PHISHING – AARP ARTICLE, SEPT. 2021

Phishing scams aim to acquire valuable personal and financial data, such as your Social Security number, credit card details or passwords for online accounts, to steal your identity, your money or both. They are mostly associated with email but can come in many forms, including social media messages, pop-up ads, “vishing” (voice phishing by phone), “smishing” (phishing by text message) and “pharming” (drawing victims to bogus websites).

By digital-age standards, it’s an old-school tool, dating to the mid-1990s, but phishing continues to grow in use and sophistication — and to respond to current events. The COVID-19 pandemic unleashed a bevy of fresh campaigns built around issues such as stimulus checks, vaccines and unproven treatments. The Internal Revenue Service, which disburses pandemic relief payments, said that in June and July 2021 reported phishing attempts "reached levels we haven't seen in more than a decade."

The scam often relies on impersonation, and phishers can be very good at it. They sound authoritative on the phone, trick caller IDs into showing a real corporate or government number and use well-known logos to make their emails and websites look genuine.

They bait the hook by promising goodies — free products or services, a big lottery prize, a government grant — or threatening legal or financial harm over a supposed unpaid tax or utility bill, for example. You might get a call or an official-looking email from your bank or from a tech company like Apple or Netflix, claiming a problem with your account.

You might even get a phishing email that appears to come from a family member, friend or work colleague. Some scammers hack accounts and gather personal details on victims to launch highly targeted attacks, a practice called spear-phishing. Global crime gangs use

phishing emails in widespread business swindles to penetrate companies' computer networks or trick employees into paying phony invoices.

Wherever their apparent source, phishing messages feign urgency (act now or you'll risk arrest/have your account frozen/miss out on this special offer). You'll be asked to quickly provide or "confirm" key pieces of personal or business information or be directed to click on a link, which might launch malware that harvests data from your computer or ransomware that takes over the machine and locks you out.

Email security company Valimail estimates that worldwide 3.4 billion fake emails are sent out every day. Take these precautions to help spot phishers and keep from getting reeled in.

Warning Signs

- Emails that contain one or more of the following:
    - A "Dear Customer" greeting — legitimate communications from companies you do business with usually include your name
    - Offers of free products or services, super-cheap travel deals, or a sweepstakes prize or other financial windfall
    - Vague or generic language, such as "payment issue," to describe a problem with an account or purchase
    - Threats of dire consequences, such as legal action or an account being frozen, if you don't act immediately
    - Requests that you click a link, open an attachment, or reply with personal or financial information to take advantage of an offer or to resolve a problem
    - Multiple spelling and grammar errors — many phishing scams originate abroad
- Pop-ups on your computer or mobile device that warn of viruses, promise a prize or redirect you automatically to another site

- Unsolicited phone calls or texts that pitch free or super-cheap products and services, or that claim to be from a government agency, public utility, bank or major company

How to protect yourself from this scam

- Do check the “From” address. If an email says it’s from Apple or Bank of America but comes from, say, a Gmail account or an address with a foreign domain, it’s phony.
- Do mouse over links in suspicious emails to reveal the true destination. Pasting the URL into a safety checker such as VirusTotal or Google Safe Browsing can tell you if it presents a phishing or malware risk.
- Do use anti-virus software and keep it up to date. Activate firewalls and other settings that block malicious files.
- Do vary the passwords on your online accounts, which can minimize the damage if you are phished or hacked. Change passwords immediately if you suspect a breach.
- Do forward phishing emails to the Federal Trade Commission (FTC) and the company being impersonated (see “More resources” below). Include the full email header, which tells investigators more about the sender. If you don’t know how to do that, search for the name of your email service (for example, Outlook, Yahoo or Gmail) and “full email header.”
- Don’t give out personal or financial data such as your Social Security number or account numbers in response to an email or an unsolicited call. A company or government office contacting you on legitimate business will not ask you for such information.
- Don’t click on a link or open an attachment unless you are certain the email comes from a trusted source.

- Don’t click links or call phone numbers provided in an unsolicited email or call. To check whether a business or government agency is really trying to contact you, use its legitimate customer-service email or hotline, which you can find online or on account statements.
- Don’t click on or call phone numbers in suspicious pop-up ads. To close a pop-up safely, find the corresponding icon on the task bar at the bottom of your screen, right-click, and select “close” or “quit.”
- Don’t drop your guard because an email features a company’s real branding or appears to come from someone you know. It could be the product of corporate “spoofing” or a hack of your friend’s email account.
- Don’t assume a website is safe because it is encrypted. Encryption, signified by a padlock icon or “https://” in front of the URL, means data you transmit to a site can't be intercepted by third parties — but it doesn't mean that receiving site is legitimate. Many phishing sites now use encryption, knowing fraud-savvy consumers look for it, according to the Anti-Phishing Working Group, a global antifraud coalition.

More Resources

- Forward phishing emails to the FTC at spam@uce.gov, and to the business or organization the sender claims to represent. Many companies have dedicated email addresses to report phishing, which you can find online.
- If you are victimized by a phishing scam, file a complaint with the FTC (online or at 877-382-4357) and visit the agency’s Identitytheft.gov site for tips on how to limit and repair the damage.
- If you are phished by email or other online means, report it to the FBI’s Internet Crime Complaint Center.