Phishing

By:Federal Trade Commission

When internet fraudsters impersonate a business to trick you into giving out your personal information, its called phishing. Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don't click on links within them either-even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels.

Examples of Phishing Messages

You open an email or text, and see a message like this:

"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 7 days to receive your refund."

The senders are phishing for your information so they can use it to commit fraud.

How to Deal with Phishing Scams

Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text.

The messages may appear to be from organizations you do business with – banks, for example. They might threaten to close your account or take other action if you don't respond.

Don't reply, and don't click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.

Area codes can mislead, too. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn't guarantee that the caller is local.

If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

Action Steps

You can take steps to avoid a phishing attack:

- Use trusted security software and set it to update automatically. In addition, use these computer security practices.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information.
- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.

Report Phishing Emails

Forward phishing emails to spam@uce.gov — and to the company, bank, or 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 find out how to include it, type the name of your email service with "full email header" into your favorite search engine.
You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group — which includes ISPs, security vendors, financial institutions and law enforcement agencies — uses these reports to fight phishing.
If you might have been tricked by a phishing email:

- File a report with the Federal Trade Commission at www.ftc.gov/complaint.
- Visit the FTC's Identity Theft website. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.