



Fraud Protection

Common Fraud Scams



FRAUD INVESTIGATIONS

- **Law Enforcement has an extremely difficult time in tracking fraud scams since the suspect(s) can be anywhere in the world**
- **Most telephone numbers and locations used by scammers are fake and untraceable**
- **A large amount of fraudulently obtained funds go over seas (Once it leaves U.S. soil it is gone)**
- **Banks have little to no responsibility in helping recuperate lost funds due to voluntarily becoming a victim to fraud**
- **Thousands of dollars can be lost!!!**



Tools of Deception



➤ Fake Phone Numbers

- Scammers can change their phone numbers to appear they are from a legitimate company
- DO NOT recontact these phone numbers from your recent call lists (Call is routed back to the suspect)

➤ Website Verification

- Scammers will provide websites that are real to gain trust

➤ Real Family Information

- The internet is a powerful tool. Vast amounts of information is available on YOU through internet searches



Internal Revenue Scams (IRS)

➤ CRIMINAL IRS Scammers

- Criminals will contact victims representing themselves as an Agent with the IRS
 - Victims are advised of discrepancies with current or previous tax filings
 - Victims are advised assets and accounts will be frozen
 - Victims are advised of pending arrest warrants for lack of payment
 - Victims are sometimes told they will be receiving a large lump sum of payment with the receipt of payment from the victim.



SOCIAL SECURITY ADMINISTRATION SCAM

- **Victims are advised of problems with SS benefit accounts**
- **Victims are advised SS benefits will be stopped unless personal information is given**
- **Scammers will attempt to retrieve more victim information (i.e., date of birth, social security numbers, banking information)**
- **Scammers will also advise of payments needed from the victim to continue SS benefits**



Law Enforcement Scams

- **Victims are contacted by scammers claiming to be from local or Federal law enforcement agencies**
- **Victims are advised there are arrest warrants issued for:**
- **Scammers use real Deputy Information obtain from internet searches**
 - **Unpaid traffic citations**
 - **Unpaid parking citations**
 - **Missed jury duty**



Utility Company Scams

- **Victims are contacted by scammers representing themselves as utility companies (NV Energy/ Southwest Gas / Charter Communications)**
- **Victim is advised of lack of payment for utility services**
- **Criminals request immediate payment and threaten immediate disconnection of services**




Family Member Scams

- **Victims are contacted by criminals representing themselves as family members of the victim**
- **Victims are told by “family member” they are in some type of financial or legal trouble**
- **This type of scam is used to play on the emotions of the victim**
- **The most common used ploy scammers use is needing money for**
 - **Bail to be released from jail**
 - **Attorney fees**



The Sweepstake You Never Entered

- ▶ **Victims are contacted by scammers representing themselves to be a part of a sweepstake winning**
- **Victims are enticed by large lump sum payment**
- **Victims are told they are “required” to make initial payments for taxes/fees prior to taking prize winnings**
- **Victims are requested to provide personal information, banking information, money transfers**



PHONE SCAMS (Most Common)

- ▶ **Phone Scams are the most common types of fraud**
- **Criminals use deception and represent themselves as:**
 - **Members of government agencies (i.e., IRS, Social Security Administration, Law Enforcement Agencies)**
 - **Members of commonly used companies (i.e., Gas and power companies, internet service providers, banks/financial institutions)**
 - **Family members of the victim**
 - **Text message links**

Internet/Computer Scams

➤ Pop ups!

