8 Shopping Tips for the Holiday Season

As you know, the Privacy Office occasionally issues tips for the purpose of assisting you in making informed decisions in your "away from work" life. The following tip is for that purpose (and we all know that we cannot use the internet for shopping, managing bank accounts, etc. while on the job and with State equipment!).

It's that time of year again, holiday shopping has begun! Everyone is looking for those unique gifts, hot toys and cool electronics. Whether it is a hard-to-find toy for kids or the latest 4K smart TV. Black Friday sales seldom fail to pique the interests of even the most casual shoppers. Yet even after the chaos of Black Friday lies both Small Business Saturday and Cyber Monday. While it's clear that businesses are after your dollars during the holidays, you should be aware that cybercriminals are on the lookout, too.
When it comes to holiday shopping, you need to be careful that you don't fall prey to these criminals. Here are some tips to following for your holiday shopping:

Online Shopping Tips

1 **Do not use public Wi-Fi for any shopping activity.**
Public Wi-Fi networks can be very dangerous, especially during the holiday season. Public Wi-Fi can potentially grant hackers' access to your usernames, passwords, texts and emails. For instance, before you join a public Wi-Fi titled "Apple__Store," make sure you first look around to see if there's actually an Apple Store in your vicinity, and thus, confirm that it is a legitimate network. To help stay secure, you should always be on the lookout for the lock symbol on your webpage.

2 **Look for the lock symbol on websites.**
When visiting a website look for the "lock" symbol before entering any personal and/or credit card information. The lock may appear in the URL bar, or elsewhere in your browser. Additionally, check that the URL for the website has "https" in the beginning. These both indicate that the site uses encryption to protect your data.

3 **Know what the product should cost.**
If the deal is too good to be true, then it may be a scam. Check out the company on "ResellerRatings.com". This site allows users to review online companies to share their experiences purchasing from those companies. This will give you an indication of what to expect when purchasing from them.

4 **One-time use credit card numbers.**
Many banks are now offering a single use credit card number for online shopping. This one-time number is associated with your account and can be used in place of your credit card number. This way, if the credit card number becomes exposed, it cannot be used again. Check with your credit card company to see if they have this option available.

5 **Keep your computer secure.**
When using your computer to do your holiday shopping, remember to keep your Anti-virus software up to date and apply all software patches. Never save usernames, passwords or credit card information in your browser and periodically clear your offline content, cookies and history.

You will want to keep your computer as clean as possible for online shopping. The world of online shopping can bring lots of new products to your door step and can prove to be a lot of fun finding that special gift. Just remember to be careful so that you don't make your data a special gift to cybercriminals.

In-Store Shopping Tips

6 **Always use credit cards for purchases.**
Avoid using your ATM or debit card while shopping. In the event that your debit card is compromised, criminals can have direct access to the funds from your bank account. This could cause you to miss bill payments and overdraw your account. When using a credit card, you are not using funds associated with your bank account. This means you are better protected by your credit card company's fraud protection program. If you pay off the credit card balance each month, you won't pay interest and your banking information will be protected.

7 **Don't leave purchases in the car unattended.**
Criminals can be watching and will consider breaking into your car to get the merchandise you just purchased. If you must leave some items in your car, consider leaving them in the trunk or glove compartment rather than in a visible location.

8 **Beware of "porch pirates."**
When shopping online and receiving purchases by mail, make sure you are always tracking your packages. The US Postal Service, FedEX and UPS all have systems to track your packages, and all three utilize tracking numbers that can be used to figure out where your item is and when it should be delivered to your home. However, the only surefire way to thwart porch pirates is to not have packages delivered to your home at all. Consider having your holiday packages delivered to a family member, your workplace, or a trusted neighbor!

Remember, always trust your instincts. If an email or an attachment seem suspicious, don't let your curiosity put your computer at risk! ~ Happy Holidays and safe shopping!

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.