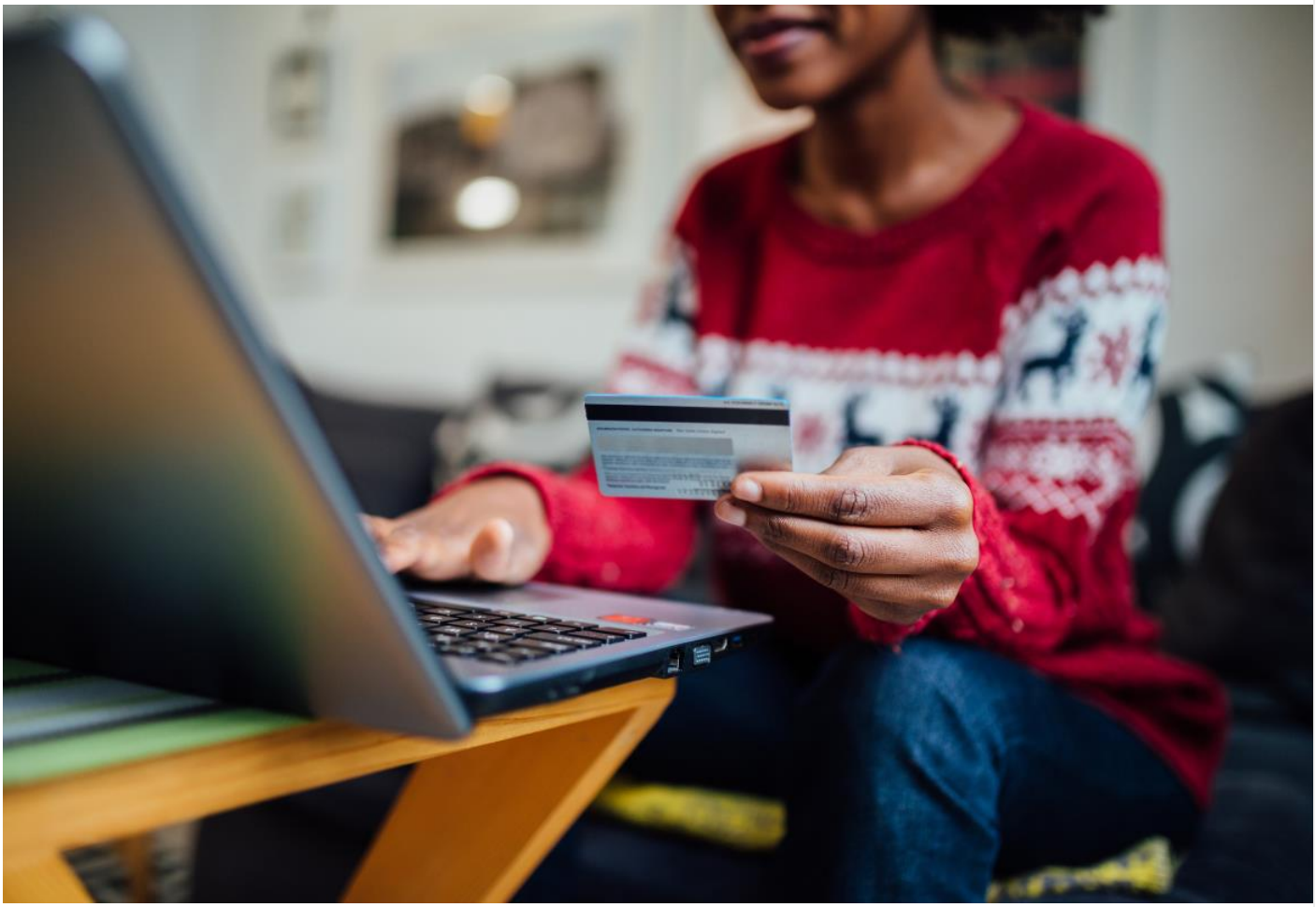
https://www.cmitsolutions.com/edison-piscataway

CMIT Solutions®

QUICK TIPS

TUESDAY, NOVEMBER 22, 2022



9 Tips for Safe Online Shopping

The holiday shopping season is nearly upon us. **Millions of Americans will flood retail stores and e-commerce sites over the next few weeks in search of the perfect gift.**

As the ease of online shopping has increased, that convenience has become a double-edged sword. It allows consumers to shop when and where they want—but it **also gives cybercriminals a chance to take advantage of unsuspecting shoppers.**

In most cases, bad actors are after home addresses, login credentials, credit card numbers, and other personal info. These online schemes can unfold in several ways.

