Speaker: Detective Sam Murray, VB Police Economic Crimes Unit

Key Takeaways (See blue sheets below)

- The most frequent crimes occurring in our area are
    - Identity Theft – watch for
        - Bills for items you didn't buy
        - Debt collection calls for accounts you didn't open
        - Denials for loan applications
    - Internet Scams
    - Check Fraud
    - Compromised Bank Accounts
- Place a credit freeze with Experian, Equifax, and Transunion - you can freeze / unfreeze for free. With the mobile app unfreezing takes only seconds if you're buying a car, etc. All of our info is on the dark web and this is one of the few things you can do to deter fraud.
- **Never** mail a check from anywhere except ***inside*** a post office. The blue boxes (even the one outside the post office), and especially your own mailbox are easy pickings for check washers. Even better, don't use checks, set up online payments.
- Key things to watch for with the internet, phone calls, etc.
    - Any time the caller wants you to do something "right away" – urgency doesn't give you time to think
    - No bank, credit card company, etc. will ever ask you for your personal information. If you still think they're legitimate, hang up and call the company directly using the number on your credit card, not one that the caller "helpfully" gives you.
    - Never click on a link in an email to go to a bank's website or use the phone number in the email. Call the bank, credit card company, etc. directly as above.
    - Never share your bank info, including routing number or account number, unless ***you*** initiated the call for something like setting up direct pay.
    - No government official, IRS rep, court, etc. will ever call you and ask you to send money.
    - Never hand your phone to anyone. Treat it like you do your wallet, and place strong security settings. If they say they need to make a call, dial it for them and put them on speakerphone.
    - Credit cards are much safer than debit cards - when a credit card is hacked, the bank's money is stolen while you dispute the charge. When a debit card is compromised, the money is immediately drained directly from your checking or savings account.
    - If at all possible, never *swipe* your credit card. Use tap-to-pay, insert the card, or use your phone (safest). Swiping is where most of the fraud is committed because the criminal gets all the card info.

    - Skimmers are almost impossible to see now, they aren't loose or give other easy "tells". Gas stations are BY FAR the biggest targets because no one is watching them attach the skimmer. In the past month multiple skimmers were found at local Kroger and Harris Teeter gas pumps.
    - Be careful at *any* terminal, even inside a store, especially if the terminal is not carefully watched.
    - At the ATM, use your other hand to shield your PIN from a camera that may be attached above the keypad.
  - If you must unsubscribe from a website, never enter your email address if they ask.
  - With AI, anyone can sound just like a loved one. If they're asking for money (for bail, kidnapping, etc.), hang up and dial your relative yourself – they're probably sitting comfortably on their couch at home.
  - Never answer "Yes" if a caller asks "Can hear me?". They can record and use your "yes" to claim you agreed to certain charges, etc.
  - Never allow anyone to remote into your computer unless you have initiated the service call.
  - **Free antivirus software is no longer enough**. Get a highly rated antivirus / malware program and stop using the same password for more than one site. Even better, get a good Password Manager that will generate strong passwords and remember them for you. Yes, even if you have a Mac.
  - Check your bank and credit card accounts regularly – Det. Murray suggested daily but said monthly would probably be ok *unless* you made one of the mistakes above – then check it daily so you can catch any problems early.
  - If a deal seems too good to be true (free vacations, lottery winnings, etc.) it is indeed too good to be true.

- **Home Title fraud**: Title fraud, or deed theft, is when someone illegally transfers the title or deed of your property without your knowledge, often using forged documents or fake IDs. The **VA Deed Alert System** will notify you when someone attempts to do so. (See VA Deed Alert System).

Updated Jan. 2025

Common Scams Affecting Virginia Beach Residents

Provided by the Virginia Beach Commonwealth's Attorney's Office

Don't fall victim!

