**COMMON SCAMS**

With more people buying holiday gifts online, scammers take more opportunities than ever to steal personal and financial data. Cyber thieves create websites, email accounts and social media accounts that look legitimate. They then send out fake shopping notices or tricking messages purporting to come from the post office, UPS, FedEx or after mailing and shipping companies. Be on the lookout for these three main scams.

1. **Spoofed and bogus websites**
   - Beware of websites, emails and social media posts offering incredible deals on electronics, clothing, toys or other items that seem too good to be true.
   - Always verify the retailer is legitimate. Type in their web address and hover over the link. It will display the real or fake site.
   - Be wary of websites, emails and social media posts claiming to offer incredible deals on electronics, clothing, toys or other items that seem too good to be true.

2. **Phishing emails**
   - Avoid using a public or unsecured Wi-Fi network.
   - Avoid using a public or unsecured Wi-Fi network.

3. **Fake shipping notices**
   - Monitor your accounts. Keep a close eye on your account statements and credit report. Make checking these items part of your holiday season.

**HOW TO SPOT A SCAM**

Take a closer look on websites and emails to spot these telltale signs:

- The website URL contains odd characters, looking different from the retailer you know.
- Don’t click links and you won’t be able to see if the link is legitimate. Type the retailer’s web address (for example, woos60z.com) and look for a small number to verify the location.
- Beware of websites, emails and social media posts offering incredible deals on electronics, clothing, toys or other items that seem too good to be true.

**OTHER WAYS TO PROTECT YOURSELF**

**SHOP ONLINE WISELY.**

- Do not visit the websites of merchants that you have not heard of.
- Do not click on links that you don’t recognize.
- Do not make purchases or take cash from your account.

**SHOP SECURELY.**

- Identify a secure website by checking for “http://” in the web address and look for a padlock symbol at the bottom of your browser.
- Identify a secure website by checking for “https://” in the web address and look for a padlock symbol at the bottom of your browser.

**THINK BEFORE YOU CONNECT.**

- Avoiding public or unsecured Wi-Fi network while shopping online.
- Avoiding public or unsecured Wi-Fi network while shopping online.

**SIGN UP FOR ALERTS.**

- Your financial institution may offer fraud and account-related alerts that will help you monitor accounts for unusual activity.
- Your financial institution may offer fraud and account-related alerts that will help you monitor accounts for unusual activity.

**LOCK YOUR CARD.**

- Check to see if your bank offers a “lock card.”
- Check to see if your bank offers a “lock card.”

**WATCH FOR HOLIDAY HACKS.**

To help you shop safer this season, review these tips from our team of cybersecurity specialists.

Visit huntington.com/Security to learn more about how we help protect your privacy and keep your information secure.