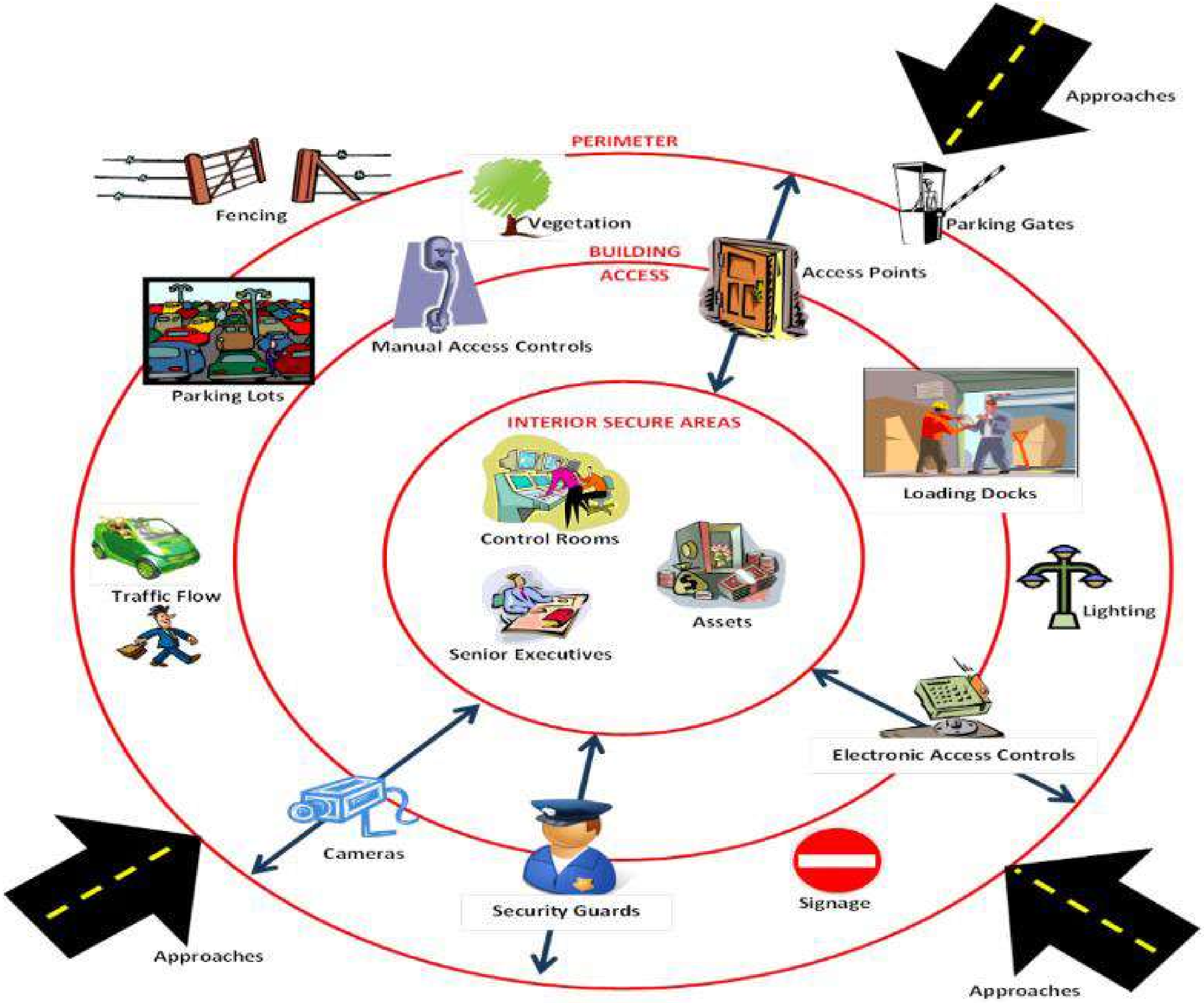
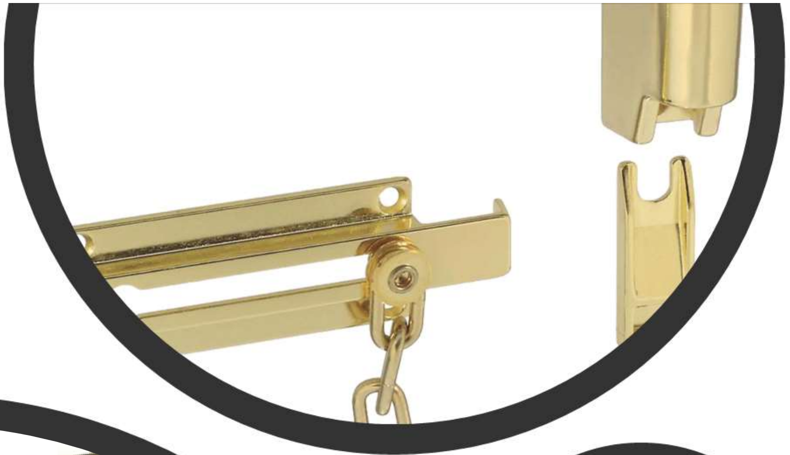
CYBER SECURITY

