Holiday Season Internet Safety Tips

Mark Burnette

While the holidays are fondly recognized as “the most wonderful time of the year,” they’re quickly becoming known for another reason: holiday hacking surges. As online shopping continues to rise, the holidays become prime hunting season for attackers.

Identity theft and financial fraud are always risks online, but never more so than when you’re shopping, because that’s when individuals are putting their personal and financial information out on the Internet in search of the best deal.

It’s a reasonable expectation (and a responsibility) that Internet companies implement safeguards and policies to protect business systems and the sensitive data they collect, but online shoppers should always be aware of the potential for data theft and infection by computer malware and, therefore, selective of where they do their online holiday shopping. Because even though online vendors may have taken steps to prevent cyber intruders, there are likely still opportunities for your computer or your data to be compromised.

Using an outdated web browser or an unpatched computer and clicking on a web page booby-trapped with a hidden virus can turn control of your computer over to an intruder, or give the intruder access to the information you’re submitting on the website. If either of these situations happened to you, it could easily turn your holiday cheer into a Blue Christmas.

Here are some tips to keep your holiday shopping a joyful occasion:

1. **Shop reputable online stores.** If you’ve never heard of the web site you’re shopping on, do some investigation before providing any of your private information to the site. An online deal that looks too good to be true is probably a scam – don’t fall for it! Using well-known companies that you do business with on a regular basis is the safest approach.
2. **Always ensure that a web site is using encryption** before submitting any sensitive information to a website. Information flowing across the Internet can be intercepted and read by others, unless it’s encrypted. The good news – your browser can do that automatically if the web site is configured for encryption. To determine if encryption is used on a site, look for the padlock icon or check the web site address and make sure that it says “https:” before the site address.
3. **Consider using a payment system such as PayPal.** If an online site will accept payment from a third-party payment system, such as PayPal or Apple Pay, that is the option you should choose. If the company you purchased from gets compromised, or if their website is hacked, your payment information will be safe because you used the

payment system instead of providing your credit card information to the site, and hackers won't have access to your sensitive data.

4. **Password selection is important.** Use strong passwords for online sites, and use a different password for each online site. With that strategy, if a website's password database is compromised, the hackers won't be able to use your password to log onto other online sites. Use password management software to keep up with the various passwords for each site, such as LastPass, !Password, or Dashlane.
5. **Use Multi-factor authentication**. Configure key online accounts for two-step verification, such as Apple, Google, PayPal, FaceBook, and Dropbox. Multi-factor authentication adds an extra layer of protection when your system is accessed remotely. Access is granted only after entering a correct username and password along with a second factor, such as a text message with a sequence of numbers sent to your cell phone. Even if the attacker guesses or hacks your password, he/she won't have your cell phone, and therefore won't receive the code needed to log in.
6. **Keep your systems patched to close off common holes.** Ensure that your operating system, Internet browser, and other "plug-in" software such as Java and Adobe Reader have the latest updates and security patches. All of today's common operating systems can be configured to update automatically. Turn on automatic updates whenever possible, so you don't forget to patch it.
7. **Watch for cyber scammers sending phishing emails.** Be wary of clicking on links to shopping sites or "hot deals" that arrive via e-mail because they may take you to a hacker's fake site rather than the real shopping site. If you get an e-mail offering a special deal, don't click the links in the email – instead, open your web browser and type the site's web address directly into the address bar. If the deal is legit, it will likely be right on the front page of the site.
8. **Don't shop from free Wifi services.** The free wireless network in your favorite deli, coffee shop, or store is a prime target for attackers, and the bad guys may have tools already in place to try to capture your information when you connect. If you must connect to a free wifi network, never conduct business or send any sensitive information while connected to the free network. Save your online shopping for networks you trust!
9. **Keep a record of your online transactions** and review your credit card statement for unauthorized charges. Dispute charges promptly so they can be investigated, and your card replaced if your card number has been compromised.
10. And, if something bad does happen to you, be aware of the **protections your credit card offers** in the case of fraud.

There are great deals to be had via online shopping this holiday season. Be mindful of the tips above and vigilant with e-mails you receive, and your online shopping can be jolly. Here's hoping you're able t

o snag the deals you’re after – safely.