Do a …

SECURITY AUDIT

And see where you need to improve your security.

Why this session?

You may be aware of many of the risks to your online safety BUT

- What are the most likely risks?
- How can you protect yourself?
- What should you focus on first?

References

- Microsoft Digital Defense Reports 2020 & 2021
- Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report July 2019 to June 2020
- Verizon Data Breach Investigations Report 2020
- SOPHOS 2021 THREAT REPORT: Navigating cybersecurity in an uncertain world
- SANS Top New Attacks and Threat Report, 2021
- McAfee Labs Threats Report, November 2020
- The biggest mistakes people make with their passwords

Caveats

- Reports tend to focus on businesses rather than individuals
- Many of the high-rated risks are probably not relevant to us as individuals - I have “cherry-picked”.
- Reports such as that by Microsoft have an inherent bias due to the way they collect data (eg via MS Defender returns to Microsoft)

Cybercrime is an Industry

The cyber security landscape is constantly changing

- *The 'bad guys' are looking for the easiest way to obtain an income … So they adapt to where that is most likely*
- *Cybercrime is now an industry of its own with a budget rivalling that of nation-states*
- *Cybercriminals occupy a role that may be at any level of the industry.*

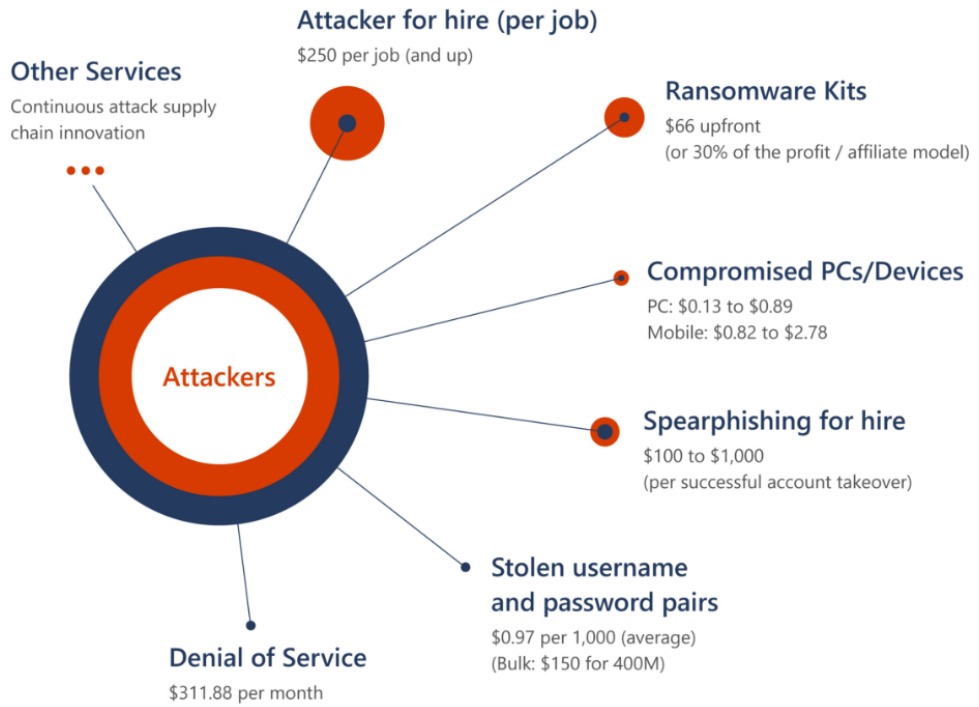
Roles in cybercrime

Ransomware taxonomy

Primary role	Description
Develops	Writes the malware
Deploys	Sends phishing emails, deploys ransomware
Provides access	Malware that loads other malware, or a group that sells access as a service
Manages/operates	Leadership of a group (such as MAZE cartel membership) and/or function that provides coordination (such as managing or operating a central extortion leak site)
Publicly reported connection	A publicly reported connection exists

[Microsoft Digital Defense Report 2021]

Average prices of cybercrime services for sale



Attackers for hire start at $250 USD per job.

Ransomware kits are $66 USD or 30% of the profit.

Compromised devices start at 13 cents per PC and 82 cents per mobile device.

Spear phishing for hire ranges from $100 to $1,000 USD.

Stolen username and password pairs begin at 97 cents per 1000 on average.