Deepal Kafle
Hornsby Shire Council

Physical Security



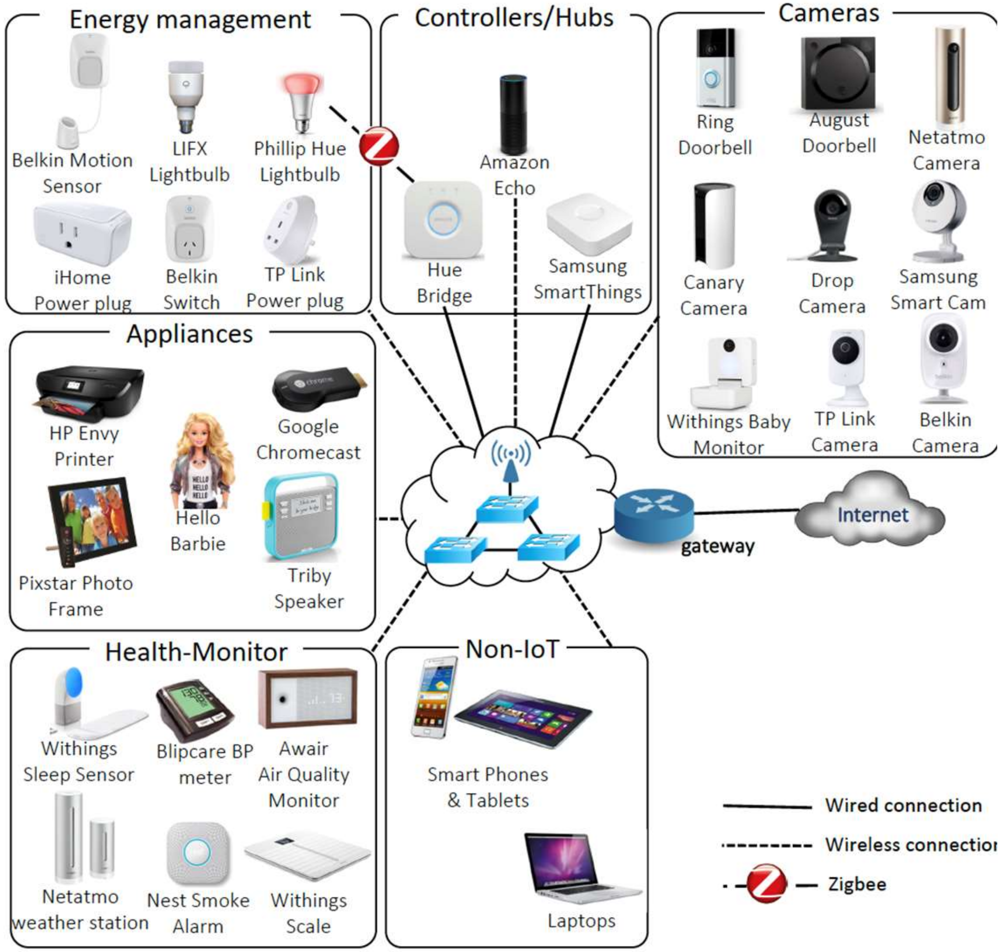


Home security

Smart Home & new ways of living

Smart Home & Challenges

- ❑ Cloud systems will have more open doors to our local network.
- ❑ Protect a computer network from intruders, including both wired and wireless (Wi-Fi) connections.
- ❑ Protect applications operating on-premises and in the cloud.
- ❑ Encrypting data for integrity.
- ❑ Privacy might be another concerning area, collecting potentially sensitive information such as when one is Home or on vacation.
- ❑ Financial damages.
- ❑ Disaster recovery plan.
- ❑ Threat actors might use IoT devices in a DDoS attack to take down a target

