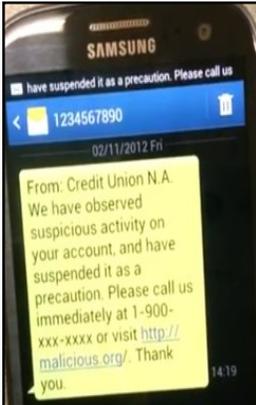


PHISHING - WHAT TO DO IF YOU HAVE BEEN HOOKED



Phishing is when someone tries to trick you, by phone or through the Internet, into providing personal information.

They may pretend to be from trusted financial institutions, credit card companies, or a law enforcement agency.

Examples of phishing messages provided courtesy of the Federal Trade Commission (FTC):



"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."

Forward phishing emails to:

- The FTC - spam@uce.gov
- Company; Bank; or Organization impersonated in the email.
- You may also report phishing email to the Anti-Phishing Working Group (APWG) at:
reportphishing@antiphishing.org

If you might have been tricked by a phishing email:

- File a report with the FTC at: www.ftc.gov/complaint
- Visit the FTC's Identity Theft website. Victims of phishing could become victims of identity theft.