Microsoft Digital Defense Report 2021

Common attacks we'll look at

Phishing & other malicious emails

Ransomware

Data breaches

Threat 1: Phishing & other malicious emails

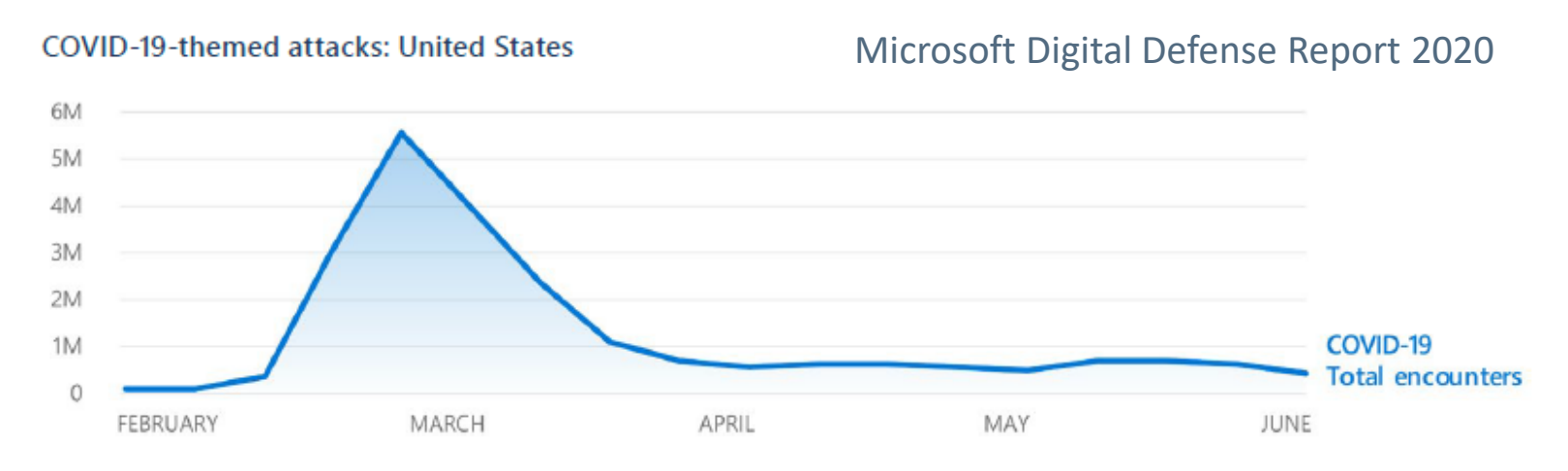
Phishing is a common way to get a foot in the door.

Be aware of the risks and learn how to identify phishing.

Ignore or delete all phishing – do not respond in any way and avoid opening phishing emails and messages if possible.

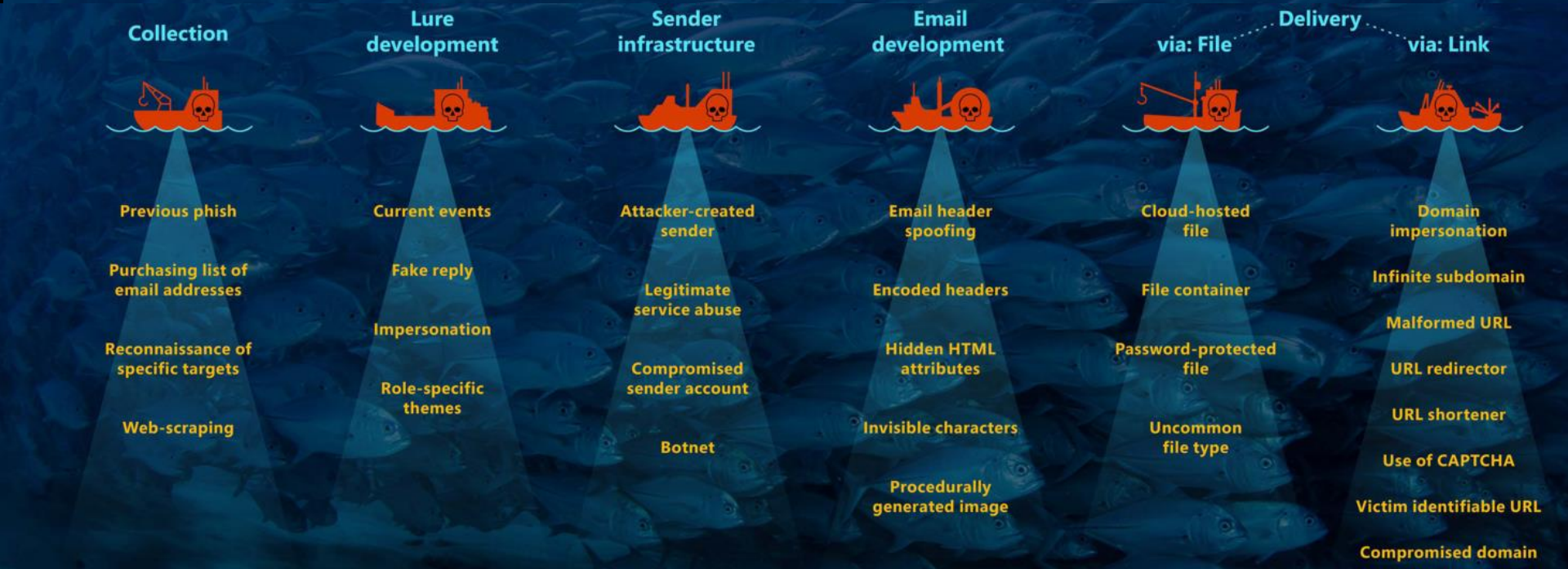
Phishing follows the issues of the day

- COVID-19! – Fear, Uncertainty
- Zoom calls
- Vaccines, RATs, masks …



Malicious email techniques

[Microsoft Digital Defense Report 2021]



