Go To What You Know – Fraud Scams and How to Avoid Them

Construction Scams – KNOW THE SIGNS:

- "We're in the neighborhood"
- "I'm working on your neighbor's house"
- "I'm from your roofing or paving company"
- "My dad worked on your property"
- No work uniform
- Vehicles do not have the company's information on them (lettering, signage, logos)
- They do not have a solicitor's permit
- They ignore "no trespassing/no soliciting" signs
- Request payment in cash or check made out to an individual, not a company
- If you pay now or in cash it'll be cheaper
- You have to commit now to get the deal/price
- They don't have, hesitant to, or won't provide a written estimate, invoice, copy of their license and insurance.
- Any invoices or estimates are not on letterhead or a form with their full contact info, license numbers, etc. and/or contain spelling and grammar errors
- They are not registered or don't have a current license with DPOR (the Virginia Department of Professional and Occupational Regulation)
- Not listed in an online/google search

Romance Scams – KNOW THE SIGNS:

- They initiate contact, usually online
- Frequently they live abroad or far away
- They move conversations to private messaging
- **You've never met in person**
- You've never conversed over live video
- They ask more questions than they answer
- The information they want to know is personal and provides ways to identify you
- They claim to be wealthy or have high status
- They complement you frequently and profess love quickly without having ever met in person
- They take their time to build up a connection
- They have excuses for why they can't meet in person (or over video).
- **They always ask for money or assistance because of a family, travel, legal or immigration problem, a health emergency, real estate problem, or for an investment**

"Family Member In Trouble" – KNOW THE SIGNS:

- You receive a panicked phone call that sounds like it could be a family member
- The "family member" doesn't use names, words, or language unique to you or them, or only starts using names after you do
- Family member has been arrested or hurt, often a car accident involved.
- Someone else may get on the phone claiming to be law enforcement, attorney, or bail bonds
- Request to wire or send money, or provide bank account or credit/debit card numbers
- Person will send a "courier" or "employee" to pick up cash, usually thousands of dollars
- Person will call back requesting more money

Computer Tech Support and Pop Ups – KNOW THE SIGNS:

- A message pops up on your computer screen from Microsoft or other company indicating a virus or your computer is hacked.
- Message may list a phone number to call
- Request is made to allow access to your computer remotely, sometimes by installing a program or clicking a link.
- Any links provided will take you to replica websites that seem realistic and may show your account information.
- You will see account activity happening in real time on the screen, sometimes showing large deposits.
- Suspect will request or move money from one account to another or make an "accidental deposit" for a large amount of money, then pressure you to help him refund it.
- Instructions to wire, transfer, or send money in cash, cashier's check, gold bullion, gift cards, Bitcoin or cryptocurrency, or electronic transfer to another account or physical address.
- Instructions to write checks to a person or business that is not your bank or mail it to an address that isn't your bank

Go To What You Know – Fraud Scams and How to Avoid Them

"Text Messages/Emails/Phone Calls" – KNOW THE SIGNS:

• Text, call, or email comes from a number or email address you don't recognize. • Some scammers can spoof phone numbers to seem like it's coming from a number you know • If from a "family member" or friend, boss/coworker, they don't use names, words, or language unique to you or them, or only starts using names after you do.	• Sometimes the language doesn't seem to match how they usually talk or write. • Family member has been arrested or hurt, often a car accident involved. • Request to wire or send money, or provide bank account or credit/debit card numbers • Instructs you not to tell anyone or won't answer the phone if you call.

"Law Enforcement/Missed Court or Jury Duty" – KNOW THE SIGNS:

• Uses the wrong terminology or departments that don't exist, such as "Bailey's Crossroads Police", "Constable" instead of Police Officer or Deputy. • Noise, other conversations in the background • Phone number area code is not for this area • Claims there's a warrant for your arrest for something that doesn't sound correct/familiar	• Tells you that you can pay now or make payment arrangements and the warrant will be cancelled (real court orders can only be cancelled at the courthouse by a judge) • Instructs you to pay by dropping off cash, gold bars, gift card, or wire money via bitcoin or cryptocurrency • They will send a courier or you can meet someone outside the courthouse

"You Won The Lottery" – KNOW THE SIGNS:

• Notifies you of winning a lottery you never played. • Lottery is from a foreign country • Notification is in an email or text message	• You have to prepay the taxes or a fee or put down a deposit • Wants you to provide a bank account number to transfer money to you

"Soliciting Donations" – KNOW THE SIGNS:

• Door-to-Door: Charitable organizations don't have a required Fairfax County solicitor permit • You've never heard of the nonprofit • You look up the nonprofit and it doesn't exist or has bad reviews	• The request for donation occurs after a disaster • Raising money on behalf of a victim's family • They don't provide a receipt

"Investments/Job Opportunities" – KNOW THE SIGNS:

• The message is unsolicited in a text message, email, phone call • You've never heard of the company • They offer profits and return on investments that are higher than they should be or seem too good to be true	• The company doesn't exist online or has bad reviews • You have to pay money upfront or provide your bank account or other information • Claim no license/permit required when it is • Handwritten signs or mailings

"Buying things from Facebook Marketplace or Other Online Listing" – KNOW THE SIGNS:

• They want to meet in a non-public place to do the sale or not in the lobby of a police station • Price seems too good to be true	• Pictures of items seem like "stock photos" or from the manufacturer's website • Pay them money in advance • The item is not as advertised.