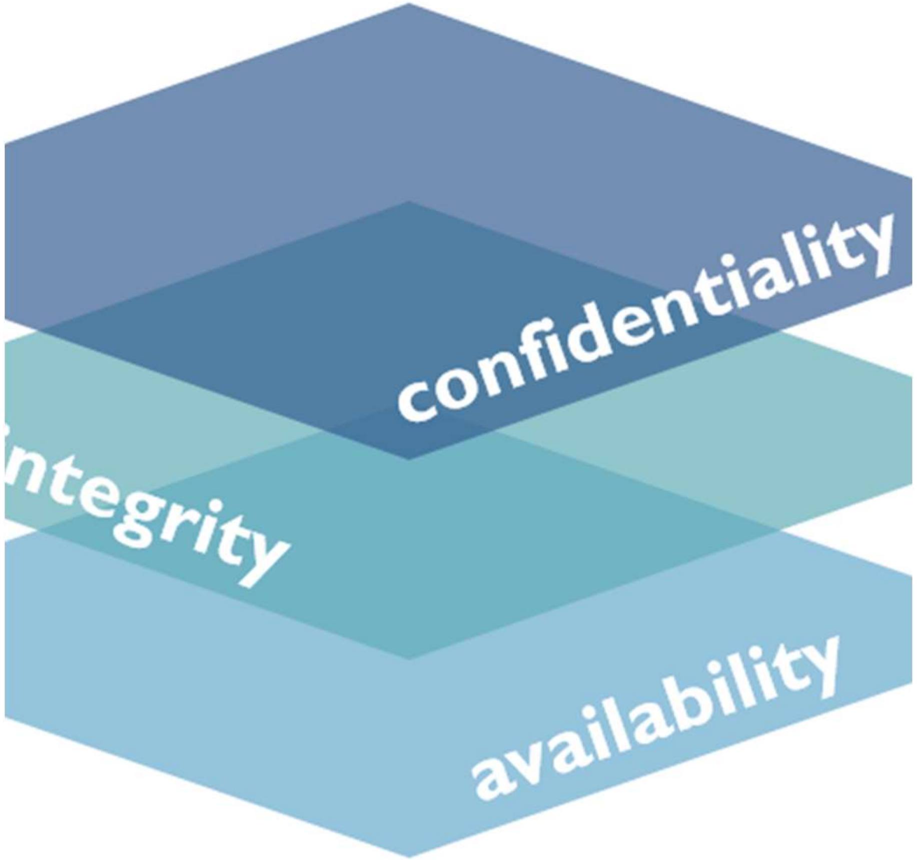


Cybersecurity and objectives

Cybersecurity is a practice of protecting electronic devices and associated data and information.

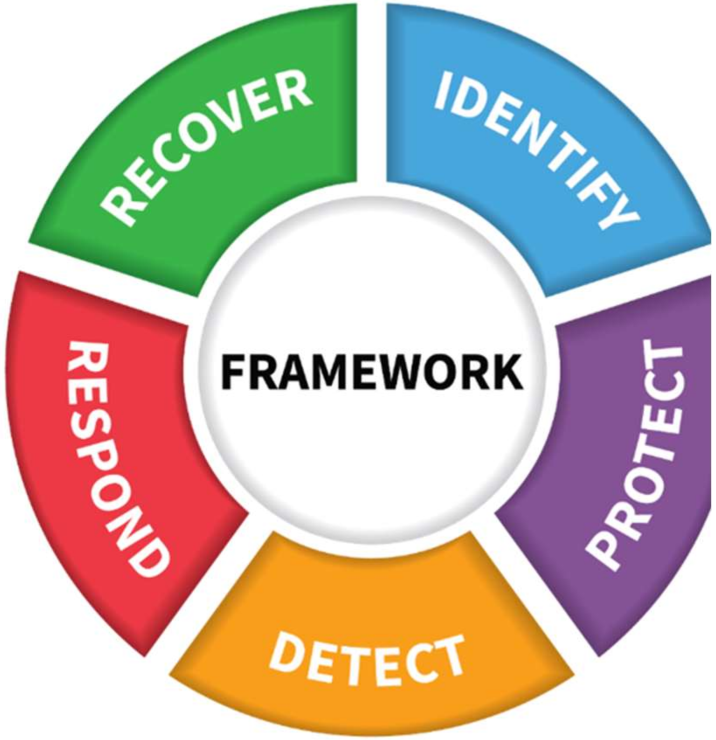
It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

- ❑ Cybersecurity objectives:
  - ✓ **Confidentiality**: Protecting information from unauthorised access and disclosure.
  - ✓ **Integrity**: Protecting information from unauthorised modification.
  - ✓ **Availability**: Preventing disruption in how information is accessed.