ATTACKER OBJECTIVES

DEVICE CODE AUTHENTICATION PHISHING

EXTORTION

CONSENT PHISHING

FINANCIAL FRAUD

INTELLECTUAL PROPERTY THEFT

CREDENTIAL PHISHING

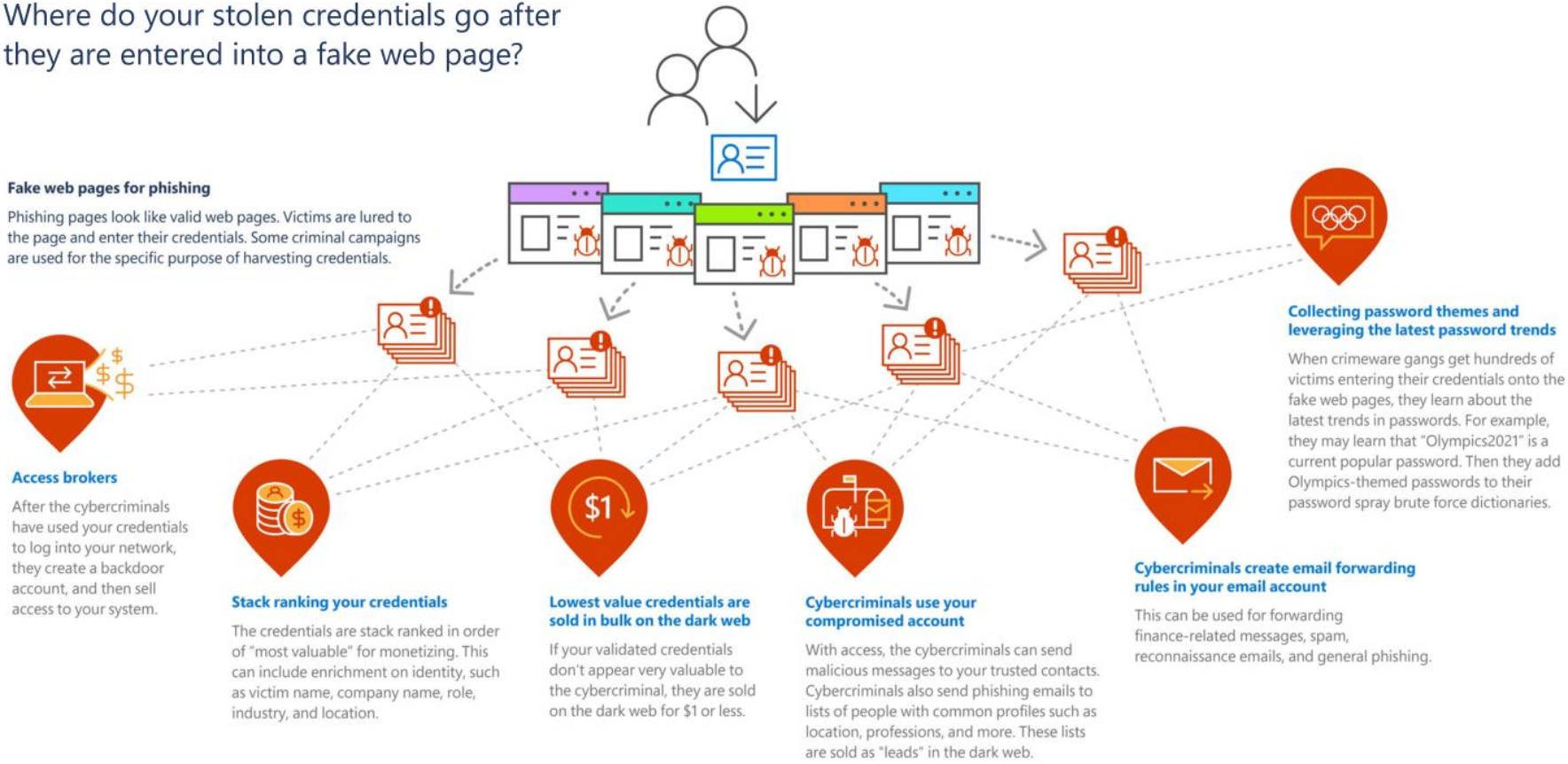
DISCOVERY / RECONNAISSANCE

MALWARE EXECUTION

The digital journey of stolen credentials

Where do your stolen credentials go after they are entered into a fake web page?

[Microsoft Digital Defense Report 2021]



Fake web pages for phishing

Phishing pages look like valid web pages. Victims are lured to the page and enter their credentials. Some criminal campaigns are used for the specific purpose of harvesting credentials.

Access brokers

After the cybercriminals have used your credentials to log into your network, they create a backdoor account, and then sell access to your system.

Stack ranking your credentials

The credentials are stack ranked in order of "most valuable" for monetizing. This can include enrichment on identity, such as victim name, company name, role, industry, and location.

Lowest value credentials are sold in bulk on the dark web

If your validated credentials don't appear very valuable to the cybercriminal, they are sold on the dark web for $1 or less.

Cybercriminals use your compromised account

With access, the cybercriminals can send malicious messages to your trusted contacts. Cybercriminals also send phishing emails to lists of people with common profiles such as location, professions, and more. These lists are sold as "leads" in the dark web.

