Fort Collins Police Services

Cyber Crimes Unit

Cyber Crimes Unit

CCU

CCU

- Currently staffed by 5 Detectives, 2 Criminalist, and 1 Investigative Aide
- Supervised by the CCU sergeant
- Financial and Child Exploitation Investigations
- Economic Crimes Task Force
  - Multi-Agency
  - Multi-Jurisdictional
- Fraud and Scam Awareness and Prevention
  - Community Presentations
  - Flyers
- On-Call Investigations

- Major Case Types
  - Identity Theft
  - Elder Care Fraud
  - Scams
  - Check Fraud
  - Credit Card Fraud
  - Contractor Fraud
  - Embezzlement
  - Child Exploitation

CCU

- Primary Investigative Techniques
  - Patrol Response On Scene
    - Documentation, Interviews, Video, Evidence
  - Case Forwarded to Criminal Investigations Division and Cyber Crime Unit if Appropriate
  - Production of Records X ∞
  - Documentation Review – Check the Books
  - Establish Normal Practices
  - Follow the Money
  - Identify and Isolate the Offender

Common Frauds and Scams Affecting Individuals and Businesses

CCU

- Identity Theft and Account Take-Over
- Credit / Debit Card
- Caretaker Fraud
- Romance Scams
- Network Intrusion / Computer Cleaning Scams
- Lottery
- Business Email Compromise
- Phone, Text, and Email Scams
- Fraudulent Online Transactions
- Rental / Employment
- Cryptocurrency Investments
- Sextortion

Identity Theft

- Identity Theft
  - Identifying Information Obtained by Suspect
    - Name, DOB, SSN, Address, etc.
  - Suspect applies for new financial accounts
    - Checking accounts, credit cards, lines of credit
  - Suspect purchases vehicles, electronics, gift cards, and other goods
  - Mail forwarded to avoid detection
  - Victim may not be aware until accounts are sent to collections
- Monitor Accounts, Freeze Credit, and Report Fraudulent Activity Immediately

CCU

- Credit / Debit Card Fraud
  - Suspect obtains credit or debit card number and information
    - Vehicle trespass, purse snatching, online, trash, observations
  - Suspect uses stolen credit card to make purchases
    - Gift cards, online purchases, quick in and out

- Monitor Accounts and Report Fraudulent Activity Immediately
  - Credit card company and banks should reimburse all fraudulent transactions – ensure this is the case when you sign up for the account

- Caretaker Fraud
  - Family or friend assigned as Power of Attorney or joint account holder
  - Suspect uses account funds, credit cards, etc. to their own benefit
  - Suspect arranges payments to themselves for services not rendered or not appropriately priced
  - Suspect will often groom victim by creating distance between them and other family members and friends
  - Can decimate savings and create barriers in receiving aid

- Romance Scams
  - Match.com, eHarmony, Tinder, etc.
  - Profile will be of someone locally or in another country
  - Suspect usually targets vulnerable people
  - Suspect often poses as a wealthy individual but needs help with unexpected expenses and cannot access funds because of travel, divorce, or another reason
  - May need help getting money, gold or jewels into country but requests money from you for good faith
  - Most scams actually originate from outside the U.S. and “mules” are used to get money to them
- Many scams will utilize vulnerable individuals as mules. The suspect will use your bank account to deposit and withdraw money with increasing frequency. This is a method of money laundering that takes advantage of you and can be used for any type of scam.

- Lottery Scams
  - Victim will win a “global” or foreign lottery
  - Taxes and fees will need to be paid before winnings can be sent
  - Taxes and fees paid by wire transfers
  - Money usually sent to “mules” before going overseas.

