PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information like account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access their accounts.

Phishing Examples

The following messages, from the Federal Trade Commission's OnGuardOnline, are examples of what attackers may email or text when phishing for sensitive information:

> *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*
>
> *"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."*
>
> *"Our records indicate that your account was overcharged. You must call us within 7days to receive your refund."*

Simple Tips

- **When in doubt, throw it out:** Links in email and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the source – it's best to delete or, if appropriate, mark it as "junk email." Contact the company directly (via phone) to be sure the email is not legitimate.
- **Think before you act:** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- **Use stronger authentication:** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Install and update anti-virus software.** Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.
- **Be wary of hyperlinks:** Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.

Source:
U.S. Department of Homeland Security. *Stop. Think. Connect. Campaign*. "Phishing Tip Card."