

COMMON TYPES OF **PHISHING** ATTACKS AND HOW TO AVOID THEM



Use this job aid to help you recognize some of the most common types of phishing attacks in an effort to avoid falling victim to them.

In addition to carefully checking your emails to ensure they are legitimate, it is helpful to be aware of some specific types of phishing attacks, so you can recognize other hallmarks that could indicate something "phishy" is going on.

DECEPTIVE PHISHING

This is the most common type of phishing attack. You receive an email that appears to be from a well-known source, or one that you know personally. The email has the intent of tricking you into sharing confidential data by clicking a hyperlink in the email body and/or downloading a harmful file to your computer and network. Look for:

- A generic greeting or salutation, rather than one specifically addressed to you
- Grammatical mistakes in the body of the email, email address, and/or sender's alias
- Spelling errors

CLONE PHISHING

This type of cyberattack replicates notification emails from trusted organizations to scam users into sharing sensitive information like usernames and passwords.

SPEAR PHISHING

This type of phishing attack has the same goal as deceptive phishing but is a little more sophisticated. The scammer spends extra time on spear phishing emails in order to target a specific individual.

The scammer researches everything possible about you – first and last name, where you work and live, and other personal details about you from social media posts – in order to customize an email sent only to you. The scammer hopes to have a better chance of you responding to the email request because you may feel like the sender is someone you know or are otherwise connected to in some way.

To protect yourself against this form of phishing:

Use social media accounts wisely and be cautious with the information you make available for public viewing, including comments you make on other people's posts

Avoid making public posts about your company, your position, or other information that can help a scammer imitate personally knowing you to trick you into giving them access to confidential information

BUSINESS EMAIL COMPROMISE (BEC)

This type of fraud, also known as “whaling,” targets executives of companies. Scammers – who see this as an opportunity to catch “the big one” rather than just a “regular fish” – attempt to trick executives into giving out login credentials or other sensitive company information. The scammer can then use the stolen information for financial gain through wire transfers or other means.

Another version of this CEO fraud is when the scammer uses the same email account as a corporate executive to seek out employees' income tax information, commonly known as “W-2 phishing” in the US. With this information, the hacker can carry out a host of harmful activities including filing fake tax returns for employees and selling the information on the dark web, where it can be used for any number of future phishing scams and worse.

VISHING or VOICE PHISHING

In a vishing attack, email is no longer the method of contact. Instead, the scammer uses a phone call to reach you and attempt to steal your information.

There are various methods the hackers can use to have the phone call appear as if it's coming from someone else. Often, it looks like a number you'd recognize as an area of town you live or work in, or that is or is very close to an important number such as your bank or another company you are known to do business with.

To protect yourself, don't answer calls from numbers that don't display a valid name on the caller ID, and never give out personal information on an inbound (caller to you) call. If you answer the call, simply tell the caller you'll call them back at a contact number you already have for the entity. Get off the call as soon as possible, because they will be persistent to keep you on the phone and urge you to give out the information they're seeking. If possible, block the number to prevent them calling back. However, be aware that these callers will call from many different numbers.

SMISHING or SPIM (SPAM OVER INSTANT MESSAGING)

Smishing attacks happen via instant messages, including text messages, that are very similar to deceptive phishing emails. A message with a generic greeting that could be meant for anyone, not just you, is sent out to a large group of recipients in the hope that one person will “bite.” Similar to vishing, smishing scammers disguise themselves as a person, company, or other entity you might interact with on the phone

in hopes of getting you to take action on the message, such as opening a link or providing information that can be stolen or used to hack your device.

Defend yourself against smishing attacks by:

- Ignoring and deleting messages that appear to be spam and junk messages. For example, do not reply to a message about lost money someone found in your name.
- Researching an unknown phone number if you receive a message you're just unsure about. If it seems legitimate, call – don't text – the person or company to discuss the matter over the phone.

HTTPS PHISHING

In this type of phishing, attackers create fake websites that use HTTPS to appear legitimate. Victims are tricked into entering their credentials on these secure-looking sites.

PHARMING

This type of HTTPS phishing uses “cache poisoning” against a domain name system (DNS) to change the IP address of a legitimate and safe website so that visitors who attempt to go to that site are automatically redirected to a malicious site set up by the hacker.

The best defense against pharming attacks is security diligence. Your company no doubt maintains its antivirus protection and upgrades for the network and connected devices.

QR CODE PHISHING

This is a type of phishing that uses deceptive QR codes to lure users to visit fraudulent websites or download malicious files.

Only scan QR codes from trusted sources such as reputable businesses, official websites, or verified mobile apps. Be cautious of codes found in unsolicited emails, on unverified social media accounts, or in public places.