Your computers has been hacked/compromised contact 775-887-2500



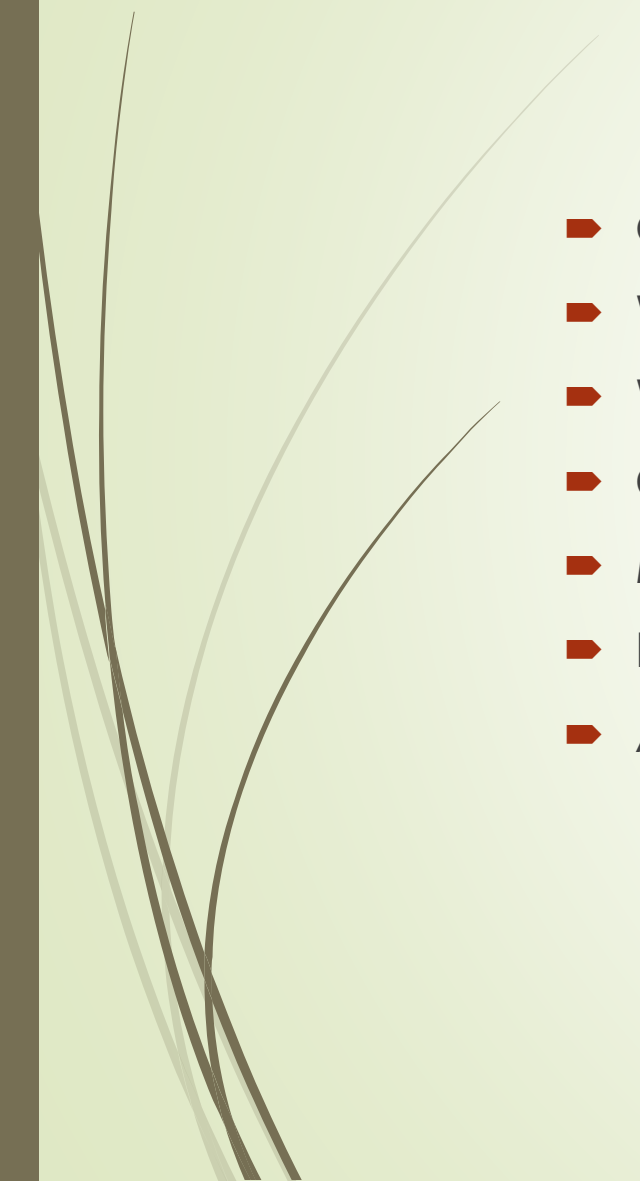


Internet/Computer Scams Continued

- ▶ Your computer can be locked by a scammer remotely if you respond
- ▶ Suspect will then hi-jack your computer demanding money for your computer to be unlocked
- ▶ Your computer may never be unlocked by the suspect even if you pay. All content on your computer could be lost or costly to repair and recover
- ▶ This can be accomplished through texts messages on your cell phone (Is the link you received by text message really from Amazon.com?)



METHODS OF STEALING YOUR MONEY

- Gift Cards
 - Wire Transfers
 - Western Union Transfers
 - Cryptocurrency ATM payments
 - Mailing Cash
 - Bank Account Numbers
 - Account/Device Take Overs
- 



GIFT CARDS

- ▶ Suspects instruct victims to purchase gift cards for payment of Fines, Fees, etc.
- ▶ Once the information from the gift cards is provided to the suspect, the money moves fast.
- ▶ Typically, not recoverable if not reported within 2-4 hours to law enforcement.
- ▶ Cards are recycled through websites making suspect identification not viable
- ▶ ***** DON'T BUY GIFT CARDS UNLESS YOU INTEND THEM TO BE A GIFT*****

QR CODES





Cryptocurrency ATMs

- ▶ These machines look just like regular ATM but convert cash into cryptocurrency
- ▶ Suspects will help victims create crypto currency account (Wallet and Address)
- ▶ A wallet is like a bank
- ▶ A address is like the account number
- ▶ QR codes are used to provide victims with access to the suspects (address)
- ▶ QR codes can also be used to install malicious software on cell phones and computers



Protecting Yourself!!!

- **The IRS will NEVER contact you via telephone**
- **The IRS will only contact you through Certified Mail if there are problems with any tax filings**
- **The Social Security Administration will notify you if there are any issues with your benefits via mail**
- **Utility Companies usually provide electronically generated voice messages if there is a problem with your utility accounts**

***You will not be contacted by a live person**




Protecting Yourself!!!

- **DO NOT provide personal information to anyone calling you on the phone asking for it**
 - *If you didn't call them there is no reason for anyone should legitimately solicit your personal information
- **DO NOT provide bank account information or Debit/Credit Card information**
- **DO NOT make any over the phone payments from solicited calls**
- **Do not give out passwords or allow remote access to your computers or other devices**




Protecting Yourself

- **DO NOT** recontact from phone number from the originally received call
 - **If in doubt, contact trusted family members or your local law enforcement agency for verification of the circumstances**
- 



I Am a Victim

- **Gather all bank records, money transfers with the dates and times of the incident(s)**
 - **If you find you are a victim of a Scam, contact your local law enforcement agency with this information to report it.**
- 



QUESTIONS?

- ▶ Detective Ramon Marquez
 - ▶ 775-283-7855
 - ▶ rmarquez@carson.org
 - ▶ Detective Sergeant Brett Bindley
 - ▶ 775-283-7815
 - ▶ bbindley@carson.org
- 