CENTER FOR DEMOCRACY & TECHNOLOGY

A SERIES ON TECHNICAL RESOURCES IN EDUCATION

Prevention and Mitigation of Successful Phishing Attacks

The most common vector for cyber crime is *phishing,* where an attacker attempts to trick a user into taking a certain action in response to an email or other message like clicking on a link, downloading a file, or revealing personal or confidential information. The access gained by the attacker can provide them with a way to download malicious software onto the user's system, allowing them to steal data or damage the system.

There are two main kinds of phishing attacks:

- **General phishing messages**, which are sent to large numbers of people and are not specific to the user. Sometimes this can make them easier to spot, but they can still seem legitimate, like a request to fill out a new timesheet that appears to come from HR.
- **"Spear phishing" messages**, which use social engineering techniques to craft a message for a specific user, often referencing specific personal details. This can be used to make the email feel more urgent or important, making the user more likely to provide the requested information or open the malicious link.

The type of work done by an organization is likely to impact what kind of phishing attacks it is likely to encounter. Organizations like an unemployment agency or other benefits organizations, particularly those that handle financial benefits, are likely to be plagued by general attacks, as a relatively low effort way to try to glean personal information about large numbers of people in order to steal identities or acquire fraudulent benefits. On the other hand, some organizations, like schools, may see more targeted spear phishing attacks like a non-custodial parent trying to fool a teacher or counselor into divulging information about their child's class schedule or home address. Regardless of the type of organization they work for, it's important for all staff to be able to recognize any type of phishing attack.

Spotting a Phish

There are a few ways of spotting phishing attacks, whether they come in by email, social media, phone, or some other channel.

General Signs of a Phish

- **Manufactured urgency**: Many attackers will frame their phishes as urgent requests, such as needing a student's file right away to meet an enrollment deadline, in order to push the target to act quickly, before they have time to realize something is suspicious or odd.

- **Manufactured rapport or history**: Attackers may make it look like the request or attack is part of an existing relationship, such as by referencing a past conversation (which may never have happened). This is meant to give the target a sense of trust in the communication, or even push them into responding by making them embarrassed to not remember the "previous discussion."

Signs of Phishing in Email

- **Mismatched or suspicious headers**: An email header is the part of the message that shows things like the sender and recipient email and IP addresses, when the email was sent, and quite a bit of other information. Some email phishes (though not all) may have information in the header that show signs of a phish, like if the name of the sender does not match the email address, or if the email appears to be from someone within the target organization, but the address is from outside the organization (like a "colleague" emailing from a personal rather than work account). Most email programs do not show the full header by default, but IT staff will be able to dig into the header to find more information if the email seems suspicious.

- **Mismatched or suspicious links**: Many phishing attacks are trying to get the target to click a link that will prompt them to enter information or download a file. One sign of a phish is a link that appears to be for a trusted website, but actually leads somewhere else. In most browsers, hovering over a link will allow the user to see where it actually leads, rather than just where it appears to lead. If the address shown when hovering over a link is different than where the message states it should go, it might well be a phish. Other concerning signals of a phish are "spoofs" that use similar characters to mimic a trusted address, like "goog1e.com" instead of "google.com."

- **Unrequested files**: Attackers may also try to get users to download malicious files. Emails that sound like they are sending along a requested file, but where the recipient does not remember asking for the file, should be treated with caution, and the recipient should not download the file without first confirming its origin.

Signs of Phishing over Phone

- **Sensitive questions presented as standard**: Attackers may try to gain information by asking a sensitive question as standard, in hopes that the target will feel pressured to "follow the script" instead of calling out the unexpected question. If a question feels overly invasive for the context with no explanation of why it is being asked, that may be a sign of a phish.

- **Refusal to provide a callback number**: One way to check if a phone call is a phish is to call the caller back at a trusted number. So, if a caller claims to be calling from, say, the DMV, the recipient of the phone call should be able to hang up, and restart the conversation by calling the listed DMV number, maybe with the caller's personal extension. If a caller refuses to provide a callback number or extension, that can be a sign that they are not actually who they claim to be, as they are preventing the recipient from double checking their identity.

While these signals are important for spotting a phish, none of them is foolproof (a phishing email can have a perfectly legitimate seeming header, for example). It is important that staff have training on what to do when they encounter a phish or are simply not sure about a given interaction.

What to Do With a Phish

It is important for staff to know what steps they can take if they are concerned that they have received a phish. Fortunately, there are some best practices to follow:

- **Follow up with the sender**: If a recipient is unsure if a given communication is a phish, they should follow up with the sender on a different channel, if possible. So, if they received an email from a colleague that seems suspicious, they should call that colleague on the phone or stop by their desk to ask if they really sent the email. If they did not, the email is most likely a phish!

- **Report any suspicious emails:** Organizations need clear channels through which employees can report suspicious messages. Often, this will be to whoever manages the organization's technology – but whatever the case, staff should be given instructions and training on how to report.
  - Organizations should try not to take a punitive approach with users who report phishing, even if the user accidentally clicked a malicious link or incorrectly reported a non-phish. Generally, a punitive approach will discourage users from reporting, which will weaken the organization's cybersecurity (though if an employee has a pattern of falling victim to phishing and not taking the issue seriously, that may present a different case). It is critical that users feel comfortable reporting a phish, *especially* if they have clicked, downloaded, or given out information, because this gives the technical staff a chance to respond quickly, potentially minimizing any damage.

- **Do not engage with a suspected phishing message:** Recipients should not click links, download files, or respond to a message if they suspect that it is a phish, unless technical staff assures them the message is safe after investigating.

- **Train users to spot and handle phishes:** Because phishing attacks always go through users, a key element of defense is teaching users how to avoid falling victim to a phish. This means offering training, running simulated attacks to figure out where there is still confusion (and providing follow-up training to address any knowledge gaps), providing clear policies about how managers and the organization will request information from staff (i.e., it is not appropriate to ask staff to send information to an outside email address), and, as noted above, providing clear channels for reporting and support.

Phishing attacks are a key way that attackers gain access to systems, but it is also possible to minimize the success rate and impact of these attacks with the above information and best practices.

Further Reading

- https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
- https://www.cisa.gov/tips/st04-014
- https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/spam-and-phishing/
- https://www.phishing.org/what-is-phishing
- https://studentprivacy.ed.gov/sites/default/files/resource_document/file/W2%20Phishing%20Scam_0.pdf
- Reporting
  - https://www.cisa.gov/uscert/report-phishing
  - https://www.ic3.gov/Home/FileComplaint

This is one in a series of information sheets designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. More info: cdt.org/student-privacy/.