Say No to Phishing and Other Online Scams

NEVER Do These Things!!

– They are Sure Signs of a Scam. – End the Conversation NOW!

1) **NEVER Pay with Gift Cards! or other non-refundable methods**, (such as Western Union, MoneyGram, CheckFreePay, Bitcoin/Cryptocurrency)
   a) Any legitimate business will take a Credit Card for payment.
   b) No, your boss or church/civic leader will not ask you to buy gift cards in a simple text or email!
   c) **Be Careful!** If you pay with Zelle, Venmo, etc. ONLY do so with previously established business relationships or someone you know in person.
2) **NEVER give out a 2FA/MFA PIN Code!!** (Sent via Text, Email, or Voice message). If someone asks for it, hang up or end the conversation!! Guaranteed scam!
   a) That 2FA PIN code is ONLY for you to use when logging into your own account.
   b) NO Legitimate company will EVER ask for the 2FA PIN code!! Only a Scammer will!
3) **Never call a phone number given in an email, SMS, or website/computer pop-up!**
   a) If you need to access a company, login through normal methods, or lookup the number and then call.
4) **Don't believe pop-up messages from your computer/web browser**, saying you need to contact "tech support" because you have a virus, or you need to update a program by clicking a link.
   a) Just update your programs as you always do! (Make sure your computer or smartphone is set to "automatically update".)
5) **Never allow someone to take over remote control of your computer!**
   a) Unless it is a trusted family member, friend, or from your employer, no legitimate support person in today's world ever needs to take control of your computer remotely. Don't allow it!

INSTEAD, Always Do These Things!

1) **Slow down! Stop. Breath. Don't Panic. Ask someone** to help confirm/validate. (No shame in asking for a second opinion!)
2) **Be VERY suspicious if a person/business is not in your Contact list**!
   a) If they ask for action or information, first use a known method to confirm their true identity, such as hanging up, looking up the real phone number, and calling back; no matter how convincing they are!!
3) **Only answer phone calls from people/businesses in your Contact list.**
   a) Unless necessary, **do not answer phone calls from numbers you don't know**. If it is legitimate, the caller can leave a voice message.
   b) It's easy for scammers to **spoof a Caller ID** and appear to be your bank or anyone! Don't answer!
   c) If you answered, but it sounds odd or you are asked to take action or reveal personal information, then: "**Hang up; Look up (the number); Call back**." (A legitimate business will respect you for that.)
4) **Contact a business via normal means** (like your app, normal website, phone number from account statement, etc.). Not from a website link or phone number emailed to you, or a text message alert received supposedly from a business.
5) **Validate Domain Name in (1) email addresses or (2) URL/website links**.
6) **Only pay via Credit Card**, not via non-refundable method. (Except in established friendships or normal account transactions with previously established businesses.)
7) **Be wary of unusual requests. If it seems odd, it probably is!** Even if talking to someone in your Contacts; their account may have been hacked. You may not really be talking to them!
8) **Hang Up, if you are being pressured to stay on the phone and not allowed to check with someone else**, this is a SCAM!! No legitimate business will excessively warn or threaten you!

Should You Ever Do These Things?!
– First Think Hard About It & Validate it is Legitimate!

1) **Should we ever click website links (URLs) or open an attachment in emails or text messages (SMS)**?!
   a) This is a common method of tricking you! Many links and attachments are scams or install malware!
   b) This may be ok if it is part of an established business relationship and a regular means of communication. Ask yourself the following:
      i) Is it from a legitimate business you have a relationship with?
      ii) Were you expecting this email or text message about this topic?
      iii) Is this their normal way of communicating? Is this a normal request?
   c) **Validate the email sender and the URL website link or attachment!**
      i) Is it really from the person it says it is from? Check the actual email address, not just the sender display name.
      ii) Does the URL/weblink point to the legitimate company website? (Hover over the displayed text to see the actual URL destination.)
   d) Even then, **WHY CLICK** on that link or **WHY OPEN** that attachment?! You know their website. Why not instead just login using your normal method? If it is legitimate, the information from the URL link or the attachment should be available when you login to their website.
2) **Should we ever fully trust someone we have only met online**?!
   a) Do you really know who you are talking to? Even in a long-term online "friendship"?
   b) Artificial Intelligence (AI) makes it easier to pretend to be someone else. Be aware of Deepfakes!
   c) Fraudsters and criminals are creating complex and realistic social media personas.
   d) Some of the most devastating scams come from long-term, trusted relationships. E.g. romance scams and Pig Butchering scams.

Important Resource: "What To Do if You Were Scammed"

From the Federal Trade Commission: consumer.ftc.gov/articles/what-do-if-you-were-scammed

Resources for Further Learning:

1) "Resist Social Engineering" Section here:
   www.ComputerSecurityNW.com/4-critical-items
2) "What are phishing scams — and how to avoid them"
   www.tomsguide.com/reference/what-are-phishing-scams
3) Excellent videos of hacking and scams: www.socialproofsecurity.com/
   a) Like this one: "Phishing you: Inside the mind of an ethical hacker" youtu.be/UwPK_ietuxg
4) Watch anything by Dr. Jessica Barker on YouTube
   a) Like this one: "Why romance scams work (You're not stupid)"
      www.youtube.com/watch?v=_LEuBmJ8bUE
5) Anything from Brian Krebs, like: "When in Doubt: Hang Up, Look Up, & Call Back"
   krebsonsecurity.com/2020/04/when-in-doubt-hang-up-look-up-call-back/

Definitions Used in This Handout:

"**Phishing**" = A cybercrime in which someone (posing as a legitimate person or institution) contacts you by email, phone, or text message to lure you into (1) providing sensitive data (such as personal information, banking details or passwords), or (2) to click a website link, or (3) to open a malicious document. See: www.phishing.org/what-is-phishing

"**Social Engineering**" = "human manipulation" = A form of psychological manipulation that attempts to trick someone into revealing sensitive information (e.g., a password) or taking actions for the advantage of a hacker. It attempts to exploit the vulnerability of human emotions to create cybersecurity errors that can be taken advantage of.
See: csrc.nist.gov/glossary/term/social_engineering and training at 405d.hhs.gov/knowledgeondemand/social-engineering