‘Tis the Season – Stay Safe for the Holidays

Original content posted by staysafeonline.org - check them out for more tips about cyber safety

For many people, online shopping is simply “shopping.” Who can resist one-click ordering and next-day delivery? However, online shopping isn’t just convenient for us and good for businesses...it can present many opportunities for scammers and cybercriminals.

Bad actors try to trick consumers into paying for goods that don’t exist. Cybercriminals seek to capture personal information for financial gain.

You don’t need to abandon your cart, though. With some simple preventative measures, you can enjoy your online shopping spree with peace of mind.

Think before you click.

Beware of emails, texts or other promotions that seem suspicious or encourage you to urgently click on links. If you receive an enticing offer, check to see if it is coming from an actual retailer and uses a web address that matches the company’s online store. If you can sense that someone is trying to imitate a legitimate retailer,
report the scam to your email provider as a phishing attempt. Remember: if it seems too good to be true, it probably is.

Do your homework.

Scammers are fond of setting up fake e-commerce sites. Prior to making a purchase, read customer reviews of the merchant. Check trusted sources, like the Better Business Bureau, as well as online platforms. In addition, see if the store has a physical location and any customer service information. If you still have doubts, call the merchant to confirm that they are legitimate.

Consider your payment options.

If possible, use a credit card instead of a debit card because there are more consumer protections for credit cards if something goes awry. You might be able to opt for a third-party payment service instead of your credit card. There are many services you can use to pay for purchases — like Apple Pay or Google Pay — without giving the merchant your credit card information directly.

Share with care.

Pay attention to the types of information a website collects to complete your transaction. If a merchant requests more data than you feel comfortable sharing, cancel the transaction. You only need to fill out required fields at checkout and you should not save your payment information in your profile. If the account autosaves it, delete the stored payment details after making the purchase.

Keep tabs on your bank and credit card statements.

Continuously check your financial accounts for any unauthorized activity. Good recordkeeping goes hand-in-hand with managing your cybersecurity. Many credit card companies allow users to set up alerts that send emails or text messages with transaction details every time your credit card is used.

Use secure Wi-Fi.

Shopping online using public Wi-Fi while at a coffee shop or airport is convenient, but it is not very secure. Avoid making online purchases via public Wi-Fi. Instead, use a Virtual Private Network (VPN) or your phone as a hotspot. You can also save items in your cart for later and make the purchases at home on your own secure network.

Enable multi-factor authentication.

Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.