Phishing

Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both.

Scammers also use phishing emails to get access to your computer or network then they install programs like ransomware that can lock you out of important files on your computer.

Phishing scammers lure their targets into a false sense of security by spoofing the familiar, trusted logos of established, legitimate companies. Or they pretend to be a friend or family member.

Phishing scammers make it seem like they need your information or someone else's, quickly – or something bad will happen. They might say your account will be frozen, you'll fail to get a tax refund, your boss will get mad, even that a family member will be hurt or you could be arrested. They tell lies to get to you to give them information.

Be cautious about opening attachments or clicking on links in emails. Even your friend or family members' accounts could be hacked. Files and links can contain malware that can weaken your computer's security.

Do your own typing. If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself. Even though a link or phone number in an email may look like the real deal, scammers can hide the true destination.

Make the call if you're not sure. Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick

up the phone and call them yourself using the number on their website or in your address book, not the one in the email.

Keep your security up to date. Use security software you trust, and make sure you set it to update automatically.

Report phishing emails and texts.

- Forward phishing emails to spam@uce.gov – and to the organization impersonated in the email. Your report is most effective when you include the full email header, but most email programs hide this information. To ensure the header is included, search the name of your email service with "full email header" into your favorite search engine.
- File a report with the Federal Trade Commission at FTC.gov/complaint.
- Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.
- You can also report phishing email to reportphishing@apwg.org. The Anti-Phishing Working Group – which includes ISPs, security vendors, financial institutions and law enforcement agencies – uses these reports to fight phishing.

Source: Federal Trade Commission: Consumer Information