“Your Bank/Credit Card Account Is Compromised” – KNOW THE SIGNS:

• You are called or receive a text message from your bank or credit card company • The phone call or text phone number displayed may be the bank’s number or the number on the back of your credit/debit card • Tell you upfront there is fraud on your account • Ask if you made purchases you didn’t make	• Request your password or identifying code • Instruct you to transfer money into another or new account • Instruct you to withdraw and mail money or a check or gold to an address to open a new account. • Instruct you to not tell anyone, including your bank branch or family members

“Extortion” – KNOW THE SIGNS:

• Phone number, text, email etc. is not from a person, phone number, etc. you know. • Claim to have your family hostage or have compromising pictures or information • Your family member is not missing or is fine • They don’t use the correct names for you or your family members.	• They “put a family member on the phone” but the person doesn’t know private/personal info only your family would know. • Pictures of items seem like “stock photos” or edited photos, or not clearly identifying photos • The photo of your house can be found on a real estate website or through Google Maps Street View

STOP THE SCAMS: "TRICKS OF THE TRADE"

Phone

- ***GO TO WHAT YOU KNOW:*** If you receive a phone call that might be suspicious, or from your bank, insurance company, utility company, "the government", or other source and they are claiming you owe money, there's a problem with your account, you're a fraud victim, you missed court, have an arrest warrant, a family member in trouble, etc., hang up! Find a number you know is real, such as on older bank statement or bill, a phone number you've used before that you know is real and works, or from a website you know is not fake (check the spelling of the name on the website address for spelling errors, extra letters, etc.). Call the company or person or entity from the good phone number and ask if someone just tried to call you.
- Scammers can "spoof" phone numbers to appear on your caller ID from a source such as your bank, other known business, or a friend or family member.
- With computers and artificial intelligence, scammers can make computerized voices sound real and interact with you.

Mail

- ***Never*** send cash or gold bars/precious metals through the mail!!!!!!
- Never drop mail into a blue mailbox outside of the post office or other location; only put it in the slot inside the post office or hand directly to a clerk.
- Do not mail bills in the envelopes provided; thieves and scammers know these envelopes often contain a check or payment information.
- Any mailed checks or money orders along with the invoice or bill should be placed inside one or two folded sheets of paper so they can't be "seen" through the envelope. If you have the option, send mail via "Certified Return Receipt" or Priority Mail. Both allow you to track the progress and delivery of your item.
- ***GO TO WHAT YOU KNOW:*** If the mail is a solicitation, an invoice, a warning letter, etc., Find a number you know is real, such as on older bank statement or bill, a phone number you've used before that you know is real and works, or from a website you know is not fake (check the spelling of the name on the website address for spelling errors, extra letters, etc.). Call the company or person or entity from the good phone number and ask if they sent you the mail.

Text Messages

- *NEVER* click on a link in a text message that claims to take you to the company website, to report a problem, etc.
- If you get a text message that appears to be fraudulent or is suspicious, block the phone number or email that is sending the message to you. NEVER reply to the message. That can confirm your information or phone number to the scammer.
- ***GO TO WHAT YOU KNOW:*** Use a link or website address you've used before and know is legitimate. Or search for the actual, legitimate website and confirm it's real and use that link. Or, find a number, website, an older bank statement or bill, a phone number you've used before that you know is real and works, or from a website you know is not fake (check the spelling of the name on the website address for spelling errors, extra letters, etc.). Contact the company or person or entity and ask if they sent you the text message.

STOP THE SCAMS: "TRICKS OF THE TRADE"

Email

- Spammers will provide email addresses, websites, etc. that look legitimate but are spelled slightly differently. Hover your mouse pointer over the link and the actual website address the link will take you to shows up. Example: "billing@veriizon.net", "afranklin@dominnion.com".
- Emails from someone who represents a government or business should never come from a Gmail address or email address that doesn't have the company name and ".gov" or ".org", etc. in it. They shouldn't appear to be a list of random letters/numbers/words or be what appears to be a private email address. For example, a legitimate government official or company employee might have their name in their email address in the format of "xxxx.xxxx@name of the agency or company, such as "john.doe@fairfaxcounty.gov", "tsmith@wellsfargo.com". It should never be "bobevans12@gmail.com" or "tiffanyjohnson@aol.com".
- *NEVER* click on a link in an email address that claims to take you to the company website, to report a problem, etc.
- ***GO TO WHAT YOU KNOW:*** If the email is a solicitation, an invoice, a warning letter, etc., use a link or website address you've used before and know is legitimate. Or, search for the actual, legitimate website and confirm it's real and use that link. Or, find a number, website, an older bank statement or bill, a phone number you've used before that you know is real and works, or from a website you know is not fake (check the spelling of the name on the website address for spelling errors, extra letters, etc.). Contact the company or person or entity and ask if they sent you the email.