Some hackers build illicit websites that look like common e-commerce portals and then try to lure users in with the promise of big savings. Some hackers send phishing messages with fake shipping notifications to capitalize on our desire to track incoming packages. And some hackers will try to intercept unsecured credit card transactions to steal account information.

Luckily, many scams are easy to spot—and easy to avoid. Consider adopting the same habits online that you do in person: keeping track of your valuables, stashing credit cards after you complete a purchase, and remaining alert to unusual behavior around you.

CMIT Solutions has compiled the following tips to stay safe this holiday season, blending common-sense advice with savvier strategies for online shopping:

1. **Only shop on reliable websites.** Does a sale sound too good to be true? Chances are it probably is. Don't get fooled by the promise of eye-popping discounts or aggressive ads that might lead to illicit websites set up by hackers. Only visit the websites of retailers you know and trust, and navigate to those sites only by typing a recognizable URL into your browser's address bar. Once that site loads, check the top left of the address bar to look for "https" or a gray lock symbol, which indicates a trusted level of security.

2. **Keep an eye out for season-specific scams.** These proliferate during the holiday shopping season, with fake package tracking emails, fake gift card offers, fake charity donation schemes, and other emails urgently requesting that you confirm purchase information. Never open attachments to emails that you aren't sure about, and as mentioned in the advice from the step above, type trusted URLs into your web browsers instead of just clicking on links.
3. **Protect your passwords.** If they aren't "long and strong," utilizing unique phrases, special characters, and a mixture of numbers and letters, strengthen them now. Never share your passwords with anyone (including friends and family) and implement multi-factor authentication (MFA), which requires a password and a unique code delivered via text or email, on every account you can.

4. **If possible, use a credit card instead of a debit card for online purchases.** Credit cards typically offer increased protection that can reduce liability if your information is stolen or improperly used. However, because debit cards immediately deduct a charge from your checking account, they usually do not have the same level of protection. To take this a step further, consider setting aside a dedicated credit card just for digital transactions. This can make limiting online exposure and quickly spot digital fraud even easier.
5. **Monitor your bank accounts and credit card statements regularly.** No matter what card you use for online purchases, this is the first place you should check for any potential hacks, breaches, or compromised credentials. If you notice a discrepancy, a duplicate charge, or an unfamiliar vendor, report it to your bank or credit card company immediately. In addition, consider setting extra alerts like text message notifications for transactions over a certain dollar amount or a daily summary of your current balance to look for further issues.
6. **Only use password-protected Wi-Fi connections.** Public Wi-Fi networks are a particularly unsafe option during the holiday shopping season when hackers will "squat" on open-source networks and try to steal any data they can. At home, ensure your wireless router is encrypted with WPA2 protection and named with a non-identifiable SSID. On the road, only use the personal hotspot on your cell phone to complete credit card transactions or online shopping purchases.
7. **Watch out for pop-ups.** These are a particular concern in free apps and on cluttered websites where an accidental click can lead you down a rabbit hole of Internet danger. Don't click on any links or ads that look suspicious. Don't respond to requests that ask you to install antivirus software or apps that can wipe your infected computer. And don't just click anywhere on an ad you want to close—sometimes the "X" to do so is hidden or counterintuitive and requires a little extra digging.
8. **Don't automatically save your passwords or credit card numbers.** We all like to save time when we're browsing and shopping. But the slight inconvenience of re-entering logins or account numbers far outweighs the time and effort that will be required if your password is stolen or your credit card is used by cybercriminals.
9. **Actually read the privacy policy before you sign up for a new**

> **account.** This might sound crazy. But in an age of rapid changes to popular social media accounts and nonstop location tracking, it's critical to know exactly what kind of information a merchant is collecting about you. Even more important is how that information will be stored, how it will be shared, and what recourse you have for opting out.

This holiday season, let's all stay safe, protect our private information, and remain vigilant to the threats posed by online shopping. Need help with any of the tips outlined above? Concerned about digital security or online shopping safety? Contact CMIT Solutions today.

And if you can, take some time to log off this week and disconnect while spending time with friends and family.

https://cmitsolutions.com/edison-piscataway **rbadge@cmitsolutions.com**