Fraud Prevention and Information Security

Presented by:

Citizens National Bank of McConnelsville

Different Types of Fraud/Theft:

- Advance Fee Fraud
- Affinity Fraud
- CATO (Corporate Account Takeover)
- Counterfeit Instruments
- Data Breaches (Internal and External)
- Skimmers
- Social Media/E-Mail Fraud

Advance Fee Fraud

Promise to send money or provide a service or product in exchange for an upfront fee

Examples of Advance Fee Fraud:

Scammers will use various terms, such as fees and taxes, to mask their fraudulent intent. In exchange for an upfront fee, promises can include:

- Money, services, or products: Nigerian Prince scams
- Opportunities to participate in special deals: insider information
- Purchases/sales: fraudulent Craigslist ads

Safeguards and Solutions:

- If it sounds too good to be true, it probably is – use common sense
- Know any individual or company before entering in a business transaction with them
- Verify funds of any suspicious items, such as personal checks, cashier's checks, etc.

Affinity Fraud

Targets identifiable groups by pretending to be a member of the group to defraud them

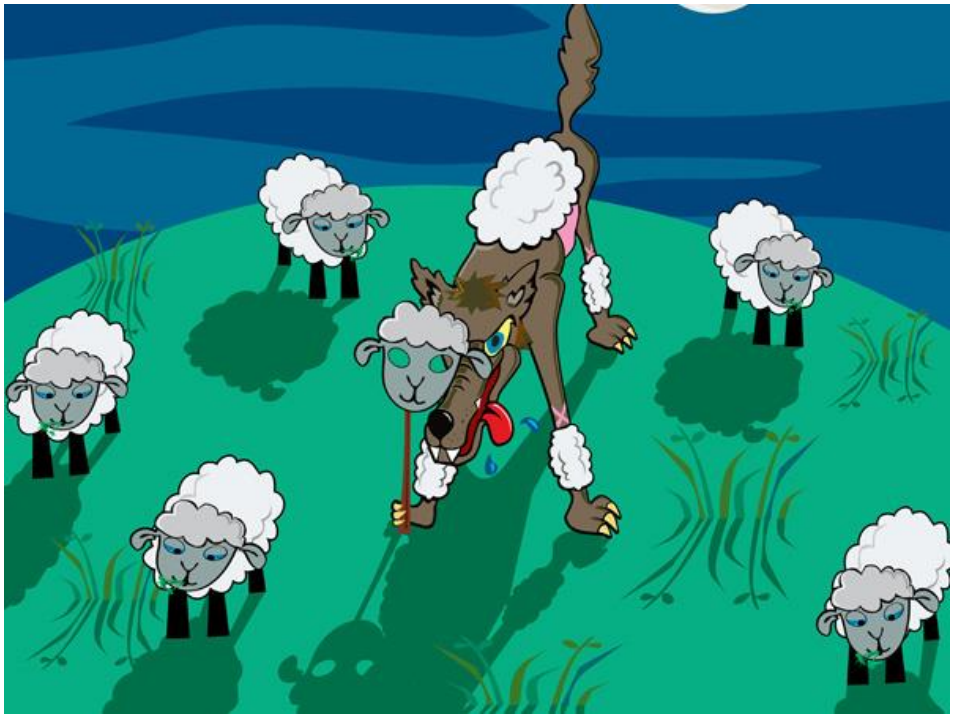
Examples of Affinity Fraud:

Fraudsters will swindle members of groups by posing as a member in order to get close to their victims:

- Pretend to attend church with elderly people in order to rip them off
- Getting close to groups of religious or minority background to gain trust before committing fraud, such as stealing from investors in Ponzi schemes

Safeguards and Solutions:

- Do not enter transactions simply because of someone's connection to your group or community
- Find out more information from the person or company regarding the details of the transaction
- Don't be afraid to question anyone wanting your money, even people you know
- Report known elder abuse to police/authorities



CATO (Corporate Account Takeover)

Cyber criminals steal credentials to initiate fraudulent activity

Examples of CATO (Corporate Account Takeover):