Personal experience

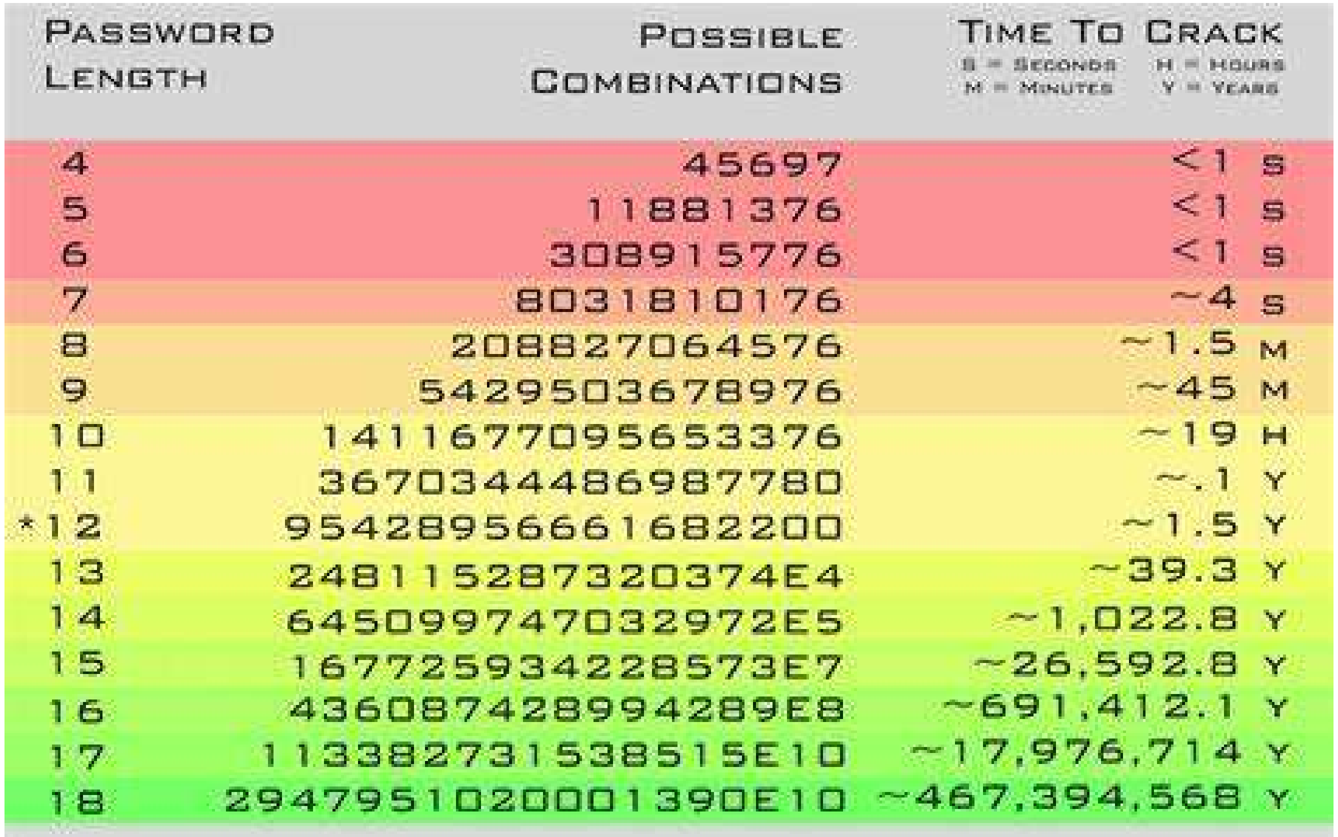
- ❑ My elder daughter’s apple account was hacked.
- ❑ Unattended i-messages were sent to my younger daughter’s friends, who happened to be our next-door neighbour.
- ❑ Action:
  - ✓ Informed affected parties.
  - ✓ Changed iCloud password and enable MFA.
  - ✓ Ensured backup was in place.
  - ✓ Monitored until we had a confidence with the solution.
- ❑ Affect/prevention:
  - ✓ Reputation damage.
  - ✓ Mental trauma.
- ❑ Lesson learnt:
  - ✓ Adopted no password reuse policy.
  - ✓ Started using Password Manager.



Cyber Aware and staying secure online

- ❑ Use a strong and separate password for your email.
  - ✓ Combine three random words to create a password that’s ‘long enough and strong enough’.
  - ✓ **Passkey** is an alternative to password.
- ❑ Install the latest software and app updates.
  - ✓ Set auto update where applicable.
- ❑ Be careful of email attachments, web links and voice calls from unknown numbers.
  - ✓ Do not click on a link or open an attachment that you were not expecting.
- ❑ Use separate personal and business computers, mobile devices and accounts.
- ❑ Use multi-factor (2-step verification) authentication where offered.
- ❑ Do not download software from an unknown web page.
- ❑ Never give out your username or password.
- ❑ Consider using a password management application to store your passwords.

Cyber Aware and staying secure online



PASSWORD LENGTH	POSSIBLE COMBINATIONS	TIME TO CRACK
		S = SECONDS H = HOURS
		M = MINUTES Y = YEARS

4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167095653376	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	2481152873203744E4	~39.3 Y
14	6450997470329722E5	~1,022.8 Y
15	1677259342285737E7	~26,592.8 Y
16	4360874289942898E8	~691,412.1 Y
17	1133827315385150E10	~17,976,714 Y
18	2947951020001390E10	~467,394,568 Y

Dealing with common cyber problems

GET THE BEST VIRUS PROTECTION
KEEP YOUR SOFTWARE UPDATED
USE STRONG PASSWORDS
REMEMBER TO LOG OFF
MANAGE YOUR SOCIAL MEDIA SETTINGS
DON'T SHARE PERSONAL INFORMATION
PROTECT AGAINST CYBER ATTACKS
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt.

❑ How do I recover my account, if it is hacked?