Jury Duty Scam:

- Scammers, pretending to be local judges or law enforcement officers, call you and claim you missed jury duty.
- They demand that you immediately "pay a fine" to avoid arrest (sometimes ask you to wire money).
- Scammers may ask for personal information in order to steal your identity.
- Scammers might even electronically send you a falsified arrest warrant.
- Court personnel communicate via mail. If you miss jury duty, you'll get a notice in the mail.
- Court personnel will not ask for money over the phone.
- Call 385-4589 to check whether you have jury duty. Don't wire money or provide personal information. Immediately report this scam to police!

Money Transfer Scams:

- Scammer approaches someone and asks to borrow their phone (scammer often pretends to be needing help – locked out of their car, lost their wallet, needs a ride, etc.).
- Scammer opens a money-transfer app such as Venmo, PayPal, ApplePay, CashApp, Zelle, etc. and wires money to themselves.
- In some versions of the scam, thieves go into a banking app and claim to do a "member to member transfer". Then, they state that they sent the victim "too much money" and show the victim their account with an inflated balance; They request the victim transfer money back to them via a money-transfer app; the victim doesn't realize until much later that they've been scammed.
- In some instances, scammers use the victim's mobile banking app to apply for a loan.
- Never share your phone with anyone. Treat your phone like it's your wallet. Ensure you have strong security settings on your mobile device.

The "Grandparent Scam":

- Scammers call a grandparent and identify themselves as a grandchild or loved one in need of money right away due to a hardship (stuck in jail, broken down car, stuck in a foreign country).
- Scammers obtain personal information from social media accounts. They use Facebook, Instagram, and other applications to learn about your grandchild, and they use your grandchild's identifying information to trick you into believing they are legitimate.
- Scammers are very convincing, sometimes sound very desperate and troubled, and they play to your emotions. They might call late at night or early in the morning when you are sleepy; some might disguise their voice or use nicknames.
- Never wire money – it is difficult to get back.
- Ask the caller some questions a stranger could never answer.
- Plan ahead. Set a password with your grandchildren now, in case you get a call like this. Ask the caller to provide that password.

- Resist the urge to act immediately. Hang up, and then call the loved one at a number you know to be valid.

IRS Phone Scams (particularly prevalent during and just after tax season):

- Scammers are posing as IRS employees, claiming you owe money now or that you are due a refund (and then ask for your personal information).
- The IRS will NEVER:
  - Call you about taxes you owe without first mailing an official notice.
  - Demand that you pay taxes without giving you the opportunity to question the amount.
  - Require you to use a specific payment method for your taxes, such as a prepaid debit card.
  - Ask for credit or debit card numbers over the phone.
  - Threaten to bring in local law-enforcement to have you arrested.
- Here's what you should do if you get called:
  - Call the IRS (1-800-829-1040) to determine if you owe money.
  - Report it to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484 or www.tigta.gov.
  - You should also notify local law enforcement so they can track crime patterns in your area and warn citizens.

"Yes" Scam:

- Scammer calls an asks, "Can you hear me?"
- You reply "yes" and the scammer records your voice.
- Scammer uses recording to claim you agreed to certain charge (authorizing phone, cable, credit card, or utility bill).
- Never answer questions on unsolicited calls. Just hang up. If it is a legitimate caller, they will call back or leave a message.
- If you already responded to one of these calls with a "yes", monitor your credit card statements and report any suspicious charges to the company or bank immediately.

General Computer/Technology Scams:

- Phishing – Scammer creates a fake e-mail pretending to be someone/something else in order to steal your information.
- Copycat Websites – Websites created to look like a legitimate website; Often looking to steal your log-in information or credit card information.
- IT Scams – Either a pop-up says there's a virus on your computer or a scammer will call pretending to be a computer technician. They'll then ask for remote access to your computer to "fix" the issue. From there, the scammer can access anything on your computer.
- Make sure to use good anti-virus software, only visit websites you know to be legitimate, and never allow someone access to your computer unless you have initiated a service request for an issue on your device.

For questions or more information:

Virginia Beach Commonwealth's Attorney's Office: (757) 385-4401 or oca@vbgov.com
Website: oca.virginiabeach.gov