WHAT IS PHISHING AND HOW TO SPOT A POTENTIAL PHISHING ATTACK

Phishing is an email fraud method in which the perpetrator sends out legitimate looking email to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. These email messages often provide links to fraudulent websites where you are asked to disclose credit card numbers, social security numbers, or other private information.

Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information. Spear-phishing attempts are not typically initiated by random hackers, but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

Whaling phishing is a type of fraud that targets high-profile end users such as C-level corporate executives, politicians and celebrities.

How does phishing work?

- Typically, you'll receive an email that appears to come from a reputable company that you recognize and do business with (such as your financial institution, government agency, or a credit card company), but phishing can also occur by phone.
- The message will describe an urgent reason you must verify or re-submit personal or confidential information by clicking on a link embedded in the message.
- The provided link appears to be the official website of the company, but in phishing scams the website is fraudulent.
- The fraudulent website asks you to provide information used to verify your identity such as mother's maiden name or place of birth, Social Security numbers, account numbers and passwords.
- Once this information is provided, those perpetrating the fraud can begin to access your accounts or assume your identity.

How to protect yourself

- Never provide your personal information in response to an unsolicited request.
- If you believe the contact may not be legitimate, contact the financial institution yourself.
- Never provide your password over the phone or in response to an unsolicited Internet request.
- Review account statements regularly to ensure all charges are correct.
- Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- If you fall victim to attack, act immediately to protect yourself by alerting your financial institution(s) and placing fraud alerts on your credit files.