Cybercriminals create email forwarding rules in your email account

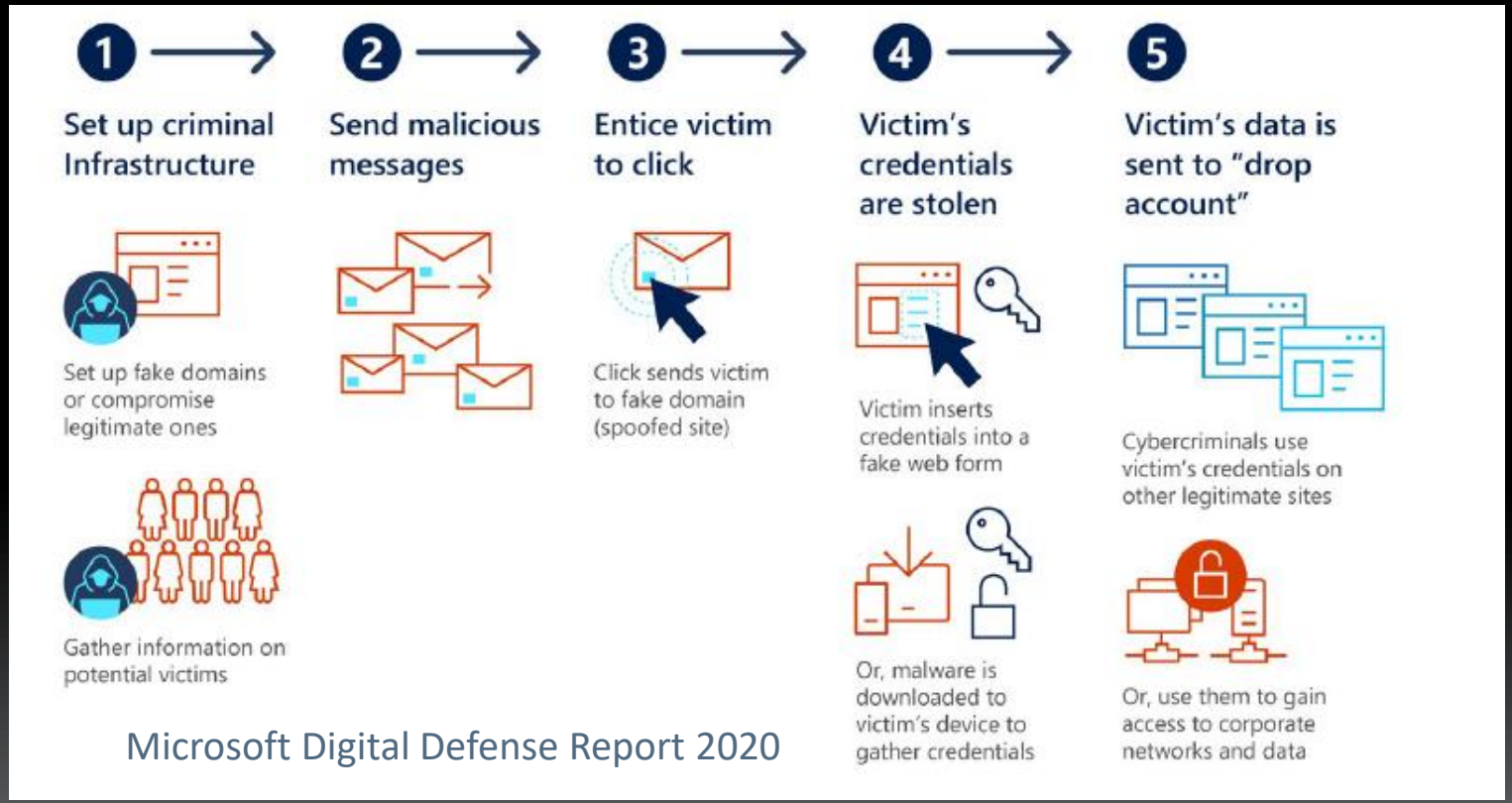
This can be used for forwarding finance-related messages, spam, reconnaissance emails, and general phishing.

Collecting password themes and leveraging the latest password trends

When crimeware gangs get hundreds of victims entering their credentials onto the fake web pages, they learn about the latest trends in passwords. For example, they may learn that "Olympics2021" is a current popular password. Then they add Olympics-themed passwords to their password spray brute force dictionaries.

Credential phishing

Credentials = username + password



Microsoft Digital Defense Report 2020

Phish kits and credential harvesting

Phish kits: enabling credential harvesting at scale

[Microsoft Digital Defense Report 2021]

Using Multi-factor authentication protects against the risks associated with credential reuse

How significant a risk?

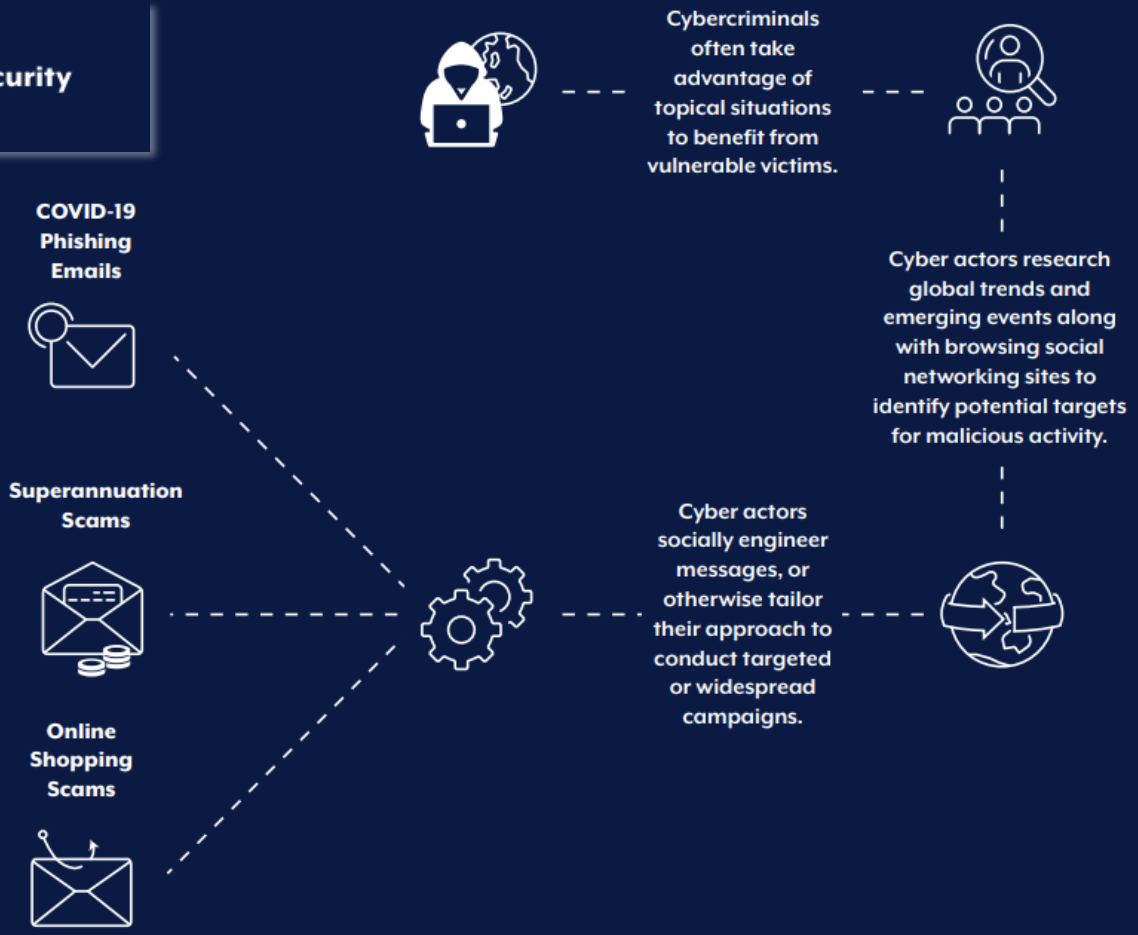
Up until a few years ago, cybercriminals focused their efforts on malware attacks because they provided the greatest ROI.