- Scam Calls, Texts, and Emails
  - You receive contact from the IRS, Social Security, police, or other government agency
    - Threats of arrest, garnishment, etc.
    - Request money through unusual means – cryptocurrency, gift cards, prepaid debit cards, wire transfer, etc.
    - If you send them money, they will continually call and demand more with increasing threats
    - Suspect will go to your banking website and transfer money from your savings to checking
    - Convince the victim it is from an overpayment of refund
    - Victim sends money back to suspect by wire, deposit into suspect's account, or by gift cards
  - You receive contact from a family member or friend stating they have been arrested, involved in an accident, or are in a situation where they can't get back home
    - The suspect will give a reason why their voice or language sounds different
    - The suspect will give a reason why you shouldn't contact another family member to verify
    - Request money for bail, to pay a debt, arrange for travel, etc.
    - Request money through unusual means

- Scam Calls, Texts, and Emails
  - You receive contact stating that an account of yours needs updating or has been compromised
    - Netflix, Amazon, Instagram, Bank, Credit Card, etc.
    - Will usually include a link for you to click on to solve the “problem”
    - Link directs you to a site where you are told to enter your information (identifying, financial, password, etc.)
    - The link, email address, website, etc. will appear very official, but is fraudulent
    - Suspect takes the information you input to the fraudulent site and uses it to take your money
  - If you believe the communication is legitimate, DO NOT click on the link. Use your regular method of accessing the account to determine if there are any issues with it

- Emphasis will often be on speed to prevent you from thinking clearly

- Cryptocurrency Investment Scams
  - Victim is convinced to invest with scammer for high returns in cryptocurrency investments
  - Victim is provided fake statements showing high returns
  - Victim will be provided with some money to encourage further investments
  - Cryptocurrency wallet not controlled by victim

- If you are not familiar with Cryptocurrency, DO NOT send cryptocurrency

- Steps You Can Take to Avoid Scams
  - Check your credit report regularly
  - Monitor statements and balances
  - As soon as you are aware of any suspicious financial activity, request a “Credit Freeze” or “Security Freeze” from the 3 Credit Reporting Agencies:
    - TransUnion
      - https://www.transunion.com/credit-freeze
      - Call 1-888-909-8872
    - Equifax
      - https://www.equifax.com/personal/credit-report-services/credit-freeze/
      - Call 1-800-349-9960
    - Experian
      - https://www.experian.com/freeze/center.html
      - Call 1-888-397-3742

- Steps You Can Take to Avoid Scams
  - Never provide identifying or financial information via phone, text, or email if you didn't initiate the conversation.
    - You can hang up and look for the phone number independently, and then call and ask for the person you were speaking with.
  - IRS, Social Security, etc. will not generally call or email you regarding sensitive information. Typically you will receive information in the mail.
  - Government agencies do not require payments over the phone or via email to cancel warrants, absolve tax, debt, etc.
  - If you are suspicious of someone on the phone or over email, don't provide them with excess information they can use to further their ruse. Don't feed them more info!
  - As a rule, don't send anyone money unless you personally know them and can verify they are in fact who you are speaking with.

- Steps You Can Take to Avoid Scams
  - Phishing Emails: Never respond or click on included links to provide information. If you receive an email from a someone requesting information, go directly to their website for and account updates, correspondence, etc.
    - Phishing emails will often use email addresses that are similar to those of a legitimate business, but the email is not correct. Look at the email address to determine its validity.
    - Phishing emails often contain spelling and grammatical errors, or other clues when the language of the email just doesn't seem right.
  - Never allow anyone remote access to your computer. Contact a tech-savvy friend or family member, or physically take your computer to a local repair shop if needed.
  - Use unique passwords and two-factor authentication for accounts

- Steps You Can Take to Avoid Scams
  - SLOW IT DOWN: Quick action regarding strange circumstances you receive via phone or email is rarely needed.
    - Scammers will push you to move so quickly that you don't have time to make good decisions.
    - There is almost always time to slow down and investigate the situation further.
    - Speak with a trusted relative or friend who can verify information and help you think through the situation.
  - TRUST YOUR INSTINCTS: If something seems off, there's a good chance it is. Businesses and government agencies work in a "normal" manner. If you are being asked to do something outside of what you know to be normal, that should be a clue that something is amiss.
    - Scammers will look for the exception to the rule to take advantage of you.
  - NO CRYPTOCURRENCY: If you aren't already familiar with cryptocurrency, be very suspicious – Bitcoin, Ether, Tether, Monero, BNB, Dogecoin, etx.

Questions?

Sergeant Mike Knudsen
Cyber Crimes Unit
Fort Collins Police Services
970-221-6558
Mknudsen@fcgov.com