OUCH! July 2022

The Monthly Security Awareness Newsletter for You

# Phishing Attacks Are Getting Trickier

Phishing attacks have become the most common method cyber attackers use to target people at work and at home. Phishing attacks have traditionally been emails sent by cyber attackers to trick you into doing something you should not do, such as opening an infected email attachment, clicking on a malicious link, or sharing your password. While traditional phishing attacks continue today, many cyber attackers are creating advanced phishing emails that are more customized and harder to detect. They are also using technologies such as text messaging, social media, or even telephone calls to engage and fool you. Here are their latest tricks and how you can spot them.

## Cyber Attackers Are Doing Their Research

Phishing emails used to be easier to detect because they were generic messages sent out to millions of random people. Cyber attackers had no idea who would fall victim; they just knew the more emails they sent, the more people they could trick. We could often detect these simpler attacks by looking for odd emails with “Dear Customer” in the beginning, misspellings, or messages that were too good to be true, such as Nigerian princes offering you millions of dollars.

Today’s cyber attackers are far more sophisticated. They now research their intended victims to create a more customized attack. Instead of sending out a phishing email to five million people, or appearing to be generic emails sent by corporations, they may send it to just five people and tailor the attack to appear to be sent from someone we know. Cyber attackers do this by:

- researching our LinkedIn profiles, what we post on social media, or by using information that is publicly available or found on the Dark Web.
- crafting messages that appear to come from management, coworkers, or vendors you know and work with.
- learning what your hobbies are and sending a message to you pretending to be someone who shares a mutual interest.
- determining you have been to a recent conference or just returned from a trip and then crafting an email referencing your travels.

Cyber attackers are actively using other methods to send the same messages, such as texting you or even calling you directly by phone.

## How to Detect These More Advanced Phishing Attacks

Because cyber attackers are taking their time and researching their intended victims, it can be more difficult to spot these attacks. The good news is you can still spot them if you know what you are looking for. Ask yourself the following questions before taking action on a suspicious message:

1. Does the message create a heightened sense of urgency? Are you being pressured to bypass your organization's security policies? Are you being rushed into making a mistake? The greater the pressure or sense of urgency, the more likely this is an attack.
2. Does the email or message make sense? Would the CEO of your company urgently text you asking for help? Does your supervisor really need you to rush out and buy gift cards? Why would your bank or credit card company be asking for personal information they should already have about you? If the message seems odd or out of place, it may be an attack.
3. Are you receiving a work-related email from a trusted coworker or perhaps your supervisor, but the email is using a personal email address such as @gmail.com?
4. Did you receive an email or message from someone you know, but the wording, tone of voice or signature in the message is wrong and unusual?

If a message seems odd or suspicious, it may be an attack. If you want to confirm if an email or message is legitimate, one option is to call the individual or organization sending you the message with a trusted phone number.

You are by far the best defense. Use common sense.

## Guest Editor

Phil Hoffman is a semi-retired IT consultant with 40 years of experience, focusing on infrastructure and security. He's a long-term contributor and editor for OUCH!, and is passionate about technology, bicycling and photography.

## Resources

**Social Engineering:** https://www.sans.org/newsletters/ouch/social-engineering-attacks/
**Top Three Scams:** https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
**Messaging Attacks**: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
**Phone Call Attacks**: https://www.sans.org/newsletters/ouch/vishing/
**Open Source Intelligence**: https://www.sans.org/newsletters/ouch/search-yourself-online/