More recently, they've shifted their focus to phishing attacks (~70%) with the goal of harvesting user credentials.

Microsoft Digital Defense Report 2020

COVID-19 themed malicious activity

ACSC Australian Cyber Security Centre



[ACSC Annual Cyber Threat Report - 2020-2021.pdf]

Threat 2: Ransomware

Cybercriminals often explore documents on the target system to work out how much ransom to demand before locking or encrypting the data

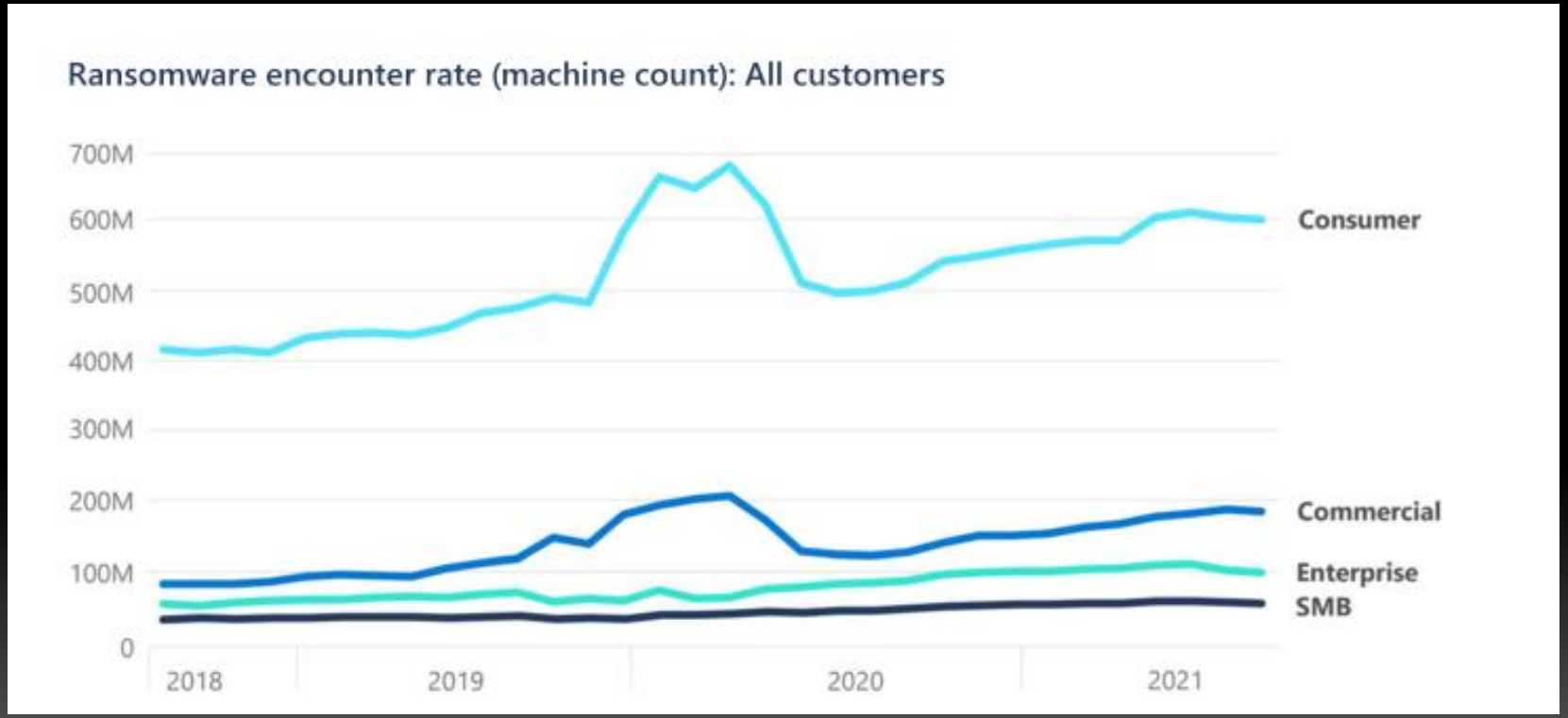
Ransomware

**Malicious cyber activity varies; the diagram below is one example of how cyber actors conduct ransomware attacks against devices and systems.*

ACSC Australian Cyber Security Centre

[ACSC Annual Cyber Threat Report - 2020-2021.pdf]

Is ransomware a threat for individuals?



