Sharpen Our Skills

Top Fraud Trends
May 9th
Presented By Shelley Dickerson
& Sheri Miles

A scammer can reach you by the following methods:

- Phone Calls or Texts
    - Robocalls or spoofed numbers pretending to be from the IRS, your bank, or tech support.
- Smishing (SMS phishing) texts that include malicious links or urgent messages (e.g., “Your account is locked, click here”).
- Email (Phishing)
    - Scammers send emails pretending to be from trusted sources (banks, delivery services, etc.) with fake links or attachments.
    - Common red flags include urgent requests, poor grammar, and unfamiliar senders.
- Social Media
    - Direct messages from hacked accounts or fake profiles offering prizes, jobs, or crypto investments.
    - Fake posts for goods available for sale.
- Pop-ups
    - Fake system alerts claiming your device is infected and asking you to call a support number (often a scammer).
    - Pop-ups urging you to download “security software” that is actually malware.
- Messaging Apps (e.g., WhatsApp, Facebook Messenger)
    - Scammers may impersonate someone you know or pose as official organizations.

Top Scams Today:

- AI Voice Cloning Scams - Scammers use artificial intelligence to clone voices, impersonating loved ones in distress to request urgent financial assistance. These calls can be highly convincing, making it crucial to verify any such requests through known contact methods. **HAVE A SAFE WORD!**
- Pig Butchering Scams- fraudsters building online relationships with victims over weeks or months, eventually convincing them to invest in fake cryptocurrency platforms.
- Deepfake Impersonation Scams - Using AI-generated videos or audio, scammers impersonate company executives or public figures to authorize fraudulent transactions or solicit sensitive information. **USE CAUTION ANYTIME CRYPTO IS INVOLVED.**
- WhatsApp Family Impersonation Scams - Fraudsters send messages like "Hi Mum" or "Hi Dad," claiming to be a child who has lost their phone and needs urgent financial help or is in jail or an accident. AGAIN **HAVE A SAFE WORD!**

Sharpen Our Skills

Top Fraud Trends

May 9th

Presented By Shelley Dickerson

& Sheri Miles

- Fake Real ID Application Websites - With the Real ID deadline approaching, scammers have created fraudulent websites offering expedited processing, collecting sensitive personal and financial information from applicants. **Real ID applications must be completed in person at authorized DMV locations.**
- Cryptocurrency Investment Scams – Scammers lure victims with promises of high returns on cryptocurrency investments through professional-looking websites and testimonials. **AGAIN USE CAUTION WITH CRYPTO.**
- Fake Parcel Delivery Texts - Victims receive texts claiming a package delivery issue, prompting them to click on malicious links to reschedule or pay a fee. These links often lead to phishing sites designed to steal personal information. **NEVER CLICK ON SUSPICIOUS LINKS.**
- Social Media Marketplace Scams - Fraudsters advertise non-existent products on platforms like Facebook Marketplace, collecting payments without delivering goods. They often use fake profiles and stolen images to appear legitimate. **ALWAYS CHECK THE PROSPECTIVE BUYERS PROFILE, NEVER TAKE A ZELLE/PAYPAL/VENMO LINK IN ADVANCE OF EXCHANGE OF GOODS.**
- Tech Support Scams - Scammers pose as tech support agents from reputable companies, claiming your computer is infected and urging you to grant remote access or pay for unnecessary services. These scams can lead to malware installation or financial theft. **SHUT YOUR COMPUTER OFF IMMEDIATELY. NEVER PROVIDE CONFIDENTIAL INFORMATION. IF CONTINUES TAKE YOUR COMPUTER IN FOR SERVICE.**
- Gift Card Payment Scams - Victims are instructed to purchase gift cards and share the codes under various pretenses, such as settling debts or securing prizes. Once the codes are shared, the funds are quickly drained, and the transactions are typically untraceable. **USE CAUTION WITH GIFT CARDS!! NEVER PURCHASE GIFT CARDS TO GIVE TO AN UNKNOWN SOURCE.**

Key Takeaways:

- If it seems to good to be true, it is!
- If there is urgency or threatening language, must “act now”, “put a deposit down,” use extreme caution.
- Think before you click!
- Never give out personal information (Account number, social security number and a google phone code)
- Follow your instincts – must fraud averted by gut instinct.