Don't take the bait; recognize and avoid phishing attacks

CANADIAN CENTRE FOR CYBER SECURITY

August 2022 | ITSAP.00.101

Phishing is an attack where a scammer calls you, texts or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source (e.g. from a bank, courier company).

Spear phishing: A personalized attack that targets you specifically. The message may include personal details about you, such as your interests, recent online activities, or purchases.

Whaling: A personalized attack that targets a big "phish" (e.g. CEO, executive). A scammer chooses these targets because of their level of authority and possible access to more sensitive information.

SMiShing: A phishing attack using SMS (texts). A scammer may impersonate someone you know or pose as a service you use (e.g. Internet or mobile provider) to request or offer an update or payment.

Quishing: A phishing attack using "quick response" (QR) codes which a scammer usually sends via email. The victim scans the QR code that re-directs them to a malicious website. Quishing can bypass your email security protection that scan for malicious links and attachments.

Vishing: Vishing is short for "voice phishing," which involves defrauding people over the phone, enticing them to divulge sensitive information. A scammer can use a voice over internet protocol (VoIP) system which allows caller ID to be spoofed to trick you into believing they are legitimate.

What Does a Phishing Attack Look Like?

Step 1: The bait

The scammer tailors a message to look like a legitimate one from a major bank or service. Using spoofing techniques the message is sent to numerous recipients in the hope that some will take the bait and fall for the scam.

In phishing and whaling attacks, the scammer first gathers details about the target individual or company. For example, the scammer can harvest information from social media profiles, company websites and internet activity to create a customized message.

In vishing attacks, the scammer might use a computerized autodialer (robocall) to deliver the fraudulent message to many victims.

Step 2: The hook

The victim believes the message is from a trusted source and contains information that entices them to take urgent action e.g. to resolve issues with their account.

If the victim clicks the link in the message, they will unknowingly be re-directed to the scammer's fake version of the real website. The victim provides sensitive information (e.g. login credentials) which is sent to the scammer. If the victim opens an infected attachment, a malicious code may get executed and infect their device.

In a vishing attack, if the victim respond by pressing a number from selected options, then they may get connected directly to the scammer.

Step 3: The attack

Credentials stolen—The scammer can now access the victim's account, e.g. email account to send more phishing emails to the victim's contacts. If the victim is an IT professional with privileged access, then the scammer can have access to sensitive corporate data or critical systems.

Malware installed—The scammer can use the malicious software to gain control of the victim's device, to steal their data, or lock access to their files until a sum of money is paid (as in ransomware attacks). Over the past 15 years, ransomware has become one of the most popular types of cybercrime.

In today's digital society, phishing attacks are so prevalent that no one is immune to them. Phishing is the number one technique cyber criminals use to infiltrate your network to install malware/ransomware or steal your data.

Scammers take advantage of times of crisis, conflicts, or world events (e.g. pandemic, civil unrest), to launch phishing attacks on financial institutions, governments, and critical infrastructure sectors. Political parties, politicians and individuals are often targets of phishing activity in the months leading up to an election in order to disrupt the democratic processes.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Don't take the bait; recognize and avoid phishing attacks

CANADIAN CENTRE FOR CYBER SECURITY

August 2022 | ITSAP.00.101

Protect your information and infrastructure:

- Verify links before you click them. Hover over the link to see if the info (sender/website address) matches what you expect
- Avoid sending sensitive information over email or texts
- Back up information so that you have another copy
- Apply software updates and patches
- Filter spam emails (unsolicited junk emails sent in bulk)
- Block IP addresses, domain names, and file types that you know to be bad
- Call the sender to verify legitimacy (e.g. if you receive a call from your bank, hang up and call them)
- Use anti-phishing software that aligns with the Domain-based Message Authentication, Reporting, and Conformance (DMARC) policy
- Reduce the amount of personal information you post online (e.g. phone numbers and extensions for employees)
- Establish protocols and procedures for your employees to internally verify suspicious communications. This should include an easy way for staff to report phishing attacks
- Update your organization's incident response plan to include how to react if you're hit with a phishing attack
- Use multi-factor authentication on all systems, especially on shared corporate media accounts

To find additional guidance and resources, you may refer to the following publications on our website:

- Tips for backing up your information (ITSAP.40.002)
- How updates secure your device (ITSAP.10.096)
- Protect your organization from malware (ITSAP.00.057)
- Secure your accounts and devices with multi-factor authentication (ITSAP 30.030)
- Spotting malicious email messages (ITSAP.00.100)
- Implementation guidance: email domain protection (ITSP.40.0645 v1.1)
- Security considerations for QR codes (ITSAP.00.141)

36% **THE NUMBER OF DATA BREACHES IN 2021 THAT INVOLVED PHISHING ATTACKS***

*Verizon's 2021 Data Breach Investigations Report

Watch out for unsolicited communications with:

- attachments
- hidden links
- spoofed websites
- malicious QR codes
- login pages
- urgent requests
- prompts for personal information
- caller claims to be government official or bank representative

Training and awareness can make a difference:

Your organization's users should know the importance of keeping their personal information and the organization's information protected. Users who are not educated on the warning signs of social engineering attacks might reveal information or infect the network's devices unknowingly. Having an informed workforce, with training on how to handle personal information (Privacy Awareness Training) and Cybersecurity Training, can reduce the risks of phishing attacks being successful. Also, implementing internal phishing simulations to enhance your employees understanding, allowing them to detect and avoid phishing attacks in a safe environment.

Something may be **phishy** if:

- you don't recognize the sender's name, email address, or phone number (e.g. very common for spear phishing)
- you notice a lot of spelling and grammar errors
- the sender requests your personal or confidential information, or asks you to log in via a provided link
- the sender makes an urgent request with a deadline
- the offer sounds too good to be true
- the caller's voice has a robotic tone or unnatural rhythm to their speech
- the call is of poor audio quality

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada