TOTAL TECHNOLOGY SOLUTIONS

NEWSLETTER

DECEMBER 2020 EDITION

9 CYBERSECURITY SHOPPING TIPS FOR THE HOLIDAY SEASON

#1: Do not use public Wi-Fi for any shopping activity

Public Wi-Fi networks can be very dangerous, especially during the holiday season. While they are very convenient, they are not secure, and can potentially grant hackers access to your usernames, passwords, texts, and emails.

2: Make sure the site is secure

Before entering your personal or financial information, you need to ensure that the site you are on is legitimate and can be trusted. When visiting a website look for the "lock" symbol; this might appear in the URL bar, or elsewhere in your browser. Additionally, check that the URL for the website has "HTTPS" in the beginning.

#3: Make sure your passwords are complex

Updating and enhancing your passwords is a cybersecurity best practice as old as time itself, and creating unique passwords is arguably still the best security when it comes to protecting your personal and financial information. If you utilize the same password for multiple sites, you are setting yourself up for disaster.

CONTINUED ON PAGE 2

9 CYBERSECURITY SHOPPING TIPS FOR THE HOLIDAY SEASON

CONTINUED FROM PAGE 1

#4: Give your debit card a holiday break

Credit cards offer more protection and less liability if your information were to be compromised. On the contrary, debit cards are linked directly to your bank account, thus, you're at a much greater risk if a criminal were to obtain this information. Additionally, in the event of a fraudulent transaction were to occur, credit card companies possess the ability to reverse the charge.

#5: Stay updated

Updating your operating system and software (including anti-virus software) is one of the most important and easiest things you can do to prevent criminals from accessing your information, and needs to be taken very seriously. Most software updates are released to improve your security by patching vulnerabilities and preventing new exploitation attempts by criminal hackers. If you see that your device needs to be updated, do it!

#6: Understand your shopping applications

Apps have a way of making everything more convenient for your shopping experience, but certain apps could also make it convenient for criminals to take your information. Make sure you are only installing and utilizing trusted applications from reliable cyber markets, such as the Apple App Store or Google Play Store. Additionally, if you find yourself questioning certain applications, be sure to check out the reviews.

#7: Outsmart the scammers

During the holiday season we often see an influx of emails with discounts. While many of these discounts and special offers might very well be legitimate, email scammers take advantage of this surge to send out their own viruses and malware, hoping it might get lost in the mix. These scams have evolved over time, and may appear legitimate. Be wary when opening an email from someone you don't know or a site you have not visited.

#8: Never save your information

Never save usernames, passwords, or credit card information in your browser, and periodically clear your offline content, cookies, and history. Always utilize strong passwords and set up Multi-factor Authentication (MFA). This is as simple as receiving a text or code that you need to type in while signing on to a system.

#9: Keep an eye on your credit

As cyber-safe and secure as you think you might be, we all make mistakes. During this time, pay close attention to your credit report to ensure that nothing out of the ordinary is taking place. The world of online shopping can bring lots of new products to your doorstep and can prove to be a lot of fun when finding that special gift. Just remember to be careful so you don't make your data a special gift to cybercriminals.