PROTECT YOUR DATA: 8 CYBERSECURITY TIPS FOR ONLINE SHOPPING

Online shopping is a common way for people around the world to get what they need delivered quickly to their door. In 2020, over two billion people shopped online[1] and e-retail sales surpassed $4.2 trillion worldwide.

With so many people shopping online, cybercriminals have no shortage of targets. Your personal and confidential information can quickly become a tool for their own financial gain. That's why it's important to learn cybersecurity tips to help you take the necessary precautions you need to keep your information safe and secure.

KNOW THE WARNING SIGNS

Online shopping can sometimes involve visiting multiple websites looking for the best deals. But doing this can increase the risk of stumbling upon unsafe sites. There are several warning signs to look for to decide whether a website is safe or not:

• The site looks unprofessional or poorly designed.

• Links are broken or disabled.

• No contact information is listed.

• Return or privacy policies are unclear or missing.

• Items are priced incredibly low.

• Credit card credentials are requested for additional reasons not related to your purchase.

• Shipping and extra charges seem unusual.

• The site has an excessive amount of negative reviews, or no reviews at all.

CYBERSECURITY TIPS TO PROTECT YOURSELF

Fortunately, there are methods you can use that can help keep you safe while shopping online. Learn more about cybersecurity with these 8 tips that you can put to use immediately:

1. Secure Your Devices
Ensure all your electronic devices, from phones to PCs, are virus- and malware-free and running on the most current software and apps.

2. Check the URL
Beware of clicking on links to deals that sound too good to be true. In some instances, hackers will attempt to redirect you to a new page without your knowledge. Always check that the URL in the navigation bar represents the site you intended to visit. When in doubt, type the URL directly into the address bar instead of clicking on a link. The same principles apply to mobile shopping apps. You should always download apps directly from the Apple App Store or Android market instead of a third-party site.

DeVry University

3. Skip the Debit Card

Using a credit card can be safer than a debit card, as more consumer protection is typically in place for credit cards. In addition, debit cards are directly linked to your bank account, putting you at higher risk for more severe damages.

4. Practice Password Safety

Your passwords for every online account must be unique and strong. It's also good practice to change your passwords every few months and use different ones for different sites. While allowing websites to remember your password may seem convenient, remember that it can also open the door to hackers if your device or the website is subject to a data breach.

5. Use Secure Wi-Fi

When making online purchases, always use secure Wi-Fi. Avoid using public networks to shop online or log into payment sites such as PayPal or your bank. If you must use public Wi-Fi, make sure you've logged out of your banking sites or any page where attackers can gain access to private information. Set your electronic devices to "ask" before they join any public networks.

6. Be Wary of Email Scams

Attackers may send fraudulent emails requesting you to confirm a purchase or account information, or use scare tactics, such as informing you your account has been breached. These links typically lead to a fake login page where attackers gain access to your account and password. If you're uncertain if an email is legitimate, the best approach is to type in the URL yourself and log in that way.

7. Check for Encryption

For added safety, check to make sure that the URL for a host, certificate or site uses encryption. Look for a closed padlock and a URL that starts with "HTTPS". Confirming that both of these elements are present helps ensure that your information will be safe and secure.

If the URL of the site starts with "HTTPS," it means it's secured using a TLS/SSL certificate. This certificate secures your data as it moves from your browser to the site's server. To check the certificate, click on the padlock icon in the address bar and a dialog box will open with information about the certificate.

8. Practice Credit Card Safety

Protecting your credit card information while shopping online can help prevent credit card fraud. Here are a few helpful cybersecurity tips:

• Keep digital receipts from all online purchases.

• Always compare your receipts to your final credit card bill.

• If you see any suspicious activity, contact your credit card issuer immediately.

• Try to designate one credit card specifically for online purchases, instead of using multiple cards.

• Avoid saving your credit card information on individual retailer websites.

If you're interested in the topic of cybersecurity, you may also be interested to know that DeVry University offers degree specializations and certificate programs that cover this area of tech education.

THINKING ABOUT FURTHERING YOUR EDUCATION?

To learn more about relevant programs of study at DeVry University or its Keller Graduate School of Management, click here.

Through an education partnership in conjunction with DeVry University, you have access to education benefits in support of your professional and life goals. To learn about transferring qualifying credits, tuition rate savings and more, contact your benefits manager or HR department for more details.

DeVry University