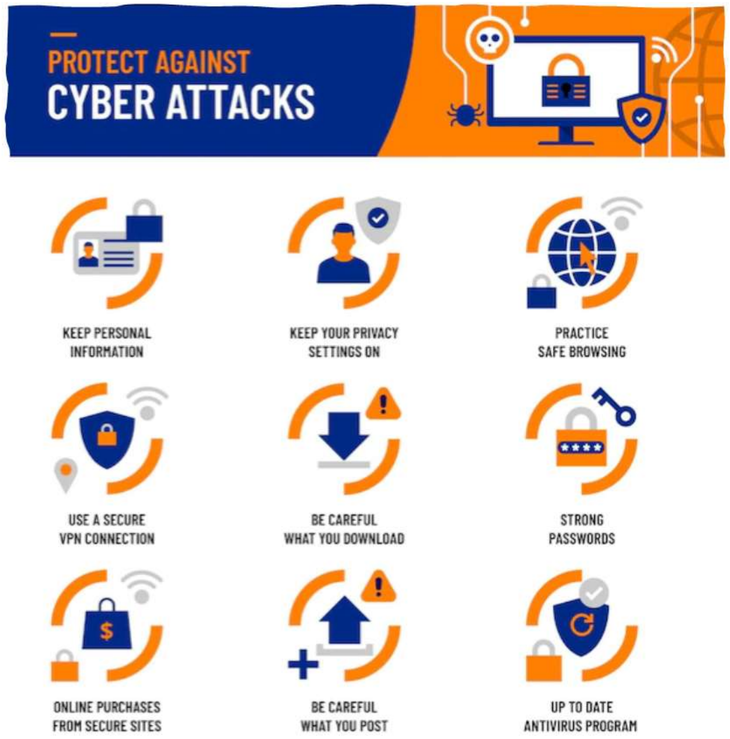
- ✓ Contact Account Provider.
- ✓ Check email account.
- ✓ Change Passwords.
- ✓ Log all devices and apps out of your account.
- ✓ Set up 2-SV.
- ✓ Update devices.
- ✓ Notify your contacts.
- ✓ Check bank statements and online shopping accounts.
- ✓ Contact Action Fraud.

If you cannot recover account and setup new account, share with your contacts and advise that old account should not be trusted.

Make sure to update any bank, utility or shopping websites with new details.

Services such as www.haveibeenpwned.com can tell you if your information has ever been made public in a major data breach, and even alert you if it happens in the future.

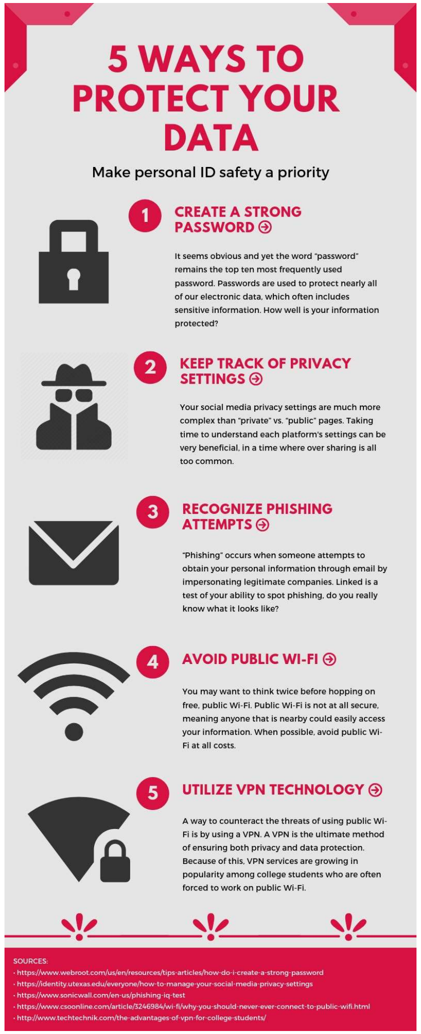
Dealing with common cyber problems


PROTECT AGAINST
CYBER ATTACKS
KEEP PERSONAL INFORMATION
KEEP YOUR PRIVACY SETTINGS ON
PRACTICE SAFE BROWSING
USE A SECURE VPN CONNECTION
BE CAREFUL WHAT YOU DOWNLOAD
STRONG PASSWORDS
ONLINE PURCHASES FROM SECURE SITES
BE CAREFUL WHAT YOU POST
UP TO DATE ANTIVIRUS PROGRAM

- ❑ Confirm your device is infected.
  - ✓ Run an antivirus scan.
  - ✓ Look for the signs of infection.
- ❑ Try and fix infection.
  - ✓ Phone/tablet may not be usually fixed by antivirus product in the same way as PCs and laptop. The safest solution is to do a **factory reset**.
  - ✓ Update devices and programs.
  - ✓ Restore backed-up data from the ‘last known’ good backup.
  - ✓ Get expert help.
- ❑ After fixing infection.
  - ✓ Keep device and programs/apps upto date.
  - ✓ Backup data.
  - ✓ Enable encryption in device.
  - ✓ Install antivirus and update regularly.

