6 Tips for Safer Online Shopping

Devolutions

FORTUNATELY, WE AREN'T DEFENSELESS!

The holidays are here, which means it's the ideal time to spend time with friends and loved ones, eat way too much food, and of course: shop online in search of great deals.

Sadly, however, we aren't the only ones who look forward to the holidays. Hackers are gearing up to hijack accounts, deploy malware, and steal confidential data — including payment card and bank account information. Fortunately, we aren't defensless! Here are 6 tips for safer online shopping this holiday season, and throughout the year:

1. Be Careful When Clicking Email Links

You probably already avoid emails from people you don't know. But hackers love "spear phishing" campaigns, which is when **they send emails that appear to be from people you know and trust** — like a family member, friend or colleague. Usually these emails are short, simple and seem harmless (something like "Hey Derick, I came across this great article and thought you'd like it".) But if you click the link in the email, it opens the door for malware, viruses and other threats to your computer or device — which can then possibly spread to your network at work.

The moral to this story? Never click a link unless you're 100% sure that it's legitimate. Better safe than sorry!

2. Use Secure Wi-Fi

As we highlighted in a previous article, in the IT world sometimes "faster and easier" can go against basic security practices. Unfortunately, free Wi-Fi at a coffee shop, store or anywhere else can qualify for this warning. That's because some **hackers set-up fake Wi-Fi networks** that look like the real thing, in order **to steal login credentials and other private data**.

If you can't access the net through a personal and secure mobile data connection hotspot (because doing so might be really expensive!), the next best option is to **confirm the name of the network with a staff member**. And even if you're 100% sure that the network is legitimate, never transmit anything sensitive or confidential (like online banking information). **It's also a good idea to use a VPN**. Here's a review of some popular options.

3. Only Shop on Secure Websites

Whatever you shop for — like a 4K TV, or maybe some of these cool high-tech gadgets — **make sure that the website is secure, by checking to see that the URL starts with HTTPS and not HTTP**. This confirms that any data you send and receive is encrypted.

4. Keep Your Browser Updated

Always keep your browser updated. Yes, I know it's a hassle sometimes when you're busy, and it's tempting to delay it until next time (and then the time after that...and the time after that!). But trust me: it's worth taking a minute to **get the latest patches and fixes**.

5. Don't Save Your Credit Card Information

Some websites invite you to save your credit card information, so that ordering next time is faster. But with so many data breaches around the world, spending an extra 30 seconds to input your card information each time you buy something is **a small price to pay for additional safety**. You never know which website is going to get hacked next, and you don't want to be among the victims.

6. Use Strong Passwords

A long and strong password with upper and lower case letters, numbers, and special characters is essential. Also **make sure that you use different passwords, and never share them** with anyone. It's also a good idea to **use a password manager to store and organize your credentials**. To help you choose the right one, we've reviewed some of the most popular options. You're also invited to try Devolutions Server, which features a built-in password manager (including a strong password generator). You can also combine it Devolutions Web Login to automatically log in to trusted websites.

What Are Your Tips?

In addition to the above, what advice do you have for safe online shopping? Please share your knowledge below. Your advice could help many people have a happy holiday this year and avoid getting victimized by hackers and having a blue Christmas.