10 TIPS

Protect your Identity from thieves

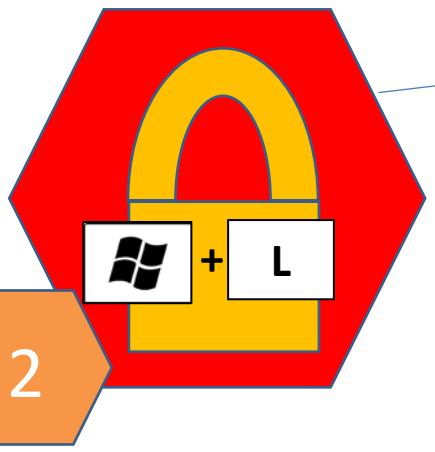
1 A BIG YES TO PASSPHRASES

81% of successful hacker attacks are the result of poor or stolen passwords

Increase your security instantly – with passPHRASES.

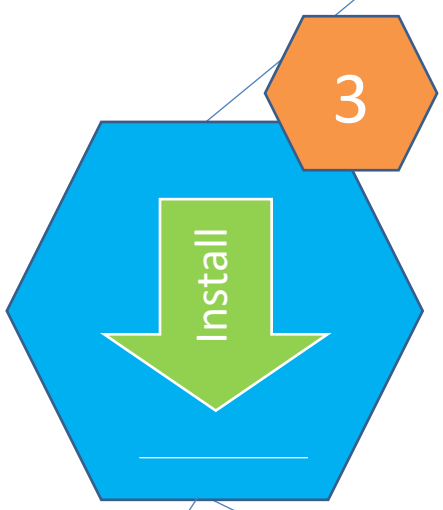
TIP: Use different offbeat sentences as your logins – for instance "I like … (plus two to four words)". These are strong and easy to remember.

Time to Crack passwords (with an i7 laptop)	
123456	1 second
Password1234	3 minutes
Amelia77	13 minutes
FancyTrees	2 Days
FancyTrees11	9 months
Ilikegreentrees	14 years
Ilikegreentreesonfridays	10000+centuries



2 LOCK IT OR LOSE IT

Leaving your device unlocked is akin to leaving your front door open. Like house theft, most cybercrimes are crimes of opportunity. Lock your device as soon as you stop using it. This is as simple as pressing Windows (+) L on a PC; CTRL, Shift (+) power on a mac, or usually the power button on a mobile.

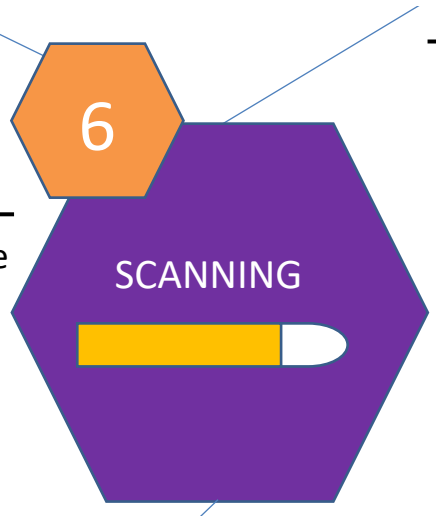


3 INSTALL THOSE UPDATES

Windows, OSx, IOS, Android, applications like MS Office and browsers like Chrome all release updates. These contain crucial security fixes to combat new threats - making your data safer!
TIP: Enable automatic updates. Also shut down or restart at least weekly.

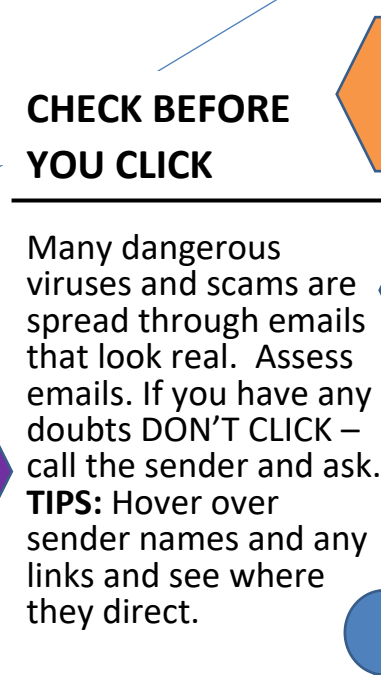
4 TWO FACTOR AUTHENTICATION

Bank accounts, secure access areas and more should be protected with 2 factor authentication – eg. a pin gets texted to your mobile.
TIP: Consider enabling a two factor password manager (like lastpass) and start to autofill and store your passphrases easily and SECURELY



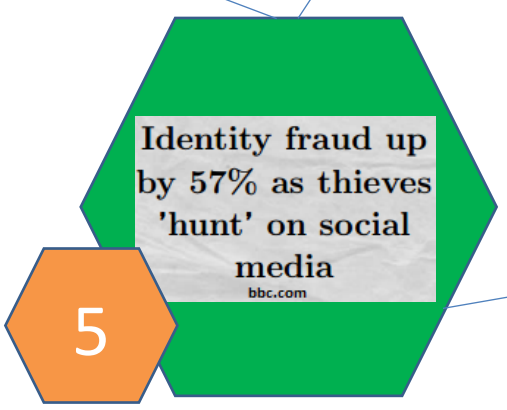
6 VIRUS SCAN EVERYTHING

Antivirus programs are designed to seek out and remove threats. such as malware, viruses and identity scams. **Tip:** Install antivirus and use it to scan websites, downloads, emails and anything you plug into your computer!



7 CHECK BEFORE YOU CLICK

Many dangerous viruses and scams are spread through emails that look real. Assess emails. If you have any doubts DON'T CLICK – call the sender and ask.
TIPS: Hover over sender names and any links and see where they direct.

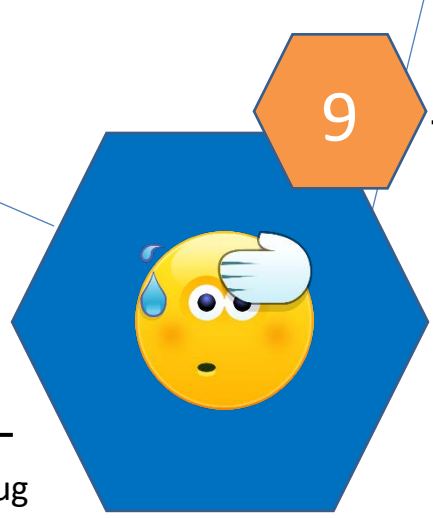


5 BE SOCIAL AND SAFE

Personal information is like money. Respect it. Protect it. Remember anything shared publicly can be seen and analysed by friends and foes alike.
TIPS: Use good passphrases, find and turn on privacy settings, hide DOB and set posts to share with "Friends" only.

8 SHOULD YOU PLUG THAT IN?

Anything with a USB plug can be infected. Never plugin unknown devices (hard drives, USB etc). **Did you know** public USB charging stations can also be a source of viruses? Don't use them, carry your own wall plug.



9 BACK UP BACK UP BACK UP

Accidents happen:
- I lost my phone
- I left my laptop in a taxi
- I got a virus and can't access my data

Backups save people all the time. Make sure you have an up to date back up plan, action it, and check it's working, just in case…

10 Be Suspicious

When in doubt, throw it out: Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious don't open or download it – talk to IT.

huonit

P 1300 HUON IT | **W** www.huonit.com.au
E info@huonit.com.au