State Privacy Office
November Privacy Tip

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!).

With holiday shopping in full swing, we wanted to let you know about a few online shopping trends we've noticed and give a few tips about how to stay safe online while buying gifts for everyone on your list. Each dollar you spend is very important, which is why we want to help you protect your hard-earned cash from the scammers and hackers that pop up every year. It's like they don't care about the naughty list!

Here is what we think is cheerful and what we think is coal-worthy for shopping online this holiday season:

Merry and Bright

Keeping an eye on your bank statements

Your first line of defense against identity theft and fraud is to pay close attention to your financial records, like bank statements and credit card transactions. You can usually follow this data up-to-the-minute online. Flag any suspicious activity (like being charged for a purchase you didn't make) and contact the institution immediately.

Knowing how much items should cost

When shopping online, have a general sense of how much the items you want to buy should cost. Not only will that make you a comparison shopping extraordinaire, but you can also get a sense if an online store has prices that are too good to be true. In these cases, you might pay less, but then you might get an item that doesn't match the description, is a counterfeit, or you might pay and not get any item at all! A little bit of research can help protect you.

Making a cybersecurity list, checking it twice

This year, give yourself the gift of peace of mind by following our Core 4 behaviors:

1. Protect each account with a unique, complex password that is at least 12 characters long – and use a password manager!
2. Use multifactor authentication (MFA) for any account that allows it.
3. Turn on automatic software updates, or install updates as soon as they are available.
4. Know how to identify phishing attempts, and report phishing messages to your email program, work, or other authorities.

Bah! Humbug!

Shopping on public wi-fi

Public wi-fi and computers are convenient, and sometimes necessary to use. However, public wi-fi is not very secure – you shouldn't ever online shop or access important accounts (like banking) while connected to public wi-fi. If you must buy a few gifts online while away from your home or work network, use a VPN (virtual private network) or mobile hotspot.

Grinch Bots

Last year, a record number of so-called "Grinch Bots" were recorded. These are automated programs that quickly buy up popular toys, sneakers, or other items and then resell the item for a huge mark-up to real people. Of course, buying supposedly new items on a resale market opens you up to an increased risk of fraud and counterfeit goods. The best way to defang Grinch Bots is to refuse to buy from them, and to only buy items from vendors you can verify.

Sharing more than you feel comfortable with

While you need to share data to make a purchase online, you should be wary of any retailer that is requesting more information than you feel comfortable sharing. Oftentimes, you don't need to fill out every field, and you shouldn't if you don't want to. If an online store requires you to share more information than you want, find another retailer on the internet – or in real life!

Keep the spirit of cybersecurity going all year long

These are some great tips for shopping safe online for the holidays, but they are also sensible habits to follow no matter what month it is. Want to make some cybersecurity resolutions for the new year? It's easy – we promise! Check out our cybersecurity basics page to learn more!

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