Key tips every computer and internet user should follow

October is known as Cybersecurity Awareness Month. Now in its seventeenth year, the campaign continues to raise awareness of the importance of cybersecurity, online privacy, and digital hygiene in general.

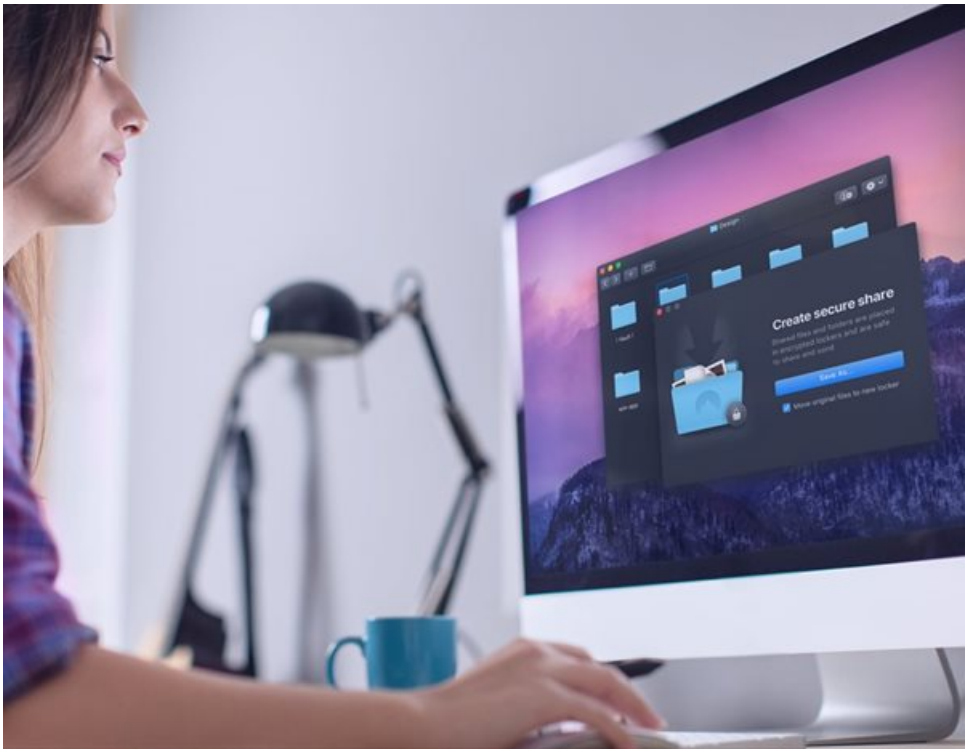

Image supplied

Did you know that approximately 6.85 million accounts get hacked every day? This is 158 accounts per second!

“Even though the statistics are shocking, every user can avoid the risk of becoming a target just by following the right cybersecurity practices,” explains Oliver Nobel, a data encryption specialist at NordLocker.

Repetition is the mother of learning, so it’s a good idea to go over the things you think you already know. The list below includes these 22 key tips every computer and internet user should follow to protect themselves from becoming a victim of cybercrime.

1. Use multi-factor authentication for an extra layer of security whenever possible.

2. Create complex and unique passwords for your online accounts. Start using a password manager to help you

generate strong passwords and store them in one safe place.

3. Stay away from unsafe public Wi-Fi and use your mobile data instead. If you really need to connect to a public network, always use a VPN. A virtual private network encrypts all communications passing between your device and the internet so no outsider can intercept your traffic.

4. Turn off the Wi-Fi on your device when you don't use it.

5. Back up your data to a portable hard disk or cloud-based storage so you can always recover your information if it ever got lost.

6. Disable Bluetooth when you don't use it.

7. Make sure your operating system is up to date both on your computer and smartphone.

8. Enable your firewall. Most operating systems have a built-in firewall, which keeps outsiders from going through the data you keep on your
computer.

9. Make sure your anti-virus is up to date.

10. Buy and download apps and software only from official stores.

11. Set your social media account to private. Before posting anything online, check who you're sharing the information with.

12. Turn off geotagging to prevent your photos from including location-disclosing metadata.

13. Don't over share online. Avoid posting your e-mail, phone number, or home address on blogs, forums, and social networks when it's unnecessary. Never share your emotions, intimate pictures, and vacation plans with strangers online.

14. Don't upload high resolution photos to social media platforms. Make sure to hide all the street names, building numbers, and any other information that can indicate your whereabouts.

15. Encrypt the sensitive files you store on your computer and in the cloud. There're easy-to-use file encryption tools that turn all your files and information into uncrackable codes that even skilled hackers can't read without your permission.

16. Shop only on secure websites. The address of a safe website should start with "https://" (often preceded by a padlock symbol), where the letter "s" stands for "secure."

17. Look for tell-tale signs of a fake e-shop to avoid scams: poor website design, broken English, shady contact information, unclear return policies, poor customer reviews, and so on.

18. Don't open emails from unknown senders, as those might be phishing attempts.

19. Don't download any attachments from suspicious emails.

20. Never click on scammy links. Always verify the sender and contents of the email before clicking on anything.

21. Don't use your work device for personal needs, and vice versa.

22. When browsing online, always protect your data and location. Use a VPN, which hides your IP address and creates a virtual tunnel for your data to safely travel across the web.