Safe Holiday Online Shopping Tips

As we begin to approach the holiday season, many of us turn to online shopping to purchase gifts for family, friends, and coworkers. Unfortunately, online shopping can lead to many headaches and problems with fraudulent retailers, credit card theft, account hacks, and more. To prevent the holidays from being ruined, please practice the following tips to ensure you and your loved ones enjoy this season:

1. Shop with reputable retailers.
   Shop with retailers you frequently do business with. Avoid shopping on websites that are unfamiliar to you.

2. Check website security.
   The first red flag to check for when shopping on a website is in the address bar at the top of the browser window. Website links should begin with “https” rather than just “http.” A website that contains “https” is using SSL (secure sockets layer) encryption ensuring it is a safe website.

3. Amazing deals too good to be true.
   If a deal for a high demand item appears too good to be true, it usually is. When this happens be sure to follow the steps above. Reputable retailers tend to run deals on high end / high demand products for Black Friday. However, if the deal is coming from someone unfamiliar, it is usually a scam.

4. Verify new retailers.
   If you are shopping on a new website recommended by a relative or friend and are unfamiliar with the retailer, be sure to verify the retailer. Check that the website link contains “https,” has a residency within the US, and is listed on the Better Business Bureau.

5. Use strong account passwords and two factor authentication.
   When setting a password for your shopping account or any account online, it is best practice to use a password that incorporates: upper case letters, lower case letters, numbers, and special characters. Avoid incorporating birth dates, your name, or other information that is easily accessible. If possible, two factor authentication should be enabled on the account and verification sent to a readily accessible device like a personal cellphone. This will prevent others from logging into your account if they would happen to get your password.

6. Use a VPN.
   If you do happen to use public Wi-Fi or a shared Wi-Fi network in a residential building, protect yourself with a VPN (virtual private network). A VPN creates an encryption between your computer and the server preventing cybercriminals and others from seeing what you are doing or intercepting your personal information.

7. Protect personal information.

   Personal information such as your social security number and date of birth (unless purchasing alcohol, tobacco, etc.) should never be required when shopping online. Be mindful of the information asked upon when checking out your shopping order.

8. Pay with a credit card, not a debit card.

   Always use a credit card to shop as securely as possible. A credit card is not directly connected to the money in your bank account, preventing a seller or hacker from accessing it. Also, most credit cards offer $0 liability for fraud meaning that if someone does steal your info and begins making purchases, you're not out of any money. Most credit card companies will block the card and follow up with a phone call and begin investigating the fraudulent activity.

9. Check your bank accounts and statement.

   Check your bank and credit card statements for fraudulent charges. Most banks have an app or website where your recent card activity can be viewed. Account alerts can be setup to notify you of any new activity on your card.

10. Contact bank immediately if you see any suspicious activity on accounts.

    If you do not recognize any recent purchases on your credit card or debit card, contact your bank immediately. Do not let any unrecognizable purchases go without notifying your bank, as this may make it difficult to be issued a refund. The sooner it is reported, the easier it is to resolve.