Financial Fraud: *Social Engineering*

Scammers use **social engineering**, such as impersonating a trusted entity or person, to trick victims into providing personal information or sending money. Fraudsters target individuals by gathering information posted on social media or other easily accessible sources to create convincing stories.

Types of Social Engineering Financial Scams and How to Spot Them:

Prize Scams – scammers contact a victim by phone, text, email, or letter to say that they have won a sweepstakes, the lottery, or some other prize.

Debt Assistance and Loan Scams – *scammers* offer consolidation of debt or debt relief assistance in return for a fee paid upfront.

Romance Scams – scammers make fake profiles on dating sites, applications, or social media and contact victims in hopes of developing a relationship, building trust, then asking for money.

Family Emergency Scams – fraudsters spoof a relative's phone number or hack into their email and send a message asking for money due to a medical emergency or financial hardship. Fraudsters use AI to create cloned voices impersonating family members to entice victim to send money.

Government Officials / Law Enforcement Impersonation – scammers pretend to be a government official or law enforcement officer, informing their target that they need to act promptly.

Tech Support Scams – fraudsters contact victims and convince the victim they have a problem with their computer that needs to be fixed for a fee.

Fraud Prevention Recommendations

- **Do not act immediately.** Stop and talk to someone you trust about the situation and seek guidance from the organization's official website.
- **Watch for scam indicators in the method of payment being requested**: scammers often ask for payment in formats that can be more difficult to trace, such as reloadable or prepaid gift cards, cryptocurrency, or money transfers, which can be initiated with a debit or credit card transaction. Sending cash or initiating wire transfers or other types of money transfers are also popular requests from fraudsters.
- **Use caution when posting on social media**. Be aware that sharing sensitive personal information can provide criminals with clues to answer your security questions or craft believable, targeted scam messages.
- **Use cybersecurity best practices**, such as enabling anti-phishing protection on your web browser, avoiding clicking on unsolicited or unknown links, adding multi-factor authentication to account log ins, and using strong, unique passwords for different accounts.

To learn more about protecting yourself from financial fraud, visit:
https://usa.visa.com/visa-everywhere/blog.html

VISA
everywhere you want to be