

# CYBER SECURITY: WHAT CAN YOU DO



01

Use complex passwords. You could use a sentence or passphrase that you love and omit the vowels. Update your passwords periodically.

02

Create airgaps between types of accounts. Use different levels of security for different applications. Set up more complex and secure password for applications related to your finances.

03

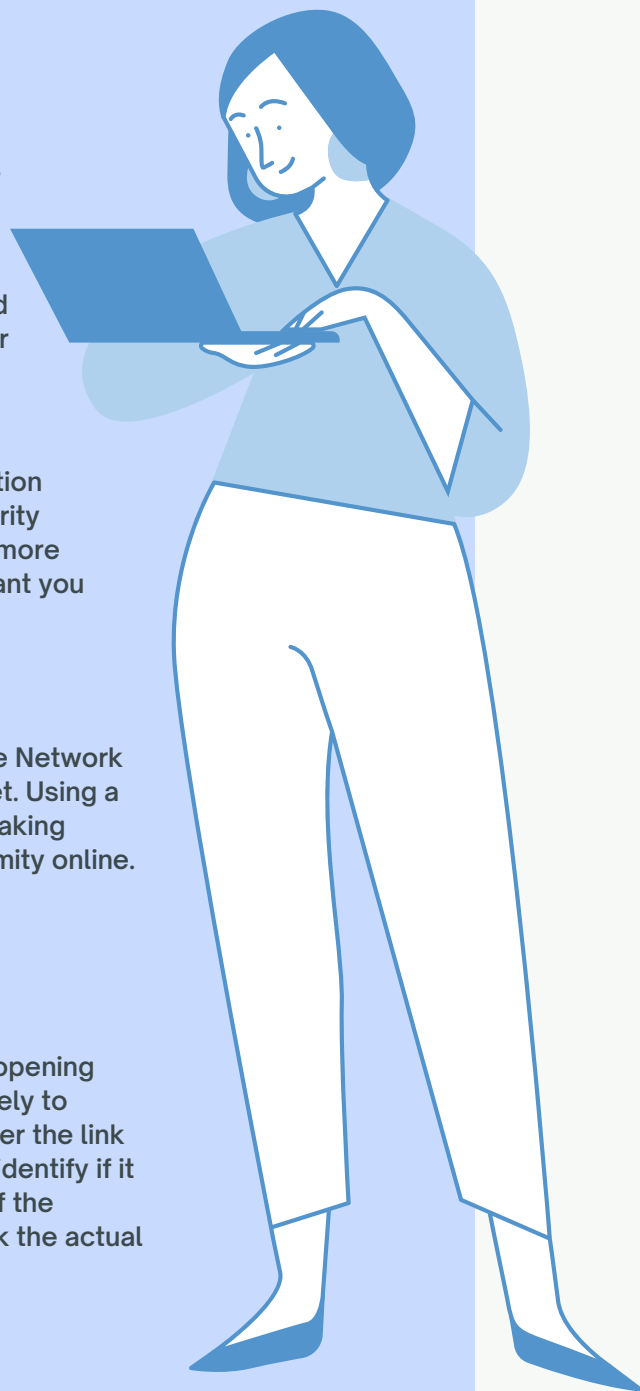
Utilise multi-factor authentication whenever you can. It is a security measure that requires two or more proofs of authentication to grant you access.

04

If you can, use a Virtual Private Network (VPN) when surfing the internet. Using a VPN masks your IP address making easier to maintain your anonymity online.

05

Think before you click. Avoid opening links when you're tired and likely to make an error. Try to hover over the link to see its real origin and help identify if it is fake. Don't trust the name of the sender of an email. Also check the actual email address.



# CYBER SECURITY: WHAT CAN YOU DO



06

Never put a USB or any other removable media/device from an unknown source into your computer.

07

To limit exposure to risks online, set up and use separate and limited credit cards for all your online purchases to protect main credit cards linked to your real savings.

08

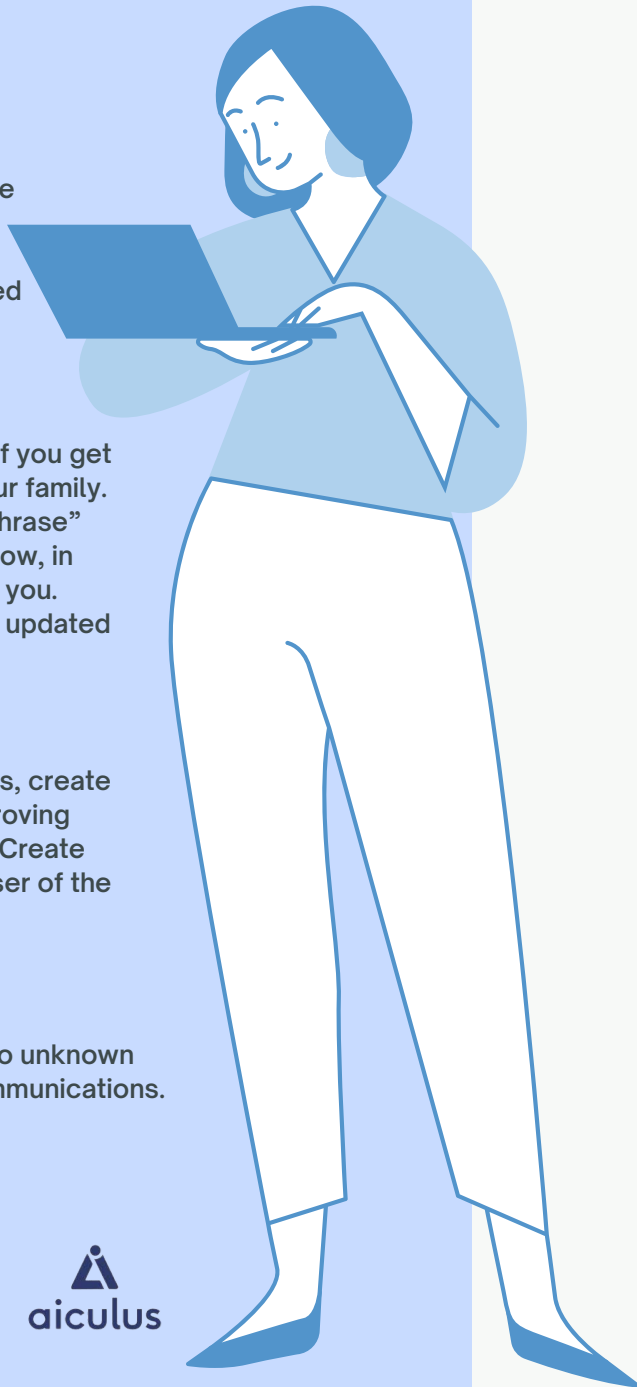
Develop a plan on what to do if you get hacked and share this with your family. Do you need to have a “passphrase” which only your close ones know, in case a scammer texts or calls you. Keep all your devices and app updated

09

For shared or family computers, create an Administrator login for approving new software or applications. Create separate accounts for each user of the computer.

10

Develop a zero trust attitude to unknown persons, applications and communications.



**STAY SAFE  
ONLINE.**