Protecting your data and devices

- ❑ Data Breaches
  - ✓ Be alert of suspicious messages.
- ❑ Buying and selling second-had devices.
  - ✓ Avoid buying phones that are no longer supported by the manufacturer.
  - ✓ Reset to ‘factory reset’.
- ❑ Smart security cameras and using them safely in Home.
  - ✓ Change default password. If possible, change default username too.
  - ✓ Disable remote access, if not required.
- ❑ Securing devices.
  - ✓ Avoid apps from unofficial sources.
- ❑ Shopping online securely.
  - ✓ Use only trusted address.
  - ✓ Consider using online payment platform, since the retailer won’t see payment details.
- ❑ Antivirus product.
- ❑ Social media and using it safely.
  - ✓ Manage the security and privacy settings on accounts, so that personal information remains inaccessible to anyone but you.
- ❑ Using smart devices safely in Home.



5 WAYS TO PROTECT YOUR DATA

Make personal ID safety a priority

1 CREATE A STRONG PASSWORD

It seems obvious and yet the word “password” remains the top ten most frequently used password. Passwords are used to protect nearly all of our electronic data, which often includes sensitive information. How well is your information protected?

2 KEEP TRACK OF PRIVACY SETTINGS

Your social media privacy settings are much more complex than “private” vs. “public” pages. Taking time to understand each platform's settings can be very beneficial, in a time where over sharing is all too common.

3 RECOGNIZE PHISHING ATTEMPTS

“Phishing” occurs when someone attempts to obtain your personal information through email by impersonating legitimate companies. Linked is a test of your ability to spot phishing, do you really know what it looks like?

