Contributed by the Technology Advisory Committee

Best Practices When Shopping Online

We live in an era when the consumer experience of shopping online is fast and convenient. That speed and convenience can present opportunities for scammers and cybercriminals. Taking simple preventative measures can help safeguard your personal and financial information when transacting online. The best practices recommended in this article, if incorporated into your online shopping routine, will ensure your online shopping experience is safe and secure.

The Cybersecurity and Infrastructure Security Agency (CISA) says that creating fraudulent websites and emails, intercepting insecure transactions, and targeting vulnerable computers and devices are the three most common ways attackers take advantage of online shoppers. What can you do to protect yourself?

Know the vendor and how they will use your information

Before providing any personal or financial information, ensure you are dealing with a reputable and established vendor. Attackers will create websites that appear legitimate in order to trick you into giving them information. Always verify the legitimacy of the vendor and their website or app. Although collection of some information is a standard method to ensure a purchase can be completed, consumers should understand how their information will be stored

and used. If you feel uncomfortable with the information being requested, cancel the transaction. Always review the privacy policies and your account settings for a vendor's website or app. Also, be wary of emails requesting purchase or account information. Legitimate vendors will not request that information through email.

Make sure your information is being encrypted

Many websites and apps secure customer information through encryption. Clear indications that your information will be encrypted include a web address with a Uniform Resource Locator (known as "URL") that begins with "https:" rather than "http:" and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by web browser. Attackers may try to trick users by adding a fake padlock, so make sure that the icon is in the correct location for your browser. These encrypted transactions are regulated by Payment Card Industry (PCI) Security Standards. This ensures that payment card use, and the transmission of consumer financial information follows industry regulations.

Protect your devices and accounts

Make sure that software for computers and devices used for online transactions are updated and protected against known threats. Ensure strong unpredictable passwords are used. Passwords should be at least 12-16 characters and use complex combinations of letters, numbers and special characters. Consumers should also consider using security measures such as multi-factor authentication (MFA), and a password manager for securely storing and managing passwords. Due to a lack of security, avoid using public Wi-Fi for online transactions. Instead, use a Virtual Private Network (VPN) or your cellphone as a Wi-Fi hotspot. You can always wait until you are home on your secure network to complete the transaction.

Payment methods and transaction monitoring

Consider using a credit card rather than a debit card, which draws directly from a bank account. There are laws that limit liability for fraudulent credit card charges that you might not get with a debit card. Secure payment services, including, but not limited to, Apple Pay and Google Pay, can also be used to complete online transactions without giving vendors your payment card information directly. Regardless of the payment method you choose, always monitor your bank and payment card statements for unauthorized activity and report any discrepancies immediately. Many banks and card issuers allow customers to set up transaction alerts for when a payment card is used, which can assist with monitoring for fraudulent activity.

Sources:

Cybersecurity and Infrastructure Security Agency (CISA)

National Cybersecurity Alliance (NCA)

PCI Security Standards Council