December is the prime shopping month of the year for everyone. Every year cyber criminals compromise systems, perform identity theft transactions, and make the holidays more about fear than cheer. But fear not! Follow these tips to help keep you safe while shopping online during the holidays.

Make time to shop without feeling stressed or pressured.
Safety is of utmost importance. Cyber criminals know that feeling pressured and stressed can cause folks to give up their guard. It is human to make mistakes while stressed and under pressure. Folks have shopped on non-legitimate websites, click on an e-mail with a deal that is too good to be true, forget their credit card on a store counter, or order a wrong gift.
When shopping online keep your machine up to date with the latest security patches.
Your Operating system, your web browser and any add-on features are the gateway for passing information securely. Both should be updated regularly to ensure you have the latest security and bug fixes.

Don’t use your debit card. Use cash or a credit card.
There is fraud protection available for both, but it can take time to clear up any issues and your account may be unavailable for use while you wait for the issue to be resolved.

DO NOT use public Wi-Fi for any shopping activities.
You may be tempted to do your shopping using the local public coffee shop wi-fi or public airport wi-fi. Stay away from using those amenities since a free item isn’t always maintained with the latest security protocols and could potentially be compromised waiting for unsuspecting connections to be eavesdropped.

Be wary of shady websites with great holiday deals.
The saying, “If it is too good to be true...” fits well here. This is especially true if the vendor selling an item doesn’t have a standing, reputable presence on the internet. Always review a vendor for legitimacy before attempting to give them your data. Gateways to illegitimate sites can come from e-mails that may look legitimate. As always, don’t open e-mails from unknown senders or click on links that may look suspicious.
Make sure that the site you are accessing is secure.

Shop securely. Look for https is the URL. Sites without the S in front of http are not safe to submit payment information or other personal details. Using http will send any data over in clear text which can be intercepted by cyber criminals. Doublecheck the website name. Check the spelling of the organization's name and the URL very closely for discrepancies. The spelling is important since cyber criminals often create websites and names that are very similar to legitimate, reputable organizations.

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

Do your research first. Never feel pressured to give on the spot. Visit the Internal Revenue Service website to learn more about what types of organizations can get tax-deductible donations. Also, use other online resources, such as Charity Navigator, CharityWatch or GiveWell, to learn about charities and how they spend the money they receive. 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 their number to donate.

Have a happy and safe holiday!

-Information Security Office