be a target of phishing.
- Be able to give some tactics to combat phishing.

Ratio

Instructor: Learners
1:10 (One instructor to ten students)

Suggested Materials

Malware Handout (English)

Relevant Articles

Lesson Content

Warmup

Get folks to talk about the terrible spam subject lines they've seen. People can check their spam inboxes (if they know where to find them), or you can just quote some that you've seen.

Some sources if you need suggestion include Busted: The Worst Email Subject Lines, Ever! and 19 Terrible Email Subject Lines

Follow up with additional questions, like:

- "Do you *just* get this sort of message via email? Has anyone ever gotten spam phone calls or text messages?"
- "What is spam trying to get you to do?" (Possible answers: Buy stuff, wire money, click on something, hand over credit card details, get involved in a scam)
- "If someone was trying to get you to click a link, how would they do it?"

Alternatively, ask learners to try and craft an email they'd send to someone else in the group in order to persuade them to click on a link. (This is best with groups where everyone is familiar or comfortable with having information shared with each other. Otherwise, pick a celebrity or a hypothetical made-up person.)

After some questions, you can offer a quick explanation along the lines of: "Phishing is a type of spam, in that's it's trying to get you to do something. But it's an attempt to get *information* out of you. Spear-phishing is when you or your organization are specifically targeted. Other types of dangerous spam will try to trick you to download and run a program that will spy on you, or make you pay to recover your files."

Knowledge Share

Phishing is an area where it's easy to overscare people, or prompt privacy nihilism. You want people to think about ways attackers could trick them—but not slip into believing that no one can be trusted, or that there is no way to guard against phishing emails. Remember: after scaring your audience with convincing emails, give them *solutions.* This can include ways to check headers, how to do out-of-band confirmation, opening documents in Google Docs, and turning on two-factor authentication.

We recommend moving from spam to phishing attacks because people often find spam attempts to trick them laughable. You can move the audience's perception of spear-phishing attempts from "super scary hacker skill" to "may be inept" depending on how apprehensive your audience is.

In general, people do not differentiate between programs that run locally and those that run outside their computer, and may not be able to recognize different types of documents. They are familiar with reading messages, and being asked to act on a message. Concentrate on increasing their vigilance when reading messages and

giving them protective steps they can realistically take rather than on what particular actions are dangerous and what are not. (For instance, instead of, “Don’t view PDF and Word documents,” say, “Think twice when an email asks you to click on something.”)

One of the key underlying points about phishing is *authentication*—how do you know who (or what) you’re talking to? How do you know the sender of the email is who they say they are? Is this strange email really from my colleague? Is this suspicious alert really from my bank? The solutions to this in spear-phishing are usually low-tech—calling a person or organization on a phone, spotting something that they wouldn’t normally say, navigating to a bank or organization’s website yourself instead of clicking any links, etc.

Once established, you can take this idea of the importance of “knowing who you’re talking to” and apply it to other, tougher, digital security concepts, like website certificates and signing.

Caution! People can react badly to the idea that they are being tricked, or push back against the idea that they might ever be tricked. Don’t try and play practical jokes on your audience, and don’t use intimate knowledge to construct phishing messages unless you’re very comfortable with the audience’s boundaries.

It can also help to share personal stories, if you have some, or generally highlight the idea that “This could happen to anyone!” This could sound something like, “Even though it’s not particularly high-tech, these phishing emails can be really sneaky. Believe it or not, I clicked on one from Bank of America several years ago—and then quickly realized what I’d done and called to cancel my card and get a new one!”

If people are embarrassed or ashamed, they will be less likely to get help or take action about a suspicious email. You can respond to this with something like, “Don’t be shy about getting a second pair of eyes on a weird email, or about calling a friend directly to make sure they sent it.”

If someone claims that they would never be fooled by an email, don’t challenge them. The chances are that everyone else in the room is accustomed to their attitude, and they won’t learn any better by being convinced that they will be fooled. Move the potential target from them, to those that they feel they must protect. (“You seem to have a very good shield against phishing! But supposing you knew someone who accidentally clicked on an attachment, and then all your personal details were exposed from their accounts. What would you want to teach them?")