

Stay Safe for the Holidays

November 9, 2023

The holidays are right around the corner. This is a prime time for holiday shopping scams and cyber threats. Bad people use this opportunity to take advantage of the holiday giving season – remain vigilant and take precautions. Don't let a cybercriminal ruin your holiday!

Safe Social Media Posting

Posting photos and status updates over the holidays can be a simple and fun way to stay connected with your loved ones. While we may enjoy sharing photos of our winter getaway and gifts, it's important to remember the content of these online posts could be dangerous in the wrong hands.

Avoid geotagging your location.

Many social media apps prompt users to add a location to their posts or to "check-in". For public, social media profiles, this information can act as a potential treasure map for burglars. This data can be used to pinpoint the general area of your home.

Geotagging can become especially dangerous when your location check-ins suddenly move from your neighborhood to a tropical beach resort – indicating to thieves you are out of town and your house is likely empty.

Be sure to deactivate the geolocation feature on all your mobile devices. Even if you do not manually check-in to locations, an enabled location setting could still reveal where you are posting.

Never reveal your address.

Avoid posting photos of your neighborhood and the exterior of your house. These posts could reveal your home address to criminals who know where to look. If you do share, make sure no identification markers such as street signs, house numbers, unique decorations or architectural elements are present in the photo.

Wait until you are home to post vacation photos.

Resisting the urge to share photos of you living it up on your winter getaway can be difficult. Yet, any photos of you enjoying the white sand and blue skies of a beachfront resort are a clear sign to burglars your house is empty. Unplug, enjoy your vacation and save the photo sharing for when

you return home.

Refrain from showing off your valuables.

It can be fun to show off your shiny new gifts to friends and family. Remember, sharing photos of your valuables online could make your home a potential break-in target for thieves.

Double check your privacy settings.

A best practice you should follow throughout the year is to regularly comb through your friends and followers lists to delete, or limit the viewing settings, of any connections you do not completely trust. Several social media platforms provide you with options to limit your posts' exposure to different groups.

Safe Online Holiday Shopping

Holiday shopping will soon be in full swing. Online shopping is often the most convenient way to buy for everyone on your list. Be sure to follow these tips to ensure your holiday is Merry and Bright!

Keep an eye on your bank statements.

Pay close attention to your financial records, such as bank statements and credit card transactions. Flag any suspicious activity (charges you do not recognize or did not make) and contact the institution immediately.

Know how much items cost.

When shopping online, have a general sense of how much the items you want to buy should cost. This will help you get an idea if an online store has prices too good to be true. In these cases, you may pay less, but what's the cost? You may receive an item not matching the description, a counterfeit item or not receive anything at all! A little bit of research can help protect you.

Remember the 4 key behaviors from Cybersecurity Awareness Month:

- Protect each account with a **unique, complex password** (at least 12 characters long) – and use a **password manager**
- Use **multifactor authentication** (MFA) for any account that allows it
- Turn on **automatic software updates**, or install updates as soon as they are available
- Know how to **identify phishing attempts**, and **report** phishing messages

Do not use public Wi-Fi (wireless network) for shopping.

Public Wi-Fi is convenient and sometimes necessary to use. However, public Wi-Fi is not very secure – you should never shop online or access important accounts (banking) while connected to public Wi-Fi. Do your online shopping at home. If you must buy a few gifts online, while away from your home, use a VPN (virtual private network) or mobile hotspot.

Happy Holidays!

This is the last MCC Cybersecurity newsletter for 2023. Due to the MCC winter break, there will not be a newsletter for December 2023. Have a safe and happy holiday season, and see you next year!

Revision #1

Created 10 February 2025 14:55:51 by Laura J. Crapps

Updated 10 February 2025 14:56:05 by Laura J. Crapps