LegnanoNews
Le news di Legnano e dell'Alto Milanese

Shopping online: what personal data you're leaking

divisionebusiness · Monday, December 7th, 2020

With the holidays fast approaching, individuals are gazing at the screens of their computers and smartphones, shopping for the perfect gifts for their friends and loved ones. Little do they know that some of them are about to become victims of cyber crime.

And with much of the population avoiding shopping in retail locations because of shelter-in-place orders to stem the spread of COVID-19 infections brought on by the new coronavirus, online shopping only continues to increase.

Those who are worried about protecting their personal data will often ask, what is VPN software, and why is it a good idea to use a virtual private network?

A VPN is a way to prevent eavesdroppers from watching your communications online. This includes terms you type into search engines and the private email messages you send to your closest friends.

People will rely on a VPN so they can feel safer while shopping online, posting a resume to a company or when logging into a bank or their doctor's internet-based patient healthcare dashboard.

As you consider all of the shopping you've been doing lately online for food and other household necessities as well as the gifts you intend to buy for the holidays, it's prudent to be aware of what personal data you're leaking.

A lot of money could be at stake. RetailMeNot projected individuals would spend $803 on average for Black Friday and Cyber Monday sales for 2018, according to NBC News.

The broadcaster also noted that 75% of retailers in the United States had reported experiencing a data breach in 2017, an increase from 52% the previous year. With such alarming statistics trending upward, it underscores the importance of consumers taking steps to protect themselves before shopping over the internet.

Online Shopping: Scope of the Threat

You might think your smartphone is safe and secure, but chances are that it carries apps that are revealing personal information without you realizing it.

As much as 82% of apps for physical stores and 92% of apps for stores doing business exclusively

online are leaking people's personal information, according to a report in Money citing a recent NowSecure survey.

What Does "Leaking Data" Mean?

Personal information about you that no one has any business looking at, other than the retailer you're buying items from, is said to be leaking when a hacker can view and copy it.

Some criminals specialize in finding, guessing or stealing account credentials. Other hackers, with less skills in breaking into consumer accounts, will buy a list of hacked passwords on the dark web and use this information to go on crime sprees.

A major scandal involved the company Instacart, which matches customers with shoppers who buy things for them and then deliver to their door. According to BuzzFeed News, which validated the data was being sold online, individuals were offering 278,531 Instacart accounts.

Instacart denied there was a data breach, while a cybersecurity expert named Nick Espinosa from Security Fanatics confirmed to BuzzFeed that the stolen accounts appeared to be genuine.

The kind of data being stored for shoppers included their names, histories of orders and the last four digits of their credit card numbers. Hackers take private information from multiple sources to help them break into the victims' accounts.

Tips for Protecting Your Data While Shopping

You're not going to completely stop shopping online out of fear of hackers getting into your accounts. By practicing good internet security and using some common sense, you can protect yourself and avoid becoming another victim of cybercrime.

When it comes to payment, it's better to use a credit card while shopping online. If you use a debit card and a hacker gets the details to make a fraudulent purchase, he or she will have direct access to your funds and it can be a chore to get your bank to reverse the charges.

But it's much easier to dispute criminal credit card charges and to have the company remove them from your balance.

Instead of using a company's app, which may not be very secure, try using your preferred web browser on your smartphone, to access the company's website. You also get the benefit of freeing up space on your smartphone when you delete store apps.

To protect your funds, set aside a credit card with the lowest limit when shopping online for the holidays. That way, if criminals do manage to steal the card details, they won't be able to make off with much. And you still will report the theft to the card issuer, eventually they can reduce the charges.

Waiting for the fraudulent charges to be knocked off, you won't have access to funds, so don't shop for holiday gifts using a credit card that's used for critical, automatic recurring payments. These would include such your internet and phone service and health and car insurance premiums.

Shopping Safer

Focusing on websites that have a padlock icon displayed next to the URL box in your web browser is a good way to protect your personal data and keep it from leaking. This is the case for your desktop computer as well as your smartphone.

You'll also want to make sure that the browser software itself is the latest available version, in case the developer found and plugged up some security holes. Firewall software installed on your computer is another tool for maintaining online security.

Once you realize that hackers consider personal data valuable because it makes their crime sprees more convenient, it should motivate you to become a more careful online shopper.

Remember that double-checking the websites you visit are marked with a padlock symbol is always prudent. Substituting credit cards for debit cards gives you an added measure of protection. And exercising common sense, such as not venturing online via a public Wi-Fi network will go a long way toward keeping your sensitive personal data safe and secure.