Computers

- If you unexpectedly experience a pop up message on your computer claiming to be from a company like Microsoft or that you have a virus (when you don't have an antivirus program currently running), etc., it is very likely that it is a fraud attempt. ***DO NOT CLICK ON IT!***. The better choice is to shut off your computer via the screen or manually push the power button or unplug it, wait a short period of time (5-10 minutes), and then restart your computer again.
- If a pop-up event occurs and there's a chance or you suspect fraud may be or is involved, have your computer examined by a legitimate professional computer service/repair company. It's possible that viruses or spyware could have been installed on your computer during the fraud activity and further use of your computer could allow the scammers to access personal information, account logins and passwords, etc.
- Never let anyone "remotely log in to your computer", unless you are *absolutely* sure that the person is reputable and from a legitimate company.
- Never let anyone who is remotely accessing your computer or assist them in logging into your bank account, credit card account, etc.

Payments

- Government and legitimate businesses will ***NEVER*** request you to send or pay in gift cards, cash, gold bullion, gold coins or bars, Bitcoin or other cryptocurrency, or checks or money orders made out to individuals or businesses that are not their own names.
- Never send cash or gold bullion via the mail, UPS, FedEx, Uber, Lyft, a "courier", or any other carrier. There is no way to trace cash, gold, or other precious metals once you send them.
- ***COURIERS:*** No government entity will *EVER* request you send money via a courier. They will ***NEVER*** send someone to your house to pick up a payment.
- ***NEVER*** agree to meet someone in person to make a payment on a company or government account or bill.
- **NO GOVERNMENT OFFICIAL OR COMPANY REPRESENTATIVE WILL MEET YOU OUTSIDE OF A GOVERNMENT BUILDING OR COMPANY OFFICE. THAT IS A SCAM!**

STOP THE SCAMS: "TRICKS OF THE TRADE"

Protect Your Information

- Lock/Freeze your credit and request copies of your credit report from the three credit bureaus:

  "One stop shopping": annual credit report (website sponsored by the federal government
  https://www.annualcreditreport.com/index.action

  - Experian
    https://www.experian.com/
    (888) 397-3742

  - Equifax
    https://www.equifax.com/
    (888) 378-4329

  - Transunion
    https://www.transunion.com/
    (800) 916-8800

- Credit Monitoring: each of the credit bureaus offers a credit monitoring service and other services for a fee. NOTE: they are required to provide a free report to you once a year and also when you are a victim of identity theft; you may need a police report number or verification letter.

Do Not Call Registry

Free federal government service that allows you to register your personal phone numbers (home, cell phone, etc.); once registered companies violate the law if they call you to solicit business. There are exceptions so check the website for details. You can also report violations there.

- https://www.donotcall.gov/

"TRUST BUT VERIFY"

Research the company:

- Professional Licenses: lookup a company or person to see if they have a license
  Virginia Department of Professional and Occupational Regulation
  https://www.dpor.virginia.gov/LicenseLookup

- Business/Corporation Registration (required by law): look up to see if they are registered
  Commonwealth of Virginia State Corporation Commission
  https://cis.scc.virginia.gov/EntitySearch/Index

- Soliciting Permits (required to go door-to-door in Fairfax County): info & look up complaints
  Fairfax County Consumer Services Division, Regulation and Licensing Branch
  https://www.fairfaxcounty.gov/cableconsumer/csd/regulation-licensing/canvassers-peddlers-promoters-solicitors

- Better Business Bureau: private accreditation for businesses, tracks complaints
  Fairfax County Better Business Bureau:
  https://www.bbb.org/us/va/fairfax

STOP THE SCAMS: "TRICKS OF THE TRADE"

"TRUST BUT VERIFY"

Research the company:

- Online Searches:
  - Search their address; example, Google Maps will show their location, look at pictures of their address
  - Look for reviews and complaints
  - Search for the name and look at any images
  - Check the spelling and their address/location; many businesses are spelled alike or very similarly. May have the same name in another state and it's a different business.

- Ask friends, neighbors, coworkers about their experiences with the company if they have any.

- Ask for a copy of their business insurance policy or find out which insurance company they have; call their insurance company and verify they have an active policy and see if there are any issues.

- Ask if the company is bonded and ask for a copy of their bond certificate; call the bond or insurance company and verify it is an active bond.