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!).

10 Tips for a Safer Online Shopping Experience

Online shopping is convenient, in that you can shop around, find the best prices, and have your packages delivered right to your doorstep without ever having to leave the comfort of your own home. But getting a great deal online involves more than just getting the lowest price. You'll want to be sure that products arrive on time, that quality is what you expected, that items include a proper warranty, and that there is a way for you to return products or get support with any questions or issues you have. Apply these tips to improve the security of your shopping experience.

1. Always place orders from a secure connection

If your computer isn't protected from potentially malicious software, your financial information and passwords are at risk from being stolen (and everything else you store on your computer or do online). This concept is so basic, yet only a fraction of the U.S. population adequately protects their computers. Use a secure connection – make sure your computer's firewall is on.

If you're shopping online while using a wireless network, it needs to be encrypted so someone who is lurking outside the house can't collect your information. Avoid making any financial transactions when using a public network, as you may not know if it's compromised.

2. Know the merchant and their reputation

If you already know the store, shopping at their online store is very safe. You can always walk into the local store for help if there's a problem, and if you know others who have had consistently positive experiences with the online store, you can be reassured of the site's quality.

If you don't know the store, it may still be the best bet; you just need to take a few more precautions. Conduct your own background check by looking at sites dedicated to reviewing e-stores. If the store isn't reviewed or does not have favorable reviews, don't order from their website.

3. Avoid offers that seem "too good to be true"

Any e-store that promises too much at too low a price is suspicious. If the price is too low, consider whether the merchant came by the items legally, if you will ever receive the items you paid for, whether the items are actually the brand shown or a cheap substitute, if the item will work, if you will be able to return damaged goods – or if the merchant is earning extra income by selling your financial information. Disreputable online stores – like their brick and mortar counterparts, may run an absurdly low price offer and then claim the item is out of stock, to try to sell you something else in a classic "bait and switch" scam.

4. If you are buying a Gift Card, read the Terms and Conditions

If the gift card is for someone else, be sure the store is legitimate, that the person uses the store, and that there are no hoops they will have to jump through.

5. Don’t use an e-store that requires more information than necessary to make the sale.

Expect to provide some method of payment, shipping address, telephone number, and email address, but if the merchant requests other information, walk away. You never want to give them your bank account information, social security information, or driver’s license number. Some companies ask questions about your interests, but these should always be optional and you should be cautious about providing the information. Does the merchant resell, rent, or share your information? Check the site’s privacy policy to understand how exposed your information may become. Many stores clearly state that they do not share, sell or rent consumer’s information – others say they own your info and can use it (or abuse it) however they choose. Stick to the companies that respect your privacy.

6. Need to create a password for the site? – make it unique.

You will often be asked to create an account with a password when you make a purchase. Usually, you can choose not to do this, and unless you will use the e-store frequently, don’t create an account. If you do want an account, make sure to use a unique and strong password.

7. Is the site secure?

Before entering any personal or credit card info onto a shopping site look to see if the web address on the page begins with "https:", not "http:" That little ’s’ tells you the website is secure and encrypted to protect your information.

8. Use a Credit Card or PayPal

Do not use a debit card or check as these do not have the same security protections in place for you should a problem arise. Credit card purchases limit your liability to no more than $50 of unauthorized charges if your financial information is stolen, and the money in your bank account is untouched. Most debit cards do not offer this protection – and even when they do, you’re the one out of funds in the meantime.

Consider designating one credit card that is only for online shopping and transactions. This way, if the card gets compromised, you can quickly shut it down without impacting any other type of transactions.

9. Always check the company’s shipping terms.

Some merchant’s charge exorbitant shipping fees that can turn a shopping bargain into an expensive mistake. Look to see if they provide tracking and insurance. Understand what carriers they use, and be particularly cautious if the item won’t be shipped within 10 days.

10. Use a reliable internet security program.

The best way to stay safe online is still by using an effective internet security product. Shopping is no exception. Rather, with the increasing volume of goods and data being exchanged online, security features like real-time anti-phishing and identity theft protection are more important than ever.

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