WHAT IS PHISHING?

Phishing is where scammers use email or text messages to trick you into giving them your personal and financial information. But there are several ways to protect yourself.

1. Protect your computer by using security software.
2. Protect your cell phone by setting software to update automatically.
3. Protect your accounts by using multi-factor authentication.
4. Protect your data by backing it up.

1. WHAT TO DO IF YOU SUSPECT A PHISHING ATTACK

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question:
'Do I have an account with the company or know the person who contacted me?'
If the answer is "No," it could be a phishing scam. Report the message and then delete it.
If the answer is "Yes," contact the company using a phone number or website you know is real — not the information in the email. Attachments and links might install harmful malware.

2. WHAT TO DO IF YOU RESPONDED TO A PHISHING EMAIL

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to www.identitytheft.gov. There you'll see the specific steps to take based on the information that you lost.
If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan and remove anything it identifies as a problem.

3. HOW TO REPORT PHISHING

If you got a phishing email or text message, report it. The information you give helps fight scammers.
If you got a phishing email, forward it to the Anti-Phishing Working Group at www.reportphishing@apwg.org
If you got a phishing text message, forward it to SPAM (7726).
Report the phishing attempt to the FTC at www.ReportFraud.ftc.gov