Hackers will exploit computer users and obtain their log-in credentials, using them to commit criminal activity from corporate accounts:

- Initiate fraudulent wire and ACH activity into accounts controlled by the thieves
- Create payroll files with fake employees linked to thieves' accounts
- Steal sensitive information that can be used for blackmail or extortion

Safeguards and Solutions:

- Always protect sensitive information, including log-ins and passwords
- ACH and Wire activity should always be verified by multiple parties and reviewed on a regular basis
- Do not send sensitive info in unencrypted fashion (e-mail) or in unsafe location

Counterfeit Instruments

Fraudsters will replicate everything from currency to checks in order to deceive

Counterfeit Instruments:

Fraudulent items can be used to defraud both consumers and companies:

- Forged money orders, cashier's checks, or consumer checks victimize banks, individuals, and the recipients
- Counterfeit currency can range from motion picture money to bleached $1's or $5's reprinted as $100's
- Counterfeit debit or credit cards have never been more prevalent or costly

Safeguards and Solutions:

- Closely examine checks, cashier's checks, and money orders – verify MICR information (on bottom of checks)
- Counterfeit bills can be any amount – know the source of funds
- Be suspicious of items that look altered or do not feel authentic
- Contact police immediately if you receive suspicious currency or checks

Data Breaches (Internal and External)

Compromised sensitive information can occur due to your own vulnerabilities or within your affiliates' systems

Data Breaches (Internal):

Data Breaches can occur internally from unintended negligence or “inside jobs”:

- In many cases, vulnerabilities are due to outdated software or lack of necessary security measures (firewalls, anti-virus, patching, etc.)
- Many organizations and corporations are simply understaffed in IT dept.
- Embezzlement schemes or fraud rings exist within many companies without management being aware

Data Breaches (External):

External data breaches can occur from affiliates, vendors, customers, or a variety of other sources:

- Target's hackers broke in via stolen network credentials from an HVAC company that services Target stores
- Target also failed to cordon off external network access to prevent HVAC company from accessing sensitive info
- Breaches can occur from fuel delivery companies, POS service providers, or anyone who has access to your network externally

Safeguards and Solutions:

- Protect your network with standard security measures – hire third party IT firm if needed
- Verify vendors' security measures and ensure they are sufficient
- Update software and network protocols on regular basis
- Test network for intrusion and recovery on regular basis
- Monitor account activity regularly for fraud

Skimmers

A device through which criminals steal card and financial information

Skimmers:

Skimmers are devices attached to ATMs, gas pumps, or other terminals to illegally obtain cardholder or personal financial information:

- PIN overlays (right) are placed on ATM keypads to record cardholders' PINs
- Skimmers come in all shapes and sizes – small enough to steal card info from your pocket or to be concealed in a gas pump
- Skimming can steal the card number, as well as personal financial information about the consumer, such as their name and residence

Safeguards and Solutions:

- ATMS are built to withstand physical damage (see right – criminals attempted to break into machine with crowbars but were unable)
- Most hardware tampering occurs by placing an overlay on the keypad or a recording device or camera
- Check for loose or suspicious items on ATMs or gas pumps, or a change in appearance of machine

Social Media/E-Mail Fraud

Fraudsters target victims through phishing, exploitation, or spoofing identities of friends or family members

Social Media/E-Mail Fraud

Criminals will use social engineering tactics, such as identifying victims' interests and likes to steal money, con into schemes, or obtain personal info:

- Facebook and other social media sites contain information that can be used by fraudsters
- Criminals will target people of a certain interest or group (affinity fraud), with promises relating to that interest
- E-Mail accounts are compromised (CATO) or spoofed to gain trust of victim and convince them to release confidential information or credentials to criminals

Safeguards and Solutions:

- Again: if it sounds too good to be true, then it probably is!
- Read before you click
- Verify suspicious email with sender via a different medium
- Beware of any e-mails or correspondence on social media that is unprompted and offers you something for free

Thank You!!

(You can wake up now.)