



Florida's Harborside Hometown

INFORMATION SHARING REPORT December 6, 2021

RETIREMENT:

The Right-of-Way Department is announcing the retirement of three long-term employees. Richard Davis 34 years, Kurt Jones 28 years and Kenneth Wagner 28 years of service. Congratulations on your retirement! The City of Punta Gorda greatly appreciates all of the employee's hard work and dedication.



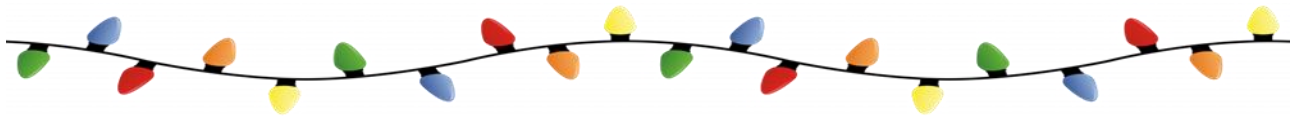
IT TIDBITS:

HOLIDAY CYBERSECURITY TIPS

Follow these simple cybersecurity tips and practices before and while making purchases on line;

- ✓ **Pay wisely.** Use a credit card or pre-paid debit card instead of a debit card linked to your bank account. Or use a reliable, established third-party payment service, such as Google Pay, Apple Pay or PayPal.
- ✓ **Shop securely.** Not only should you make sure your internet connection is secure. Check to make sure you're shopping on a site that uses SSL protection. The easiest way to tell is to check your browser's address bar. Look for https is the URL. Sites without the s are not safe to submit payment information or other personal details.
- ✓ **Monitor your accounts.** Check your online financial accounts regularly for suspicious spending. Also, take advantage of text and email alerting services that many banks and credit card companies now offer.
- ✓ **Resist the urge.** Be wary of offers too good to be true – no matter how tempting they might be. Buy only from trusted and established online retailers and avoid websites of retailers you've never heard of.

- ✓ **Lock down your login.** Create long and unique passphrases for all accounts and use multi-factor authentication wherever possible. Multi-factor authentication will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-timecode sent to your phone or mobile device.
- ✓ **Think before you click.** Pay attention to emails you receive. Don't open emails from unknown senders or click on links in suspicious messages.
- ✓ **Keep a clean machine.** Before picking out that perfect gift, be sure that all internet-connected devices – including PCs, smartphones and tablets – are free from malware and infections by running only the most current versions of software, web browsers and other apps.
- ✓ **Use secure Wi-Fi.** Using free public Wi-Fi to shop online while at your favorite coffee shop is tremendously convenient, but it is not cyber safe. Don't make purchases while connected to public Wi-Fi; instead use a virtual private network (VPN) or your phone as a hotspot.



Safety TIPS – Giving online

Online thieves know the holidays spark the desire to give back, making charity donations a hot target.

- Ignore unsolicited requests. Be wary of emails and phone calls asking for donations, especially from organizations unfamiliar to you. If you want to donate, visit their websites directly or call to donate.
- Think before you pay. Never wire money or send cash. When writing a check, make it payable to the organization or pay via credit card. If you donate online, make sure the website is secure by looking for the **s** in **https** at the beginning of the URL.
- Doublecheck the website. Check website URLs carefully since cybercriminals often create websites and names that are very similar to legitimate, reputable organizations. Check the spelling of the organization's name and the URL very closely for discrepancies.

Safety TIPS – While Traveling

- **Avoid free Wi-Fi.** Although connecting to free public Wi-Fi sounds great, it is often unsecure and can expose your devices and personal information to hackers. Instead, use a VPN or your mobile phone as a hotspot when going online.

- **Confirm your network.** If you do connect to public Wi-Fi, be sure to confirm the name the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
- **Disable auto-connect on your devices.** If your mobile phone or table automatically connect to wireless networks or Bluetooth devices, disable those features, and connect manually only when you want to.
- **Secure your devices.** Keep track of your laptop, smartphone, tablet and even accessories such as USB drives – especially while on the go, and don't leave your devices unattended in public places.
- **Avoid shared computers.** If using computers at hotel business centers and other places that offer shared systems, avoid making purchases or logging into email. You don't know if the systems are up to date with the latest security software or if the machines are safe.

