**Safety/Security – March 2024**

Bottom Line Up Front:

- Stretch and Warm Up Before Yard Work
- Au Revoir All-Day Free Parking in Croatan Lot
- General Booth Road Closure
- Security Assignments and Funding
- CAC – Next meeting March 13
- VBCCO – Fraud and Scam Warnings

**Stretch and Warm Up Before Yard Work:** The robins have never really left, but there can be no doubt that Spring is nearby as colorful blooms and blossoms awaken from them winter hibernation. If you're doing your own lawn and garden work, be sure to stretch and warm up a little bit before hauling heavy bags of mulch and soil, bending over to pull weeds, or conducting any late-winter/early-spring pruning. Muscles that have lain dormant over the winter may object to overly strenuous use and abuse if you don't.

**Croatan Parking Lot:** A more dependable sign of seasonal changes (than robins) is the cessation of all-day free parking in the Croatan lot at the south end of Vanderbilt Avenue. Beginning April 1, those parking after 10:00 AM will incur a $3 VB-Resident ($7 non-VB resident) fee. Payment is made at kiosks located near the bathhouse. A welcome change is that new provisions allow for reentry the same day without having to repay. Hours of operation are listed as 6:00 AM until 8:00 PM.

**General Booth Road Closure:** Northbound General Booth Boulevard from Birdneck Road to Rudee Inlet will be closed on **Sunday, March 17 from 8:00 AM until 2:00** PM to accommodate the Shamrock Marathon. Police will be monitoring the Croatan Road intersection so you ***may*** be able to turn south during gaps in runners, but will not be able to return until the road reopens. Plan ahead if headed to church, brunch, the airport, or other events.

**Security Assignments and Funding:** Changes are coming to the way Croatan engages our officers for off-duty assignments. Under a new Off-Duty Management (ODM) system being implemented by VBPD, we must now be more descriptive of which hours our officers work and work blocks must be at least three hours in duration. Captain Michelle Wyatt (VBPD) will brief the March meeting of the Citizens Advisory Committee (CAC) on these changes.

Thank you to all who have contributed to our Security Fund. We're roughly two-thirds of the way to our goal. Contributions can be made online at https://www.croatanbeach.org or mailed to our Treasurer.

**Citizen's Advisory Committee (CAC):** There was no February CAC meeting. The next meeting will be held on Wednesday, March 13, 2024 at 7:00 PM in the conference room of Virginia Beach Volunteer Rescue Squad #14, 740 VB Blvd (17th Street). Please park on the east side of the building. CAC meetings are open to all.

**Virginia Beach Council of Civic Organizations:** Jim Ferrera asked me to cover the February VBCCO meeting for him. I am glad that he did because VBPD Detective Caleb Davey gave a superb presentation on Frauds and Other Scams, especially those being perpetrated locally. Scamsters are so accomplished and smooth, that many people do not realize that they've been "taken" until after the fact. This says a lot about both the goodness of human nature and the absolute disregard for people by nefarious individuals. Some key scams notching victims every week include:

**Cell Phone Scam:** Someone comes up to potential victim in the parking lot with a sob story, "My mother was just taken to the hospital and my phone is out of battery, can I use your phone to call her?" In less than a minute, they can access your banking information and take out a loan in your name or transfer money to an account they control. If you can't say "no," dial the phone yourself and put it on speaker. **UNDER NO CIRCUMSTANCES ALLOW THEM TO TOUCH YOUR PHONE**.

**Romance Scam:** There are a lot of lonely people out there. Pictures and profiles are not always accurate, but even if one does hit it off with a potential partner, beware of the "need" of some financial assistance with rent, car payment, because ex-spouse left them destitute, airline tickets, until deceased-spouse's life insurance payment is received, etc.

**Puppy Scam:** Puppies are endlessly cute. Photos and sob stories tug on heartstrings. "Breeders" promise pure-bred puppies for anywhere from a few hundred to several thousand dollars. Usually, you won't get a dog at all, but if you do, it may be sick, require shots, spaying/neutering, etc. Quick solution – VB Animal Shelter on South Birdneck Road is overflowing with adoptable pets. Adoption fees are just $1.00.

