Safety Tips for Online Shopping

Online shopping is the way of the world now. Shopping has never been so easy and cost effective. From the convenience of your home, you can shop and to your hearts content which saves time, money, and opens up a whole world of possible purchases.

The convenience of making purchases online may also put you at risk for cyber security breaches and scammers.

Be a safe and secure shopper by taking security precautions, think about the consequences of your actions online and enjoy the convenience of technology with peace of mind while you shop online.

Online Shopping Tips:

Think before you click: Beware of ads encouraging users to click on links. Go direct to the company website to verify the offer is legitimate.

Do your homework: Prior to making the purchase, read reviews, look for physical location and customer service information and call the merchant to confirm they are legitimate.

Consider your payment options: Using a credit card is much better than using a debit card; there are more consumer protections for credit cards if something goes wrong. Or, you can use a third-party payment service such as Google Pay without giving the merchant your credit card information directly.

Watch what you give away: Be alert to kinds of information being collected to complete your transaction. If the merchant is requesting more data than you feel comfortable giving, cancel the transaction. Do not save your payment information in your profile. If the account autosaves it, after the purchase go in and delete the stored payment details.

Watch Your Bank and Credit Card Statements: Continuously check your accounts for unauthorized activity. Do not delay in reporting entries you do not recognize. Set up alerts for your credit card so you receive emails or texts when the card has been used.

Use a Secure Wi-Fi: Public Wi-Fi to shop online is not cyber safe. Don make purchases via public Wi-Fi: instead use a Virtual Privat Network (VPN) or use your phone as a hotspot.

Lock Down Your Login: Create complicated passwords, use multi-factor authentication (MFA) wherever possible. Use biometrics or a unique one-time code sent to your phone or mobile device.

Keep a Clean Machine: Be sure that all internet connected devices – including PCs, smartphones and tables are free from malware and infections by running only the most current versions of software and apps.