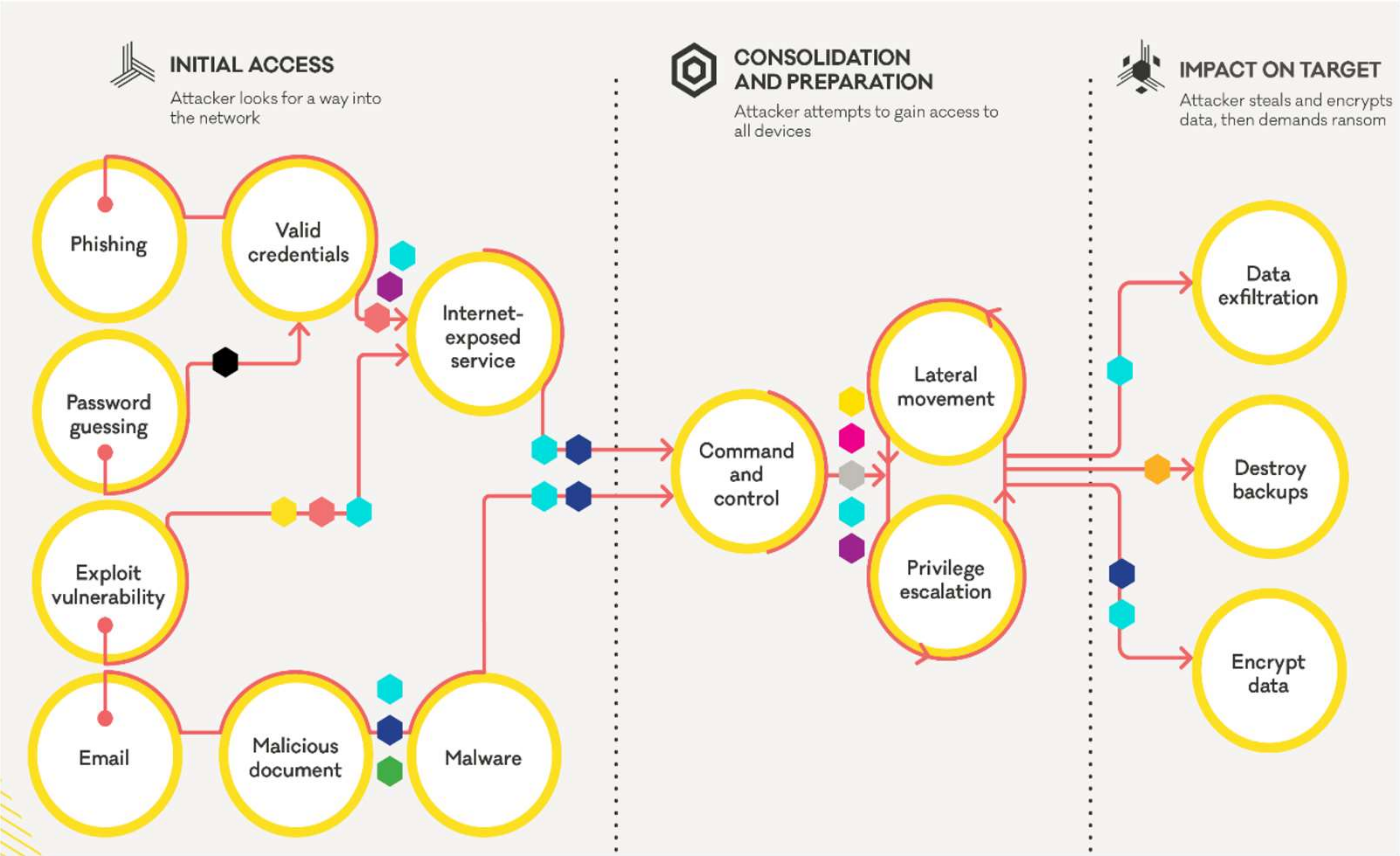
4 AVOID PUBLIC WI-FI

You may want to think twice before hopping on free, public Wi-Fi. Public Wi-Fi is not at all secure, meaning anyone that is nearby could easily access your information. When possible, avoid public Wi-Fi at all costs.

5 UTILIZE VPN TECHNOLOGY

A way to counteract the threats of using public Wi-Fi is by using a VPN. A VPN is the ultimate method of ensuring both privacy and data protection. Because of this, VPN services are growing in popularity among college students who are often forced to work on public Wi-Fi.

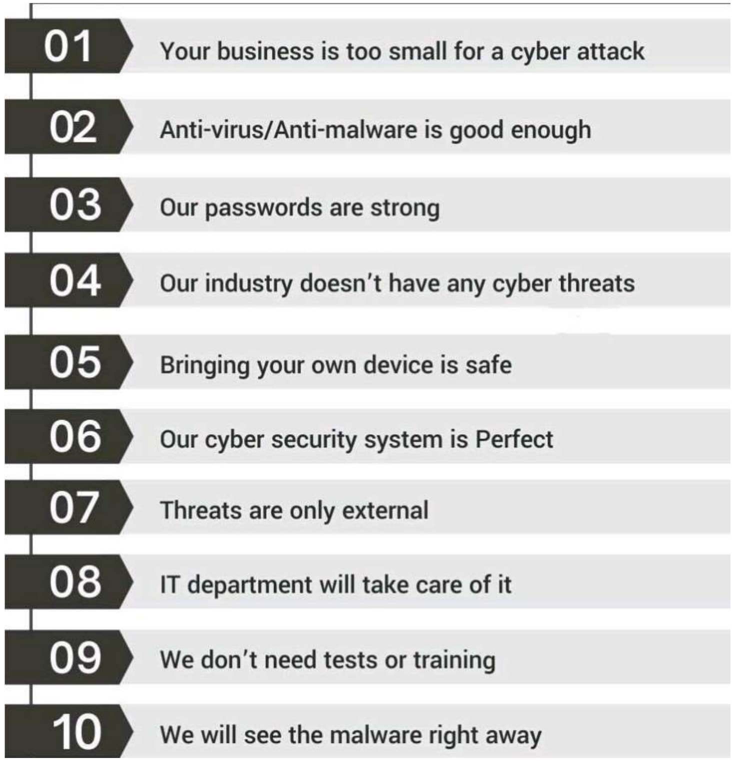
SOURCES:
- https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password
- https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings
- https://www.sonicwall.com/en-us/phishing-iq-test
- https://www.csoonline.com/article/3246984/wi-fi/why-you-should-never-ever-connect-to-public-wifi.html
- http://www.techtechnik.com/the-advantages-of-vpn-for-college-students/


INITIAL ACCESS
Attacker looks for a way into the network
CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices
IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom
Phishing
Valid credentials
Password guessing
Internet-exposed service
Exploit vulnerability
Email
Malicious document
Malware
Command and control
Lateral movement
Privilege escalation
Data exfiltration
Destroy backups
Encrypt data

Ransomware

Cybersecurity myths

- ❑ Cybercriminals are outsiders.
    - ✓ Insiders can be a part of well-organised groups, backed by nation-states.
- ❑ Risks are well-known.
    - ✓ Users unintentionally cause a data breach
- ❑ Attack vectors are contained.
    - ✓ Cybercriminals are finding new attack vectors all the time.
- ❑ My industry is safe.
    - ✓ Cyber adversaries exploiting the necessities of communication networks within almost every government and private-sector organisation.



