25 STEPS TO SAFE ONLINE SHOPPING

There exists a tremendous difference between what computer users should do to enhance their cyber security and what they really do. What is the primary reason for this? People are ignorant of the dangers that are present out there and neglect all the warning signs.

Each year, nine million people in the USA fall victims to identity theft. Their private data can be used to open bank accounts, get loans, rent cars, hackers can simply still money from credit card accounts. The price of not protecting your online posture is tremendous.

Cyber criminals are regularly improving their methods and thus raising the likelihood for you to fall their prey. With the Holiday shopping time at its top, I have prepared a detailed guide to help you shop safely.

REPUTATION AND RECOMMENDATIONS

Shop primarily from recognized and trustworthy web-stores. Select shops that are in business for at least one year. This approach does not provide you a 100% security against scams and frauds because legitimate web shops are likewise susceptible to cyber-attacks. However, they are going to pay attention to their customers' safety and spend more on securing your sensitive data. If you need to buy an item from a store you have not ordered from before, perform a little research first. Inquire around, maybe some of your friends or co-workers have previously tried their services. Try to find reviews in social media and forums.

CONTACT DETAILS

Do not purchase anything from sites that do not give detailed info about their company. Check out what is put in the Footer. Look at their Contact and About pages. Does it have the full business name? Can you see a detailed street address and contact person information? Do they have a local phone number or 1-800 number? One more bad indicator is a free webmail address like Yahoo or Gmail. It demonstrates the webstore staff members are incompetent and unprofessional. In case you discovered a page with just a contact form, that is a red flag.

TERMS OF SERVICE

Invest some time to study the Terms and Conditions, Privacy and Return Policies. Be well informed and understand your rights. Watch out for additional fees and charges. Find if they provide shipping insurance and what is the refund policy in the event your parcel is lost or spoiled. Pay attention to mistakes or discrepancies - does the site state one thing on a webpage that conflicts with their own policy?

RED FLAGS

Do not order anything when you notice these red flags: misspellings, poor grammar, low resolution or bad quality photos, copied or stock photos.

5

QUALITY SEALS

Check if they have trust and quality seals. These prove that the site has gone through an independent assessment and review procedure and satisfied all the quality criteria of the organization that grants the seal. Quality seals were introduced with the goal to raise online shoppers' confidence, but you need to know that some dishonest webstore owners may put fake seals that were not issued to them.

SSL

Prior to deciding to submit any personal information or credit card data, be sure that you are on a safe connection. Take a look at the address bar. Does the web address begin with HTTPS or HTTP? That additional S means the online store has a legitimate Secure Sockets Layer set up, briefly SSL. It is a way to guarantee the transmitted computer data is encrypted and cannot be intercepted by the third parties.

6

7

PHISHING

Avoid phishing tricks. These are techniques to deceive you into reveling secret info needed to access bank accounts or steal identities. E-commerce phishing operates by means of fake email messages that impersonate a reliable company or organization, for example, PayPal, Amazon or your bank. Criminals attempt to trick you into providing your SSN, passwords, CC data. This occurs if you reply to the email, click a link on a phishing website and fill in the web form. Cyber crooks often take advantage of your feelings or need. They may offer better deals or inform you that there is a problem with your account. A phishing link may open a malicious website that looks like the real one and requests you to type in private data.

URLs

Look out for phony and misleading links. Simply clicking on a web link can get your PC into trouble. Examine links, hover the mouse over them. Sometimes links might seem matching, however, hackers utilize a spelling deviation or another type of top domain *.org* instead of *.net*. Be mindful of URL shorteners and do not click on them carelessly. Hackers like to shorten their malevolent URLs with the help of popular services like Bit.ly. It is better to inspect URLs with the help of URLvoid.com or other free services.

8

9

DIRECT INPUT

Most secure method to visit a website is to take the trouble and type each letter into the address bar.

UNNECESSARY INFO

Use caution with what private data the web store is asking from you. They do not need your SSN or birthday.

10

11

DEDICATED EMAIL

Create a separate email account specifically for online shopping. By doing this, you are going to minimize the probability of potential spam and phishing emails to your primary email address.

CREDIT CARDS

While buying on the Internet, use your credit card to pay for goods and refrain from paying with debit cards. Credit cards possess integrated safety mechanisms that defend you from any type of scam, overcharging, theft, unauthorized transactions. Credit cards also give you a time interval to analyze bank statements.
It is advised that you utilize a dedicated card specifically for online shopping.

12

13

TRANSACTIONS

Set up two-steps approval process for all your payments by adding your smartphone number. It is better to use security tokens rather than SMS. Enable SMS notifications for all CC operations.

WEB FORMS

14

Do not store CC info with web shops for further usage. For your security, it is advisable to invest some time and fill them in each time you wish to make a purchase.

15

CREDIT REPORT

Freeze your credit report. It is not expensive and should make it hard for criminals to open new bank accounts in your name. You will need to remove it each time you ask for a loan, rent a home, etc.

BANK STATEMENTS

16

Get a habit of monitoring your accounts on a regular basis, desirably every day. Search for unidentified or suspicious records. If something is wrong or there is an unfamiliar purchase, immediately call your bank regardless of how tiny the amount is.

17

PASSWORDS

Use only strong passwords because they are the main reason for hacks and data breaches. Choose passwords that longer than twelve characters. Every additional character increases your security exponentially. The password should consist of both lowercase and uppercase letters, symbols, and numbers. Do not use the same password for several accounts. Think of it. You are not using the same key for your car, house, and office, correct? In case hackers manage to compromise one account of yours, it will allow them to login to all of them. Abstain from passwords which can be quickly guessed.
Change passwords regularly. Do not keep passwords inside a text file on your computer or webmail draft.

MULTI-FACTOR AUTHENTICATION

18

Turn on multi-factor authentication for your emails and other accounts where they are available. As a result, you will get a unique, one-time code on your phone that should be entered as an additional password. It builds an additional security layer that is a lot more problematic to overcome by an attacker.

19

RECOVERY QUESTIONS

Do not ignore the importance of your recovery questions. Pick recovery questions with answers only known to you and not guessable. Treat answers like your passwords.

HACKED?

20

In case one of your accounts with any online service got compromised, immediately modify the password used for it. If you used that password for other online accounts, change all of them too together with passwords for all email accounts linked to them.

21

PUBLIC HOTSPOTS

Do not hook up to open public hotspots or use public PCs. They could be very easily hacked, and your complete web session might be tracked together with your credit card information. When it is absolutely necessary to connect and only public Wi-Fi is available - use VPN, virtual private network. Still, do not log into your e-banking. e-mail or other major accounts.

UPDATES

22

Keep your software updated all the time. Do not disregard update notifications. Uninstall risky apps such as Flash Player, Acrobat Reader, Java and Quicktime as they are famous for many vulnerabilities.

23

ANTIVIRUS

Buy paid antivirus software from a solid company, compare antivirus tests results published by independent AV testing laboratories. Your antivirus should consist of the real-time scan, automatic updates, and firewall. Keep in mind that AV is just an additional tech layer that cannot protect from all threats, the best AV is in your head.

MOBILE

Apply all these security measures to mobile devices.

24

25

FAMILY

Educate your family members on how to apply the above-mentioned measures. Children should learn who to stay safe online as early as possible.