Presented by Barefoot Resort and North Tower Neighborhood Watch groups

Avoid Becoming a Victim

As the holidays and shopping season approaches criminal activity intensifies

Your Neighborhood Watch Committees offer the following safety tips for your safety

Personal Safety When Walking at night

More suggestions

- If carrying a purse, hold it in front of you. Draping it over your shoulder makes it easy to grab and run
- Cell phones can be a distraction or target for theft. Keep them out of sight and reach

Tips

- Walk in groups, there is safety in numbers
- Let someone know your destination and time of arrival and departure
- Stay in well lit areas
- Walk on sidewalks wherever possible
- Be aware of your surroundings
- If wearing headphones don’t turn up the volume so high you cannot hear outside noises
- Wear bright clothing

Vehicle Security

More Suggestions

- Consider theft prevention devices for older vehicles
- Place decal on window to advertise presence of a car alarm or tracking system
- Carry Pepper Spray or Mace

Tips

- Always lock your vehicle-**always**
- Do not leave keys or key fob in the vehicle
- Park in well lit areas
- Do not leave personal papers or valuables in vehicle
- Do not leave vehicle running if you can’t lock it or engage the alarm
- Carry car keys in your hand and press the “Emergency” button if trouble arises

Protect your Packages

Another Suggestion

- Install a Video Doorbell with camera such as Ring

Tips

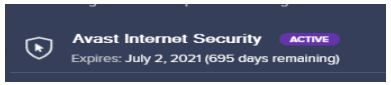
- Have packages delivered to your work
- Have packages delivered to the home of a friend or relative that you know will be home
- Have packages held at the Post Office
- Take advantage of “Ship to Store” options
- Amazon, among others, offers a “locker” feature that allows you to pick up packages at at secure location
- Request signature confirmation upon delivery
- Ask you carrier to place packages in an area out of plain view

Before you click another “Buy” button

- There’s been an explosion in coronavirus phishing emails designed to steal sensitive data
- The FTC received more complaints in April and May 2020 than any other months on record!
- Collective cost of online fraud is $240,000,000 since 2015

Actions You Can Take

- Be selective about which online companies you shop, use familiar companies
- Search the company or website along with the words “scam” or “review” to learn if there are bad reviews
- Pay attention to subtle differences in the websites URL
- **Do** look for a message from your internet security provider at the bottom of the page such as this one:



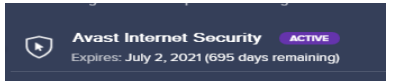
- Report scams to FTC at (877) 382-4357 or ftc.gov/complaint

Retailer Email Links

Be alert: If it sounds to good to be true it probably is!

Do’s and Don'ts

- **Don’t** click on links you’re unfamiliar with
- **Don’t** click on email links with an “Unsubscribe” button
  - Scammers use that link to send you to a website that can download virus’s to your computer, it also confirms your email is active
- **Do** mark the message as “Spam” instead
- **Do** type the merchant’s website address into your search bar instead of clicking the link
- **Do** look for a message from your internet security provider at the bottom of the page such as this one:



