From the office of
Information Technology

10 Cybersecurity Shopping Tips for the Holiday Season

It's that time of year again -- holiday shopping is in full swing! Even though the shopping insanity of Black Friday, Small Business Saturday, and Cyber Monday have come and gone, holiday shopping is still at the forefront of many consumers' minds. Due to the fact that many consumers are avoiding stores and buying more online, e-commerce sales are rapidly on the rise, with no sign of consumers reverting to their old ways anytime soon.

Thankfully, online shopping gets more intuitive and simplistic by the day, allowing you to get that perfect gift with ease. However, while embarking on your online shopping conquest, make sure you're not leaving yourself at risk. It's clear that businesses are after your dollars during the holidays, but cybercriminals are on the lookout as well, now more than ever.

While you may not have to worry about being pickpocketed in the cyber world, you still need to be careful that you don't fall prey to criminals. Here are 10 online shopping tips that can help you keep your information out of the hands of those who are most certainly on the naughty list:

1. Do not use public Wi-Fi for any shopping activity.	Public Wi-Fi networks can be very dangerous, especially during the holiday season. While they are very convenient, they are not secure, and 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. While it is best to avoid public Wi-Fi altogether, if you need to utilize a public network ensure that you never establish an autoconnection, and that you are logged out of all personal accounts, such as your banking sites. Though it is perfectly acceptable to auto-connect to a trusted source such as your home, when out in public, consider shutting off the Wi-Fi option on your phone and use your data plan. Yes, it's slower, but if you can wait for Santa's elves at UPS to deliver your presents from Amazon, you can certainly wait the few extra seconds it takes to use the internet, especially if it means your information is not at risk.
2. Make sure the site is secure.	Before entering your personal or financial information, you need to ensure that the site you are on is legitimate and can be trusted. When visiting a website look for the "lock" symbol; this might 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. Give your debit card a holiday break.	When you are shopping online always remember that it is best to rely on your credit cards or payment services such as PayPal. Credit cards offer much more protection and less liability if your information were to be compromised. On the contrary, debit cards are linked directly to your bank account, thus, you're at a much greater risk if a criminal were to obtain this information. Additionally, in the event of a fraudulent transaction were to occur, credit card companies possess the ability to reverse the charge and hopefully, investigate the issue further.
5. Stay updated.	Updating your operating system and software (including anti-virus software) is one of the most important and easiest things you can do to prevent criminals from accessing your information, and needs to be taken very seriously. Most software updates are released to improve your security by patching vulnerabilities and preventing new exploitation attempts by criminal hackers. While waiting for your computer or mobile device to update might seem tedious, the benefits it can provide could be a blessing in disguise. If you see that your device needs to be updated, do it!
6. Outsmart the scammers.	During the holiday season we often see an influx of emails with discounts. While many of these discounts and special offers might very well be legitimate, email scammers take advantage of this surge to send out their own viruses and malware, hoping it might get lost in the mix. These scams have evolved over time, to the point that they are depicted as a legitimate discount or special offer. Be wary when opening an email from someone you don't know or a site you have not visited.
7. Make sure your passwords are complex.	Updating and enhancing your passwords is a cybersecurity best practice as old as time itself, and creating unique passwords is arguably still the best security when it comes to protecting your personal and financial information. If you utilize the same password for multiple sites, you are setting yourself up for disaster. If you have difficulty creating a large number of unique passwords for all of your information, be sure to take advantage of password generators and managers to not only develop more complex passwords, but allow you to store them securely as well.
8. Understand your shopping applications.	Apps have a way of making everything more convenient for your shopping experience, but certain apps could also make it convenient for criminals to take your information. Make sure you are only installing and utilizing trusted applications from reliable cyber markets, such as the Apple App Store or Google Play Store. Additionally, if you find yourself questioning certain applications, be sure to check out the reviews by legitimate user accounts, as this can help you identify if there is anything suspicious surrounding them.
9. Never save your information.	Never save usernames, passwords, or credit card information in your browser, and periodically clear your offline content, cookies, and history. Always utilize strong passwords and consider setting up Multi-factor Authentication (MFA). This is as simple as receiving a text or code that you need to type in while signing on to a system. Oftentimes within the account preferences of your device, you can set up an Authentication Application. Additionally, when online shopping, consider checking out as a guest user rather than creating an account, as well as utilizing your private browsing feature. For instance, Google Chrome's Incognito Mode won't save any of your browsing history, cookies, site data, or information you enter on forms. While the convenience of online shopping is unparalleled, never let this convenience override your security best practices.

10. Keep an eye on your credit.

As cyber-safe and secure as you think you might be, we all make mistakes. During this time, pay close attention to your credit report to ensure that nothing out of the ordinary is taking place. The world of online shopping can bring lots of new products to your doorstep and can prove to be a lot of fun when finding that special gift. Just remember to be careful so you don't make your data a special gift to cybercriminals. Always trust your instincts and make sure you stick to these cybersecurity best practices! ~ Happy Holidays and safe shopping!





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.