Review the following recommendations to stay safe this holiday season:

# Online Shopping Top Scams

* **Phony retail websites.** Stick to reputable sites, type a retailer’s address directly in your browser, and look for “s” in the address bar, such as https://.
* **Malicious mobile apps.** Be wary of bogus smartphone applications, often having names similar to legitimate retailers. Use the retailer’s website to shop.
* **Fake product ads.** Prevalent on Facebook and Twitter, if the price or discounts look too good to be true, or if they request immediate action, they are probably a scam.
* **Phony contests for popular gift items.** Promoted via email or social media, fake contests entice shoppers to share personal or financial information. Always verify that a contest is legitimate and go directly to the retailer’s site for entry information.
* **Bogus gift cards.** Deeply discounted gift cards are a recent scam. To protect yourself, buy gift cards directly from the retailer or a reputable reseller.
* **Holiday smishing.** Phishing text messages, or smishing, arrive in your text inbox advertising phony contests or prizes and contain a link to a malicious website. It’s best to delete text messages from unrecognized senders and avoid clicking suspicious links.

# Protect Financial Information

* Be wary of any requests to wire funds and avoid doing so
* Use credit cards for online shopping rather than debit cards
* Avoid conducting financial transactions or online banking over public Wi-Fi
* Only provide the information needed to complete the transaction when opening online accounts
* Save records of online transactions, review credit card statements thoroughly, and report any discrepancies immediately
* Be aware of your surroundings when entering your PIN at ATMs or making purchases in stores

# Use Secure Passwords

* Use a unique password for each system or site that requires a password
* Create a passphrase that is eight characters or longer and includes letters of mixed cases, numbers, and symbols
* Be cautious of requests for passwords and do not share them with others
* Change passwords periodically
* Store passwords in a secure location

# Seasonal Phishing Scams

* Be aware of targeted email campaigns disguised as deals on holiday items or gift cards that seek personal or financial information
* Avoid downloading malicious software or entering personal information into a directed website
* Use trusted sites and type their address directly into your browser rather than clicking links
* Avoid clicking holiday electronic card message hyperlinks
* Use charitable organizations’ secure websites to donate directly and verify the address typed into the browser includes an “s”, such as https://

# Seasonal Travel

To decrease risks of device or data loss when traveling:

* Transport devices in carry-on bags rather than checked bags
* Disable Wi-Fi and Bluetooth settings when not in use
* Familiarize yourself with the laws in any foreign destinations as they relate to security screening and surveillance
* Avoid posting vacation plans on social media
* Move valuables such as electronic devices away from windows
* Ask a trusted friend to receive mail and packages to help safeguard personal and financial information

# Working Outside the Office

* Familiarize yourself with firm policies on remote access and connectivity
* Use secure Wi-Fi, which requires a password to connect

# Physical Threats

* Be wary of holding secure entrance doors open for strangers, as criminals often pose as delivery persons, new hires, or repairmen
* Question strangers in the building and escort them to the appropriate reception area to receive credentials
* When holiday gatherings take place onsite, lock your computer and store electronic devices in a locked drawer, or keep them with you
* Lock purses, wallets, and paper-based information in a drawer when leaving your workspace
* During off-site holiday gatherings, use caution discussing sensitive firm matters and keep briefcases, purses, bags, and electronic devices close to you

# Before Selling or Donating Devices

If you receive a new device as a gift, before selling or donating your previous device, keep the following in mind:

* Back up data, including photos, videos, and contacts
* Use the device reset command to restore it to the factory default state, also known as “wiping the device clean” (visit the device website for exact instructions)
* Contact the wireless provider to cancel service for the device; or
* Contact the firm technology department to ensure the device has been wiped in accordance with firm policies and procedures if the device was used to access firm resources or contains firm information