M

How to stay safe while shopping online

by Lucia Danes - - 2017-09-26

Shopping online has become as normal as going to a local store to buy some milk – everyone is doing it in one way or another. It is very convenient to simply sit at home and browse the Internet for nice clothes, books, jewelry, or even food. However, this convenience has a few downsides, and they are not limited to a wrong dress size. Exposing your details to a wrong vendor can cause you significant monetary damage or even result in an identity theft.

Here are some steps you should take to stay away from people with malicious intentions while shopping online.

- **Install a reliable security tool**

It should be obvious without saying that you must possess a good anti-malware program on your computer if you want to avoid the biggest online dangers. A reputable security application will help you avoid dangerous pages and phishing cases.

Remember to update your antivirus tool regularly so that it could protect you from the latest malware, especially zero-day viruses. The best option is to let the security tool update automatically. In this way, you will know that you are protected at all times.

- **Keep your computer and software up-to-date**

This is important – do not ignore the updates of your OS. These can contain some very important security upgrades that will increase your security level dramatically. Don't forget to also update your browser – the newer the version, the fewer vulnerabilities it has.

- **Buy only from reputable sources**

One of the best ways to protect yourself is buying only from reputable sources. This includes the biggest online shops that have a lot of users and are trusted worldwide.

Of course, you can give a chance to smaller retailers, but be very careful about exposing your details to them. Pay attention to the website – does it look trustworthy to you? If you see even the smallest hint that it might be unreliable, don't use it.

Sometimes scammers provide seemingly good deals on their fake pages. For example, you may see a phone or tablet that is twice as cheap as it should be. Don't fall into the scammers' trap by believing something that seems too good to be true.

- **Avoid public Wi-Fi**

Never perform any monetary transactions or provide any personal details online when you are using public Wi-Fi. Usually, it is not encrypted, so any information you are sending can easily get snatched by hackers. It is advisable to use public Wi-Fi for simple browsing only. If you need to shop online, do it with an encrypted connection.

- **Use complicated passwords**

The passwords you use for online shopping (this includes banking) should differ from the ones you use for your regular accounts. Actually, it should go without saying that you mustn't use the same password twice. The best thing to do is changing the passwords regularly. In this way, it becomes extremely difficult to hack them.

- **Find out if the website is securely encrypted**

When you choose your items and go to the payment section, take a closer look at the page URL. Even though it might seem confusing at first, you simply need to know one letter combination – HTTPS. Be sure not to confuse it with HTTP. You see, HTTPS is encrypted by using SSL (secure sockets layer).

The site is also secure if you see a green padlock in the URL section. Avoid providing sensitive information on pages that are not secure.

- **Read the seller's privacy policy**

Even though it might seem like a lot, it is advisable to read the privacy policy of the page that you are buying from. In this way, you will see how the website is going to use the information provided by you. For example, whether any of your details will be shared with third parties.

- **Be careful with the emails you get**

Nowadays, you can encounter a lot of phishing scams that use email. You can easily receive a letter that looks legitimate from the first glance – for example, it might seem to have come from Amazon.

However, hackers use this trust to spread ransomware or collect money. If you get an email from a seller, don't blindly click on links but type them into your URL bar instead. In this way, it will be impossible to deceive you with a malicious link in disguise.

Another important thing is not opening email attachments, especially those that are in PDF format. They can contain ransomware that encrypts your files and demands a ransom for decryption.

- **Use two-factor authentication**

It is advisable to use two-factor authentication if the website provides such an opportunity. It is available on Amazon and other bigger websites. This way is much more secure because, for example, you receive a unique code into your smartphone that you have to provide in order to complete a transaction.

Keep all of these steps for secure online shopping in mind, and you will likely avoid scammers and loss of private information