01 Your business is too small for a cyber attack

02 Anti-virus/Anti-malware is good enough

03 Our passwords are strong

04 Our industry doesn't have any cyber threats

05 Bringing your own device is safe

06 Our cyber security system is Perfect

07 Threats are only external

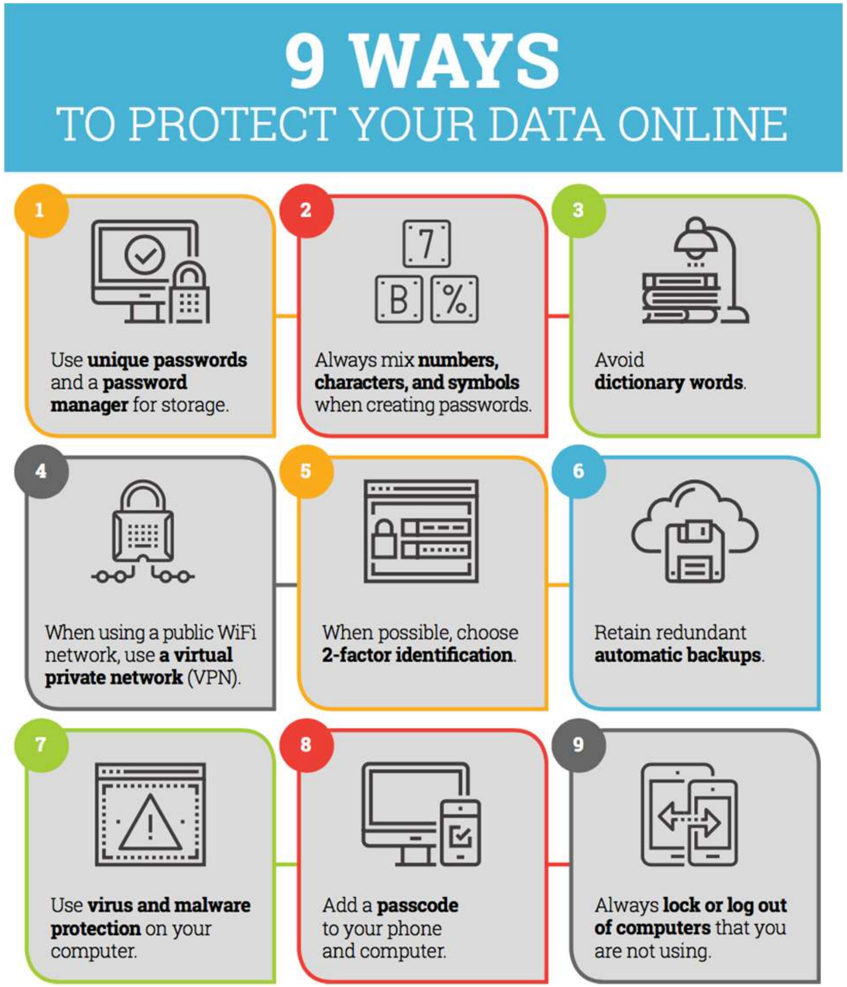
08 IT department will take care of it

09 We don't need tests or training

10 We will see the malware right away

Reporting cyber crime

- Immediate threat to life or risk of harm, call **000**.
- Cyber crime: Report | Cyber.gov.au
- Scamwatch: Report a scam | Scamwatch



9 WAYS
TO PROTECT YOUR DATA ONLINE

1 Use **unique passwords** and a **password manager** for storage.

2 Always mix **numbers, characters, and symbols** when creating passwords.

3 Avoid **dictionary words**.

4 When using a public WiFi network, use **a virtual private network** (VPN).

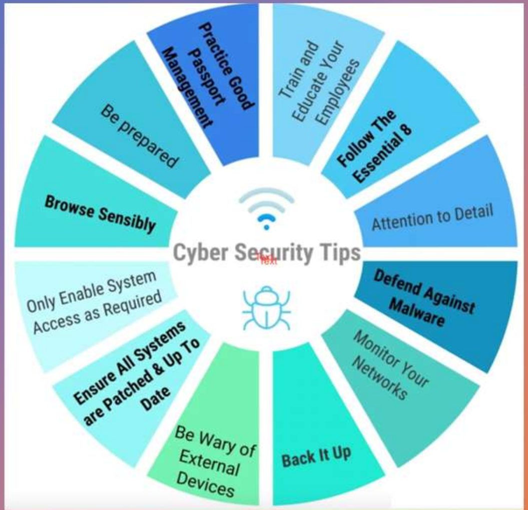
5 When possible, choose **2-factor identification**.

6 Retain redundant **automatic backups**.

7 Use **virus and malware protection** on your computer.

8 Add a **passcode** to your phone and computer.

9 Always **lock or log out of computers** that you are not using.


Cyber Security Tips
Practice Good Passport Management
Train and Educate Your Employees
Follow The Essential 8
Attention to Detail
Defend Against Malware
Monitor Your Networks
Back It Up
Be Wary of External Devices
Ensure All Systems are Patched & Up To Date
Only Enable System Access as Required
Browse Sensibly
Be prepared

Stay on top

- Sign up for alerts. Sign up for alerts | Cyber.gov.au
- ACSC: Home | Cyber.gov.au
- Cyber Security NSW: Cyber Security | Digital.NSW
- Cyber security News|Bulletins
- Cyber security podcasts

It pays to keep an open mind, but not so open your brains fall out.

CYBER SECURITY

Q&A

Deepal Kafle

Hornsby Shire Council