**Imposter Scams:** "Hello, this is Deputy Sherriff Dawg, Badge number 12345, calling to inform you that a warrant has been issued for your arrest for having ignored your Jury Duty summons." But you never received a summons? So, Deputy Dawg offers to quash the warrant if you wire $500 to XYZ Account immediately. If you do so, fraudster gets $500. If you get sucked into providing your bank routing number and account number, you lose it all. NO ONE from the Police, Sherriff, Social Security, FBI, Secret Service, CIA, etc. will ever call you with such a pitch.

**Nigerian Scam:** Called this because of its source of origin, this comes in many forms but is usually similar in that some prince, lawyer, agent, widow, caretaker, missionary, etc. represents someone who has come into several millions of dollars but needs a U.S. bank account to affect the wire transfer. If you are willing to provide a good faith payment of $10,000 and allow use of your bank account, they will split their millions with you. I receive email to this effect every week. **Do not open, do not reply, and do not click on any hot links**. Just delete it from your in box and delete it again from your trash folder.

**Grandparent Scam:** I love when someone calls with this one because I have no grandkids – but it usually consists of a late-night/wee-hours emotional phone call, "Hello Grandma/Grandpa, I'm in trouble. We were in Timbuktu on spring break and our rental car was hit by a taxi. Police are saying that I was driving and I need money to hire a lawyer." On comes a well-spoken, less emotional individual ("the lawyer") with specifics of how serious this offense is, how severe the penalties can be, and how he can be retained for $15,000 wired overnight to an account. Before the victim is even awake, the transaction is done.

**Charity Scam:** Scammers call seeking money for some police or veteran's organization that may sound legitimate. **They're not!** The names are changes ever so slightly from the true organization (which will not call you). And your kind-hearted donation ends up lining some fraudster's pocket rather than benefiting those you want to assist. For example: rather than Disabled American veterans (DAV) – legit – they'll use something like American Disabled Veterans – bogus.

**Tech Support Scam:** You receive a call from "Microsoft Tech Support" (always fun if you have an Apple), "We've noticed that your computer is running slowly [or hasn't been updated with the proper software], if you allow us remote access, we can make the correction for you." As obvious as this is, people fall for it and "poof" – all of your passwords, personal information, financial data, etc. is compromised. Never, ever let someone remote into your computer unless you initiate the call and know you speaking with bona fide tech support.

**A few computer basics**:

- Regularly (i.e., daily) process updates to computer programs and virus definitions.
- Invest in TotalAV, Norton, Bitdefender, McAfee, or some other reputable brand of computer protection software. Avoid Kaspersky unless you want Russia to know everything you are doing.
- Use a Virtual Private Network (VPN)
- Build passwords that are easy for you to remember but difficult to crack, incorporating – upper- and lower-case letters, numerics, and special characters.
- Change passwords often
- Password protect any file in which you store other passwords
- Use different passwords for each banking account
- Use multi-factor identification
- Use fingerprint biometric identification on cellphone, if possible. It is safer than facial recognition.
- Use a single credit card for internet purchases (easier to identify unauthorized purchases)
- Do not conduct online banking from a non-secure WiFi network unless absolutely necessary. If necessary – make it quick!

- Hover your mouse over the “From” address of any email that seems suspicious (e.g., from someone you haven’t heard from is a long time, a bank, anything that discusses a late or delayed shipment, account, or potential charge)
- Artificial Intelligence is reducing the incidence of telltale signs formerly used to identify scam and phishing emails such as misspelled words, poor grammar, syntax errors, etc.
- Rather than clicking on embedded hot-links in messages – go separately to the company’s known website and investigate from there. Telephone the company, if necessary.
- Don’t automatically click on the first returned website of a Google, Bing, Safari, or other search result.

If there is a short-fused time window to act or you’re being asked to pony-up some money – it is most likely a scam. There’s a sucker born every nano-second, or, in the immortal words of Abraham Lincoln – “Not everything you read on the Internet is true.”

M. C. “Connie” Agresti,
CCL Safety and Security Director