Financial Literacy Event Handout

Do Your Part, Be Cyber Smart

EVENT KEY NOTES

✓ Goals of Social Engineering

- There are generally two goals that come out of social engineering:
    1. Access
    2. Data
- Once access/data are received there is often a financial motive.
- Social engineering is not always driven by finances but there is always a motive.

✓ Social Engineering – How It Works

- 60% of businesses fall victim to social engineering.
- Social engineering works because it's easier for hackers to exploit the natural inclination to trust someone than to figure out a new way to access a computer.
- The key is training and education!

✓ Phishing

- **Phishing:** The activity of defrauding an online account holder of financial information by posing as a legitimate company. Phishing season is year round.
- Phishing uses open source intelligence (LinkedIn, Company Website, etc.) to catch the "Big Fish" (CEO, CFO, President, etc.).
- **Spear Phishing:** fraud attempt targeting a specific individual/organization.
- If you think you have a phish – REPORT IT!
- **Cost:** Fraudsters could get their hands on everything in your bank account or life savings.
- 95% of successful cyberattacks are the result of a phishing scam.

✓ Common Scams

- **Lottery/Sweepstakes Scam:** You receive a letter with a large-dollar check that you are asked to deposit into your personal checking account; however, you need to immediately wire a portion of the funds to cover various taxes and administrative fees.
- **Online Dating/Romance/Friendship Scam:** A participant on an online dating site or chat room begins communicating with you via instant messaging. After some time goes by and they gain your trust, they mention some personal financial difficulties. They want to have the funds sent to you because they are out of the country and can't access their bank account from where they are. They then will have you wire the funds to them
- **Work At Home/Work Out of the Home Scam:** You apply for a job online. The employer sends a check that includes not only your salary, but funds to purchase the supplies you'll need to complete the work. The employer asks you to deposit the check and wire a portion of the first check to cover the supplies.
- **Mystery Shopper Scam:** You apply for a position to be a mystery shopper. You receive a package containing instructions and evaluation forms for your first assignment. You also receive a check that includes your salary for the assignment as well as the amount you will use in your mystery shopping. You are instructed to deposit the check to your personal account and withdraw cash to take to a money transfer service at a local retail store. You are asked to wire the money so that you can evaluate the customer service.
- **Online Sales Scam:** You are selling an item via an online auction site. The purchaser mails a check for more than the final sales amount. The purchaser explains this was a mistake and to save time they ask you to go ahead and deposit the full amount but wire them the difference.
- **Grandparent Scam:** You get a call from someone claiming to be your grandchild. They tell you they are not at home and have either gotten into a car accident or gotten into trouble with the law and ask you not to tell their parents. They then ask that you wire them money to cover the cost of the dilemma they are in.
- **Tax Scam:** A fraudster will pose as the IRS or Department of Justice informing you that you owe back taxes or underpaid your taxes. They will then be instructed to pay or have a warrant issued for your arrest.
- **Contractor Scam:** Neighborhoods with a high concentration of older residents are frequently targeted by individuals that pose as contractors and claim to have identified something on your

Financial Literacy Event Handout

home or property that needs to be repaired (e.g. driveway, roof, clogged drain pipe, etc.). The fraudster will demand payment up front. The homeowner will find that the work completed is shoddy and the expense is not in line with what was actually done. The contractor is usually unlicensed.

- **Charity Scam:** You will receive a solicitation to support a charity that doesn't really exist and the funds donated are leveraged for the fraudster's personal use.

✓ Multi-Channel Fraud

Occurs when more than one channel is used to conduct fraud. Money comes into an account and promptly leaves the account.

- Fraudulent Mobile Deposits → Customer Withdrawals Funds → Western Union/Money Gram/ gift cards.
- Incoming Wire → Online Banking Credentials Compromised → Debit Card sent to new location Fraudulent ATM Withdrawal

✓ Ransomware Preparation

- Have an anti-virus program on your computer.
- Always back up your data.
- Don't click the link! Ransomware generally starts with a fraudulent link or attachment

✓ Account Takeover

An account takeover of a business is where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transfers to accounts controlled by the fraudsters.

✓ Cyber Security Tips

- Create strong passwords for your accounts and update your usernames and passwords regularly.
- Always be sure to have the most up-to-date anti-virus software and anti-spyware installed on your home computer.
- Don't respond to online solicitations from people you don't know.
- Don't overshare your personal information, which would be used by banks or companies to verify your identity, on social media. Be sure to set your social networking profiles to private. Be careful what you post online.
- Don't click on links, open attachments or provide sensitive information through an email or text message, even if the sender appears to be a reputable company or someone you know. Instead call that company or individual to inquire if they sent you an email or text message.
- Shred documents that contain personal information before you discard them.
- Be careful what you do on public Wi-Fi hotspots. While they can be great for convenience, avoid conducting financial transactions on them.

✓ Fraud Resources

Agencies that provide fraud awareness, prevention tips, resources as well as fraud and identity theft reporting tools.

- Contact your financial institution.
- Report the scam to authorities.
- Change your online passwords.
- Federal Trade Commission
  https://www.ftc.gov
- Internet Crime Complaint Center
  https://www.ic3.gov
- Identity Theft Resource Center – 1.888.400.5530
  https://www.idtheftcenter.org
- U.S. Postal Service
  https://postalinspectors.uspis.gov
- Have I Been Pawned
  haveibeenpwned.com