Microsoft Digital Defense Report 2021

ACSC Australian Cyber Security Centre

How can I prevent a ransomware attack?

Install software updates

NEVER click on suspicious links

NEVER open suspicious attachments

Backup your devices regularly

Microsoft Digital Defense Report 2021 also recommends using 2FA and encryption of “data at rest”

Avoid ransomware

Ransomware can infect your devices in the same way as other malware or a virus. For example:

- visiting unsafe or suspicious websites
- opening emails or files from unknown sources
- clicking on malicious links in email or on social media
- downloading software from untrustworthy sites.

Common signs you may be a victim of ransomware:

- pop-up messages requesting funds or payment to unlock files.
- you cannot access your devices, or your login doesn't work for unknown reasons.
- files request a password or a code to open or access them.
- files have moved or are not in their usual folders or locations.
- files have unusual file extensions, or their names or icons have changed to something strange.

Check with your family first to see if they made any changes.

Cybercrime –Microsoft key takeaways

- **Identity and password/phishing attacks** are cheap, and on the rise. Why would an attacker break in when they can log in?
- **Distributed denial of service (DDoS) attacks are cheap** for unprotected sites—about $300 USD/month.
- **Ransomware kits** are one of the many types of attack kits designed to enable low-skill attackers to perform more sophisticated attacks.

Cybercriminals follow the money

- Australia is relatively wealthy
- We have high levels of online connectivity
- We are increasing delivery of services through online channels
- This make it very attractive and profitable for cybercriminals

Threat 3: Data Breaches

Unlike the previous 2 attacks, this one doesn't target us directly.

However, the impact is just as severe.

Credentials (username + password & sometimes other data) are stolen from websites we have an account with.

What is a data breach?

A data breach comes as a result of a cyber attack that allows cybercriminals to:

- gain unauthorized access to a computer system or network
- steal the private, sensitive, or confidential personal and financial data of the customers or users contained within.

With most data breaches, cybercriminals want to steal:

- names, email addresses, usernames, passwords, and credit card numbers.
- But they will steal any data that can be sold, used to breach other accounts, steal your identity, or make fraudulent purchases with.

Notable data breaches

Largest breaches

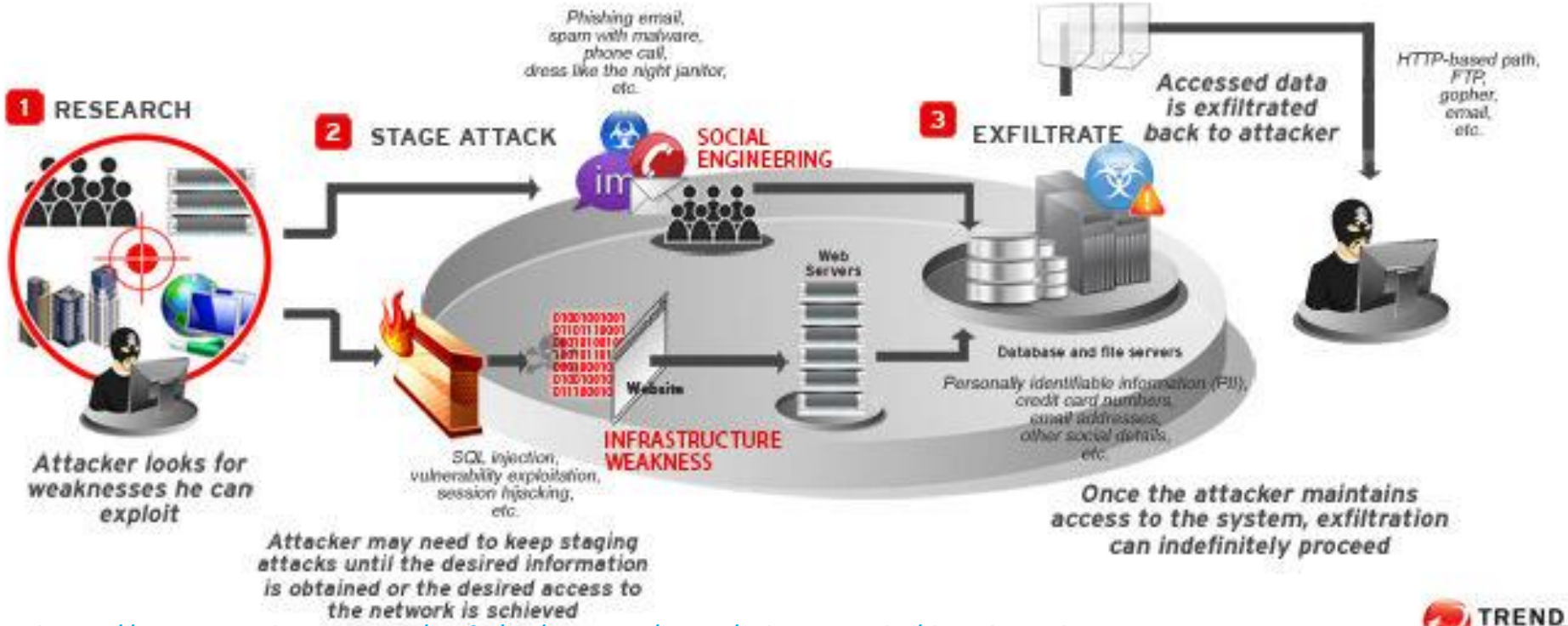
772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List

Recently added breaches

5,890,277	RedDoorz accounts
362,426	BTC-Alpha accounts
73,944	ShockGore accounts
6,783,158	Open Subtitles accounts
111,002	Upstox accounts
303,877	Carding Mafia (December 2021) accounts
5,470,063	Aditya Birla Fashion and Retail accounts

https://haveibeenpwned.com/

How a data breach happens



https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101

What happens with the stolen data?

