

THREE KEYS TO AVOIDING PHISHING EMAILS AND RANSOMWARE ATTACKS

Cyberattacks rely on human error.

Whether a large-scale onslaught or a smaller, more targeted campaign, all successful phishing and email-based ransomware attacks are disruptive and damaging on some level. And the simple reality is that they rely on human error; in order for cyberattacks to succeed, someone, somewhere, needs to take the bait. Cybercriminals utilize social engineering techniques—some basic and some very sophisticated—to manipulate human emotions and trigger a response.

It can feel overwhelming sometimes given that we, as the targets, need to be right all the time while the attackers only need to be right once. But the good news is that small steps can amount to big strides when it comes to protecting data, devices, and systems at work and at home. Here are three simple, practical cybersecurity awareness training tips you can use to identify and avoid malicious emails:

#1 Stop Skimming and Start Studying

We receive so many emails that we've conditioned ourselves to skim messages and make quick

decisions. But when we do this, we take unnecessary risks. That's because there can be clues both on the surface and just below the surface of the message that can alert us to things that aren't right.

For example:

- **“From” addresses, URLs, and embedded links can masquerade as things they aren't.** Do not take these items at face value (even if a name, logo, or other identifiers seem familiar and safe). On your PC, hover over—or “mouse over”—these pieces of content and examine the info that appears (you will often see the true destination of a web address in the bottom left of your browser window). On mobile devices, use a “long press” or “long click” and review the information in the pop-up window. If there appears to be a mismatch between what you expected to see and what is actually presented, steer clear.
- **The content or topic of a message might not be quite right or not fully relevant to you.** Be on alert if the tone of an email from a colleague, friend, or relative seems inappropriate or just doesn't “sound like” them. Likewise, be sure to question receipt of an invoice or shipping notification that doesn't make sense based on your ordering history. Thoroughly read what is written; don't just skim past details.
- **Misspellings and poor grammar can be indicators that the email did not originate from a trusted source.** This is particularly true with messages that appear to be from a well-known, well-established individual or organization.
- In general, any unsolicited email—that is, any email that you were not explicitly expecting to receive—should be looked at carefully. But you should **be particularly wary of any email that seems like it's designed to trigger an emotional response—**

fear, surprise, excitement, concern—and that urges you to respond or act in some way (click a link, download a file, confirm/change a password, etc.).

#2 Think It Through

After you read an email, take a moment to digest it. What you want to do is give yourself the space to act thoughtfully, rather than just reacting in the moment. To help get yourself out of the habit of skimming and reacting, consider asking yourself a few quick questions about any email that requests a response or action that could compromise sensitive data, devices, or systems.

For example:

- *Was I expecting this message?*— If the answer is “no,” ask more questions.
- *Does this email make sense?* – If the tone doesn’t seem right or the information you’re being provided doesn’t make sense, it could very well be a phish.
- *Am I being pushed to act hastily or out of fear?* – If you are, this is a major red flag.
- *Does this seem too good to be true?*—If you can’t believe what you’re reading, it’s likely you’re reading a phish.
- *What if this is a phishing email?* – This is a great question to ask yourself, because it can help you work

through the things that could happen if you’re dealing with a phishing attack. Could you be downloading malware that would corrupt all your files? Could you be turning over a password or credit card number to a criminal? Could you be exposing your coworkers’ private information to a scammer?

#3 Verify, Verify, Verify

So nice, it’s worth saying thrice.

It’s critical to remember that, with phishing scams, things are never what they seem. The reality is that a message can look and even sound legitimate but still set off a warning bell. For example, an email that comes from a corporate IT address and tells you to download new security software can seem trustworthy; it appears real and is on topic. But would that really be the process your IT department would follow?

If reading and thinking don’t get you to 100% confidence, you must take extra steps to verify that you are dealing with a legitimate request before you click a link, download a file, or reply with sensitive data. Here are some easy ways to confirm that the information presented in an email is legitimate:

- Instead of clicking on a link, open your web browser and type in a known, trusted URL and navigate to the site yourself.

- Instead of replying to an email or calling a number included in the message, do your own fact-finding. Use an email address or phone number that you are able to confirm.
- If you’ve received a questionable message from a colleague or friend, contact them via another channel (like a phone call or text message) to make sure they sent it.
- Reach out to your IT team for advice (and to alert them that there is a potential phishing threat active on your organization’s network).

It takes just a minute to confirm a questionable message, whether it comes from a coworker, internal department, financial institution, or other source. In contrast, it can take days or weeks (or even longer) to remedy the consequences of interacting with a phishing or ransomware email. And sometimes you can’t ever remedy the consequences.