Say No to Phishing and Other Online Scams

NEVER Do These Things!! Sure Signs of a Scam. – End Conversation NOW!

1) **NEVER Pay for Services 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 PIN Code (used for 2FA/MFA)!!** (Sent via Text, Email, or Voice message). If someone contacts you and 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) The only time you might have to provide a PIN code is if you initiate the call or walk into a business.
   c) NO legitimate company will ever call/text and 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 devices are set to automatically update.)
5) **Never allow someone to take over remote control of your computer!** (The method may begin by asking you to download software like AnyDesk, TeamViewer, UltraViewer.)
   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!
6) **Don't answer phone calls from people/businesses not in your Contacts, unless necessary**.
   a) **If you must**, and the call is from an important business (your bank, IRS, Amazon, etc.), don't engage!
      i) It's easy for scammers to **spoof a Caller ID** and appear to be your bank or anyone!
      ii) Only calls you initiate can be trusted. Hang up, look up the number, and call back.
   b) Best not to answer these calls! If they are legitimate, the caller can leave a voice message.

INSTEAD, Always Do These Things!

1) **Slow down! Stop. Breath. Don't Panic. Ask someone** for a second opinion. (No shame in asking!)
2) **Be VERY suspicious of calls (or texts) that you did not initiate (esp. from businesses)!**
   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, even then …**
   a) 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, computer pop-up, phone number in email, or a text message alert.
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, pressure, or threaten you!

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

1) **Should we ever <u>click website links</u> (URLs) or <u>open an attachment</u> 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's "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) <u>Even then</u>, **WHY CLICK** on that link or **WHY OPEN** that attachment?! You know their website. Why not instead just login via 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 or app.
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 or stealing them.
   d) Some of the most devastating scams come from long-term, trusted, online-only relationships. E.g. romance scams, Pig Butchering, and sextortion.

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) "Cybercrime Support Network" FightCybercrime.org
3) "What are phishing scams - and how to avoid them" www.tomsguide.com/reference/what-are-phishing-scams
4) 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
   b) Anything by Dr. Jessica Barker on YouTube, 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/
6) Caller ID Spoofing: www.fcc.gov/spoofing

<u>Definitions Used in This Handout</u>:
"**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 <u>vulnerability of human emotions</u> to create cybersecurity errors that can be taken advantage of.
"**Phishing**" = A type of social engineering 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, (3) to open a malicious document, or (4) take action (call a number, buy a gift card, etc.).