BLACK

FRIDAY

Savings Start Early...
But Cybercriminals Lurk -
Stay Vigilant Online

SECURE OUR WORLD

ACT SMART I.T.
Helping You Benefit From Today's Technologies

Online Shopping – "Black Friday Sales" Start Earlier Every Year!

While online shopping offers convenience and benefits for consumers and businesses, it also presents numerous opportunities for scammers and cybercriminals to exploit unsuspecting individuals. Here are some of the common threats and tactics employed by bad actors in the online shopping space: With some simple preventative measures, you can enjoy your online shopping spree with peace of mind.

CLICK

Think Before You Click:

Beware of emails, texts, or other promotions that seem suspicious or encourage you to click on links urgently. If you receive an enticing offer, check to see if it comes from an actual retailer and uses a web address matching the company's online store.

Look for HTTPS and a Padlock Symbol:

Before entering any personal or payment information, ensure the website has a secure connection.
Look for "https://" in the URL and a padlock symbol in the address bar.

Do Your Homework:

Scammers create fraudulent e-commerce websites that mimic legitimate ones. These sites often offer enticing deals on products that don't exist or are of poor quality. See if the store has a physical location and any customer service information. If you still have doubts, call the merchant to confirm 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. Opt for a third-party payment service instead of your credit card if available. You can use many services to pay for purchases – like Apple Pay or Google Pay — without giving the merchant your credit card information directly.   Your credit card might offer "virtual account numbers" that work similarly.

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 the 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 purchasing.

You never need to give out your Social Security number to make a simple purchase. Consider it a red flag if a website seems to be asking for more information than is normal or necessary.

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 their credit card is used.

Save receipts, order confirmations, and all communication with the seller. These can be helpful in case of disputes or issues.

Use strong, unique passwords:

Create strong and complex passwords for your online shopping accounts. Use a password manager to keep track of them.

Use secure Wi-Fi:

Shopping online using public Wi-Fi while at a coffee shop or airport is convenient but 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:

Whenever possible, enable 2FA for your online shopping accounts, adding an extra security layer.

GIVE THE GIFT OF CYBERSECURITY:

Purchasing an internet-connected device for a loved one? Research how to make the device secure and let the recipient know. Make sure they know how to configure privacy and security settings, set up a strong password, and deactivate any features they don't need.