“Credential Stuffing”

- The “bad guys” try the stolen usernames and passwords on multiple other sites
- If a password has been reused, it may work!

Now we've seen the top risks …

What do we need to do to keep safe?

Protect against Phishing

Count 1 point for each one you do

1. Be aware of scams – recognise scams, social engineering and phishing. Don't open links unless you're sure they're safe. Take care with social media networks.
2. Enable multi-factor authentication when it's available
3. Update devices and systems – turn on automatic operating system updates
4. Use strong passwords or (better) passphrases
5. Use a different password / passphrase on each account
6. Don't remember your passwords – manage them properly
7. Consider using a virtual private network (VPN) if connecting from an insecure wifi

HOW SAFE IS YOUR **PASSWORD?**

Time it would take for a computer to crack a password with the following parameters

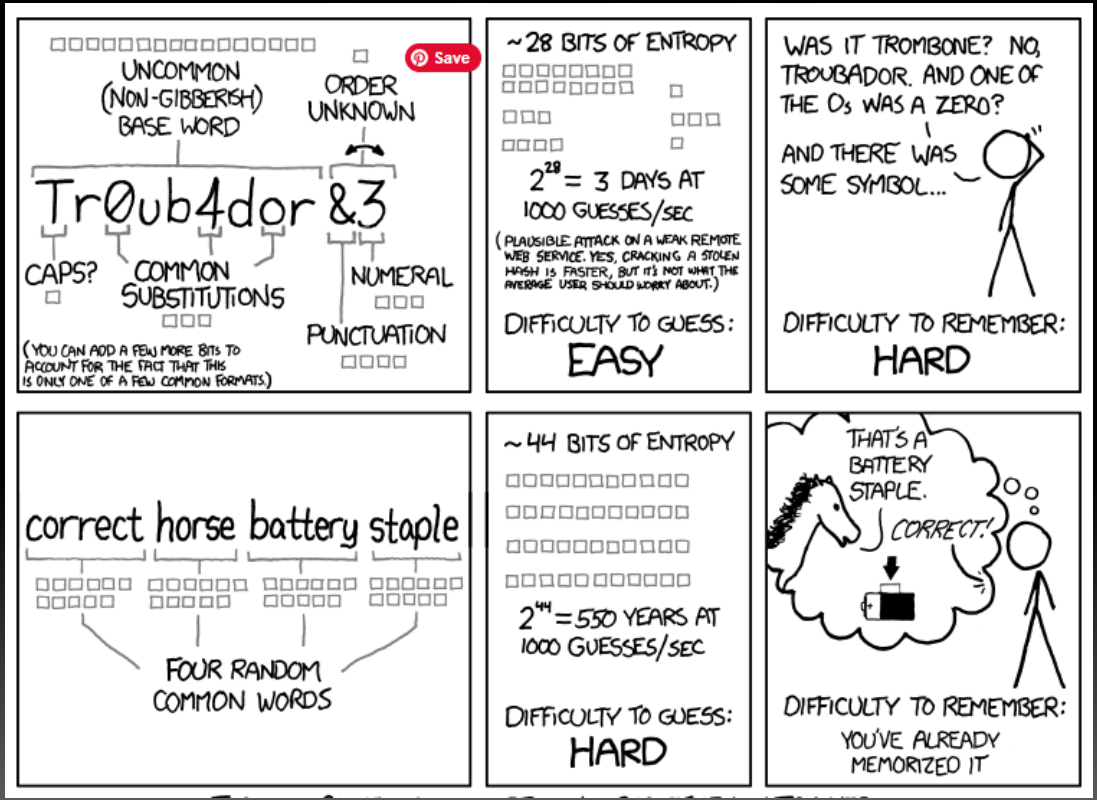
Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter + number	At least one uppercase letter + number + symbol
6	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
7	INSTANTLY	INSTANTLY	1 MINUTE	6 MINUTES
8	INSTANTLY	22 MINUTES	1 HOUR	8 HOURS
9	2 MINUTES	19 HOURS	3 DAYS	3 WEEKS
10	1 HOUR	1 MONTH	7 MONTHS	5 YEARS
11	1 DAY	5 YEARS	41 YEARS	400 YEARS
12	3 WEEKS	300 YEARS	2,000 YEARS	34,000 YEARS

businessaustralia.com

- This refers to "brute force" cracking.
  Other forms of cracking look for:
- Common passwords
- Passwords that are easy to guess:
  - dog's name,
  - mother's maiden name,
  - kids' names etc
- Any password that has been cracked before!

The biggest mistakes people make with their passwords

Passphrases



Suggestion:

Use an app such as:

- APG2Go
- Mantra

to generate a starting point.