  - It will warn you if a page is safe or a security risk

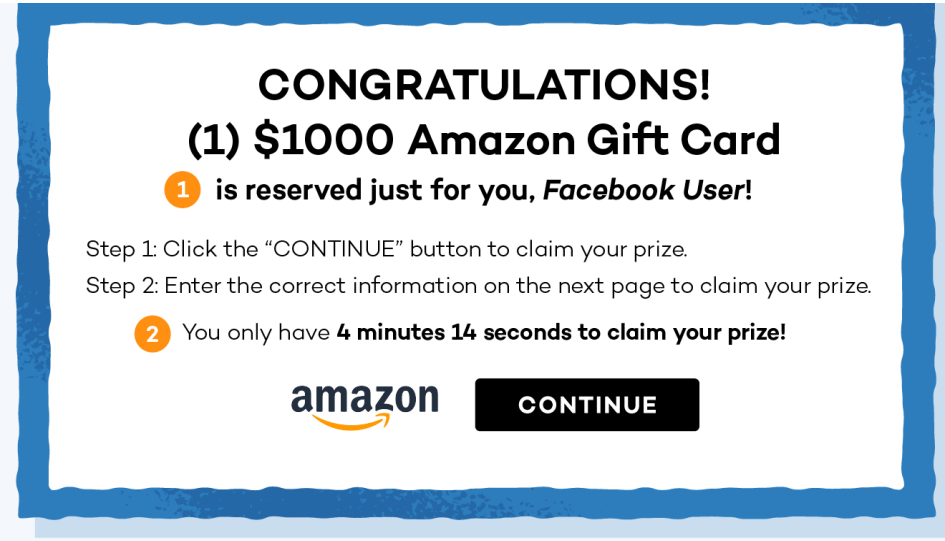
Credit Card Fraud

Don't be a victim, be proactive!

Here's what you can do

- Be stingy with your credit card information
- If a merchant notifies you of a credit breech, immediately notify your credit card issuer, cancel your current cards and ask for new ones
- Many credit card companies offer credit monitoring services in these situations. If they do not offer it, ask. If not free, it may be worth purchasing the protection on your own
- If you lose a credit card, immediately notify your card issuer and repeat the above process
- Change your passwords often

“You’ve Won” Scam



Here’s what you can do

- Never share your financial information
- Never directly wire money to anyone

Here’s how it works

- You get a card, a call, or email telling you that you won a trip or prize, lottery or sweepstakes!
- The person calling is so excited and can’t wait to get you your winnings
- They tell you there are fees or taxes to pay
- They ask for your credit card number, bank account information, or ask you to wire money
- You never get the “big prize”, you get more requests for more money

Charity Fraud

Here's what you can do

- Tell the caller to mail you information
- Research the charity online
- Ask what percentage of your donation goes to the charity
- Ask if your donation is tax deductible
- Consider adding your home phone and cell phone to the Do Not Call List at www.donotcall.gov

Here's how it works

You're contacted by someone asking for a donation. How do you tell if its legitimate or a scam?

- Scammers pressure you to donate right away
- They may ask for cash or ask you to wire money
- They may refuse to give you details of the charity or tell you how the money will be used
- They may even thank you for a pledge you don't remember making
- They will try to shame you into giving

Tech Support Fraud

Here's what you can do

- Stop, close the pop-up window
- Don't call or click a link
- Don't send money
- Don't give out your credit card information
- Don't give control of your computer to anyone

Here's how it works

- You get a pop-up or urgent message saying your computer is infected from someone posing as Apple or Microsoft
- It tells you there are viruses or malware on your computer and you have to call a number or risk losing your data
- Is this problem real? The FTC Says, no
- These scammers want to sell you useless services, steal your credit card information, or gain access to your computer to install malware which would allow them see everything on your computer

Beware of Public Wi-Fi

Here's how it works

- Hackers position themselves between you and the Wi-Fi connection point
- This "man in the middle" then collects your data when you use the free Wi-Fi

Wi-Fi Do's and Don't

- **Don't** access personal bank accounts or sensitive personal data on public networks
- **Don't** leave your laptop, tablet, or Smartphone unattended
- **Don't** shop online on public networks

- **Do** turn off automatic connectivity on your device
- **Do** think about using a virtual private network (VPN) to ensure your privacy

Identity Theft

What can you do

- Shred documents or bank statements
- Provide your SS# only when you must
- Use strong passwords
- Review monthly statements and credit report at least once a year
- Get a free annual credit report at: AnnualCreditReport.com

How it works

- Someone gets your personal information and runs up bills in your name. They may use your SS#, Medicare # or credit card information
- You get bills you don't expect
- Your bank account may have withdrawals you didn't make
- Your credit report shows accounts you never knew about

Important Contact Information

Phone Numbers

To report something or someone suspicious:

- NMB Department of Public Safety: **843-280-5511**
- Horry County Sheriff: 843-915-5454

Online websites to verify

- To check on scams regarding corona virus:
  Federal Trade Commission: ftc.gov/coronavirus
- To verify business worthiness:
  Better Business Bureau: bbb.org
- To get a copy of your credit report:
  annualcreditreport.com
- To report price gouging:
  SC Attorney General: scag.gov
- To add your phones to a Do Not Call list:
  www.donotcall.gov