How to identify and avoid phishing scams

Phishing scams are one of the most common and most dangerous types of cyberattacks that businesses and individuals face. Cybercriminals often prefer this method because of its simplicity and rate of success. According to a report by cybersecurity firm F5 Labs, phishing scams incidents rose significantly during the COVID-19 pandemic, while Verizon reports that 32% of all data breaches in 2019 involved phishing.

What is phishing?

Phishing is a form of social engineering attack in which cybercriminals disguised as a trusted entity trick a victim into opening an email, instant message, or SMS. The victim is then duped into clicking on an attachment or a link that will either take them to a spoofed website to steal their private information or install malware on their computer.

Types of phishing scams

Phishing scams can be classified based on the medium used, which may include any of the following:

1. Email phishing

One of the most common types of phishing, email phishing involves sending an email with a message that asks the recipient to click on a link, download an attachment, make a payment, or reply with personal information. Variations of this method include spear phishing and whaling.

2. Vishing

In vishing or voice phishing, scammers will pretend to be calling from a government agency, bank, or even a police station to trick their victims into giving up sensitive information.

3. Smishing

Smishing or SMS phishing is similar to email phishing, but instead of using email, cybercriminals will send their victims text messages that come with either a malicious link or phone number.

4. Social media phishing

This type of phishing method involves the use of social media to launch scams — either via fraudulent posts or direct messages — to take advantage of unsuspecting users.

How to protect yourself from phishing scams

Fraudsters are getting more creative and devious nowadays, and by following these simple guidelines you can avoid getting scammed:

1. Do not open suspicious emails

Emails with subject lines such as "Account on hold," "Funds suspended," and other similar subject lines that evoke alarm or panic may be indicators of a phishing scam. Fraudsters use such subject lines to

capture their victims' attention and get them to open the email and click on a link and/or download an attachment in the email.

In addition, phishing emails will have misspelled domain names such as HR@m!crosoft.com or cred!tcard@cit1bank.com. If you receive emails like these, it's best to delete them or mark them as junk. If you're worried that your account may have been compromised, contact your bank or credit card issuer via their published phone number or secure messaging system.

2. Don't click on links and attachments
Randomly clicking on links and attachments coming from unknown sources increases your risk of being redirected to a fake website designed to steal your information, or being infected with malware that can damage or disable your device.

3. Install an anti-phishing toolbar
Most browsers can now be equipped with an anti-phishing toolbar capable of running checks on the sites you visit against a list of known phishing sites. In case you stumble upon a spoofed site, the anti-phishing toolbar will notify you immediately.

4. Beware of pop-ups
Some pop-up windows are phishing attempts often disguised as components of a legitimate website. Most browsers can be customized to block pop-ups, but if one manages to slip through, avoid clicking on any portion of the pop-up as this will take you to a phishing site. Instead, you can right click on the pop-up window on the taskbar and choose the "Close window" option.

5. Use firewalls, spam filters, and antivirus software
Firewalls monitor all traffic coming in and out of your network and decide which ones to block based on a predefined set of rules. They are your network's first line of defense against various cyberthreats such as phishing.

Spam filters are email features that sort out unwanted and malicious emails and prevent them from reaching your inbox. While they are not 100% effective, spam filters are essential to protecting your email account and make you much less vulnerable to phishing scams.

Antivirus software protects your computer from malware, phishing attacks, and other online threats. It can scan every file coming from the internet and prevent various types of malware such as viruses, Trojans, and spyware from infecting your computer.

6. Never give out your personal information
As a general rule, you must not share any personal or financial information over the internet. Legitimate organizations will never ask for such information via email, SMS, or social media. When in doubt, don't give it out and contact the company in question directly.

7. Keep your browsers updated

Security patches for browsers are released regularly to address security loopholes that cybercriminals can exploit. This is why you should download and install a browser update as soon as it becomes available.

Keep your business safe from phishing and other scams by partnering with a trusted managed IT services provider like Complete Document Solutions. Our cybersecurity solutions will provide you with powerful safeguards against all forms of cyberthreats. Call us today to learn more.