Modify as needed to include:

- upper case
- numbers
- special characters

Protect against Ransomware

Count 1 point for each one you do

1. Update devices and systems – turn on automatic operating system updates
2. Enable multi-factor authentication when it's available
3. Backup data regularly
4. Regularly save a backup offline
5. Always run good anti-malware software
6. Restrict access to your devices with a keyboard lock
7. Reduce the chance of theft with a physical lock
8. Keep administrator privileges safe – use an "ordinary user" account
9. Turn on ransomware protection – if available

Malware

- Viruses, trojans, worms, rootkits, spyware, bots, …
- ‘Anti-virus’ software aims to trap all of these
- ‘Real-time’ operation relies on ‘sniffing’ out ‘fingerprint’ patterns in data – needs up-to-date ‘fingerprint’ data from the anti-virus vendor
- Regular scanning of your computer to look for any ‘fingerprints’ not identified initially

Administrator accounts

- Your computer uses an administrator account to:
  - Install new software
  - Change permissions on your computer
- You should avoid using an administrator account for your day-to-day interactions

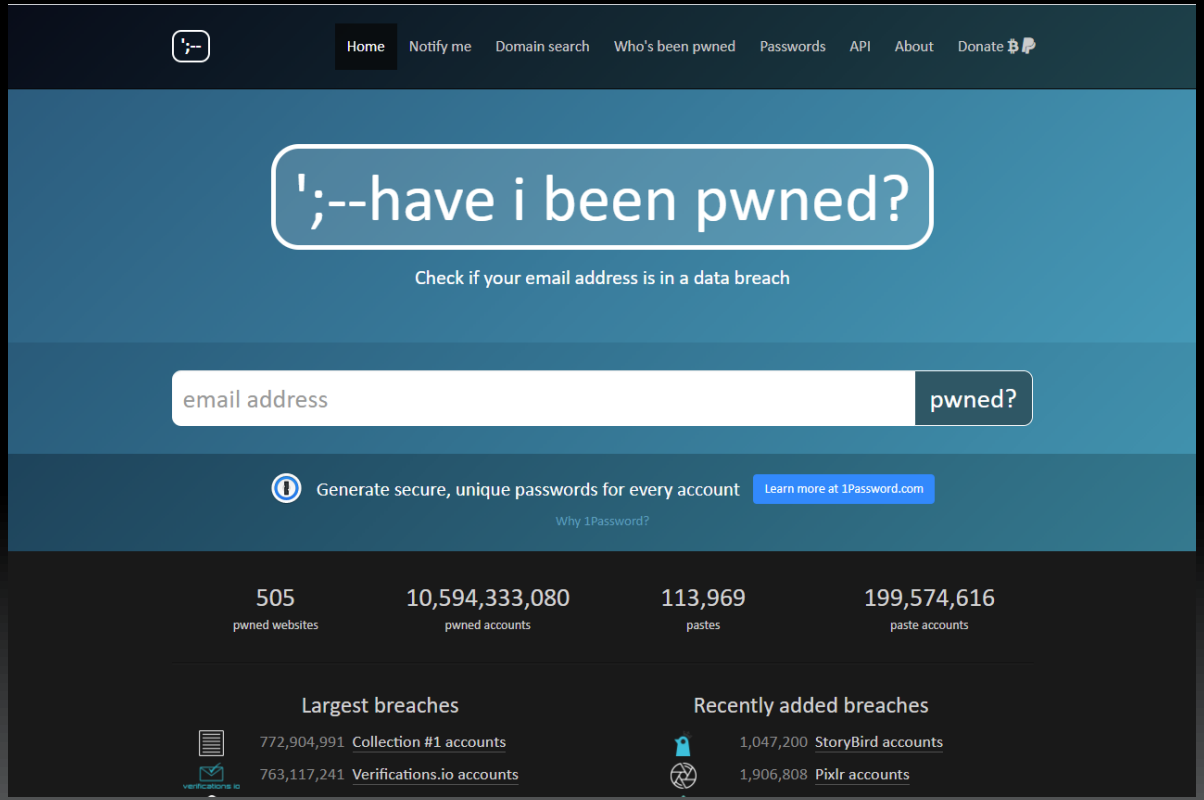
Protect against data breaches

Count 1 point for each one you do

1. Use a different password for every online account
2. Use a strong password / passphrase (>12 characters etc)
3. Use multi-factor authentication when available
4. Be aware of data breaches – subscribe to Have I Been Pwned for each email account you own
5. When you are notified of a breach affecting you, change your password for every affected account
6. Consider using a different email address for each account (eg Apple's hidden email facility)
7. Be aware of scams – don't respond to spam in any way

Have I Been Pwned?

https://haveibeenpwned.com/



What to do if you're in a data breach?

- Act immediately – the bad guys have had a lot of time to use your credentials
- Change your password for the account that was breached
- Change the password for any other account that used the same or similar password
- Make sure you use strong passwords (>12 characters, mixed alpha, numeric, special)
- Turn on 2FA if available for that account

If your email account is hacked

You'll find out about this in a different way:

- E.g. Your contacts get spam from your email address

WHAT TO DO:

- Act immediately! See: https://askleo.com/email-hacked/ for full details of what to do including:
- Try to recover your account
- Change your password
- Check your recovery information etc

How did you go?

- Maximum score = 7 + 9 + 7 =23

What do you need to know more about?

1. Scams
2. 2FA
3. Updating
4. Passwords and passphrases
5. Password manager
6. VPN
7. Backups
8. Anti-malware software (anti-virus)
9. Physical protection for devices
10. Account privileges – admin vs user
11. Ransomware protection
12. Data breaches and credential stuffing
13. Hidden email facilities
14. Spam

SUMMARY

- Online risks keep changing – we need to keep aware
- Major risks are:
  - Phishing
  - Malware that ransoms your computer or steals your credentials
  - Theft of credentials from online accounts
- You can set up automatic routines and develop habits that protect yourself!

ANY QUESTIONS ?

Thank you for attending this
U3A presentation / demonstration