

A matter of 'when', not 'if'...

What happened in 2021-22 (that was reported)



- 76,000 cybercrime reports via ReportCyber equivalent to **one report of a cyber attack every 7 minutes**.
- Cost of cybercrime up to **\$33 billion** in Australia.
- Average self-reported loss was **\$39,000** for **small businesses** and **\$88,000** for medium businesses **(on average)**
- Approximately **52%** of **ransomware** cybercrime reports were by small-medium businesses
- No sector of the Australian economy is immune. Government, industry, families and individuals were all targeted.

Common Cyber Security Threats

Phishing

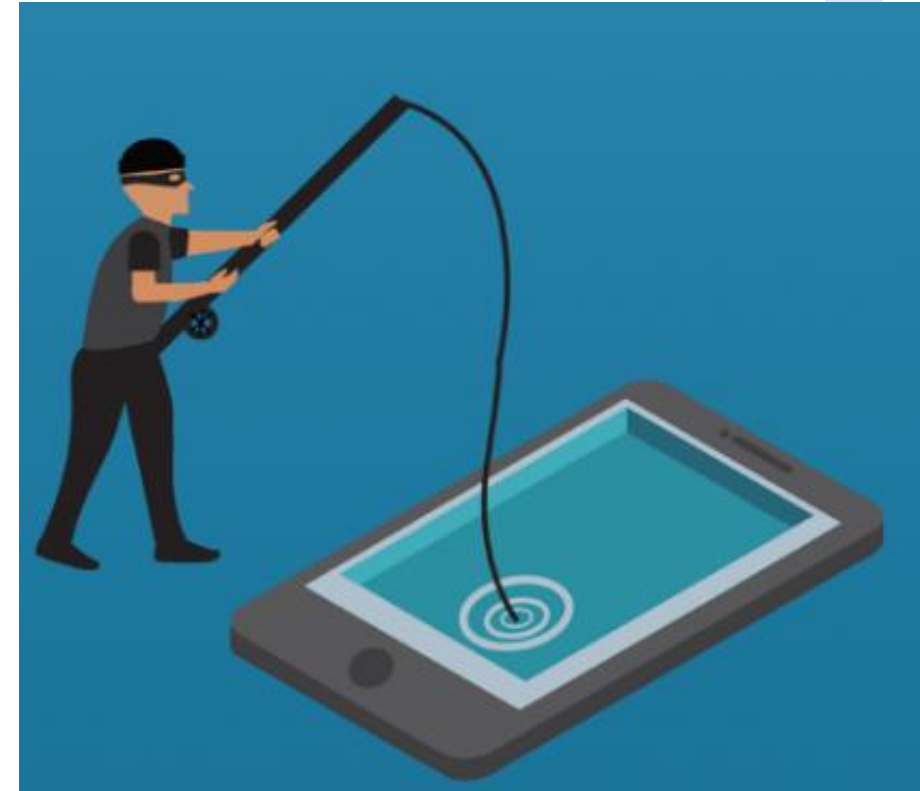
- Malicious links
- Random

Ransomware

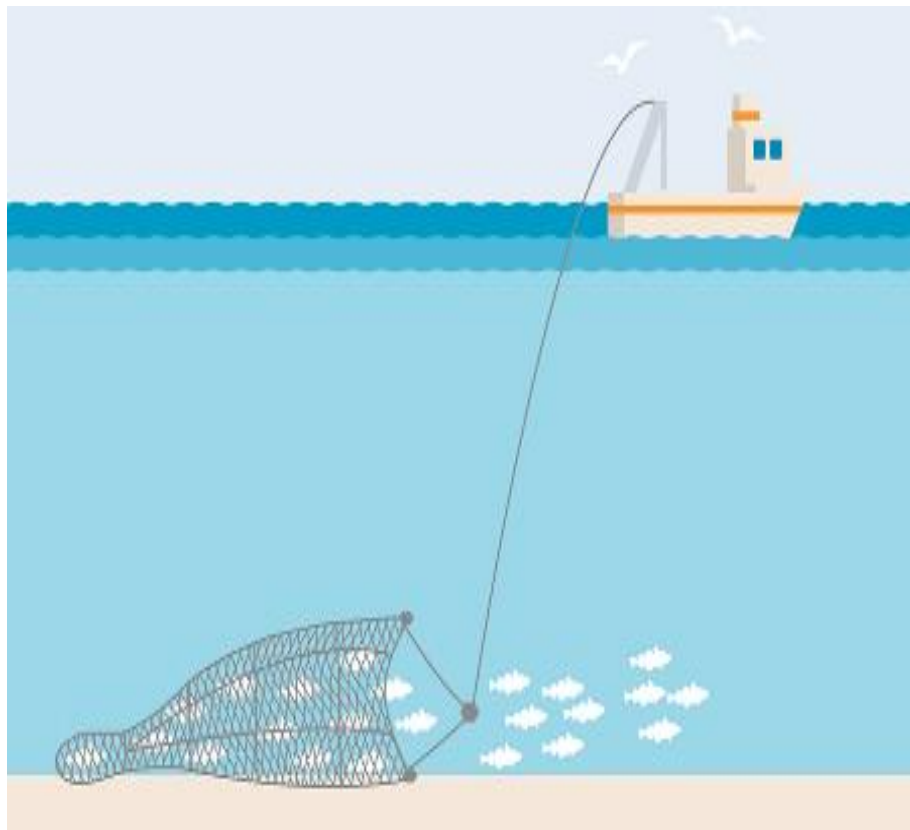
- File encryption
- Ransom demand

Business Email Compromise

- Invoice fraud, employee and company impersonation.



Phishing



What is it?

- Messages to trick you into sending money or providing your personal information.
- The message may tell you there is a problem (e.g. overdue payment or an instant refund)
- Usually includes a link that takes you to a fake website

Who will receive this type of scam?

- Anyone. Phishing is random. Spear-phishing can be more targeted.

How is this scam sent?

- Emails, SMS, Instant Messaging, Social Media

THINK BEFORE YOU CLICK ON A LINK!

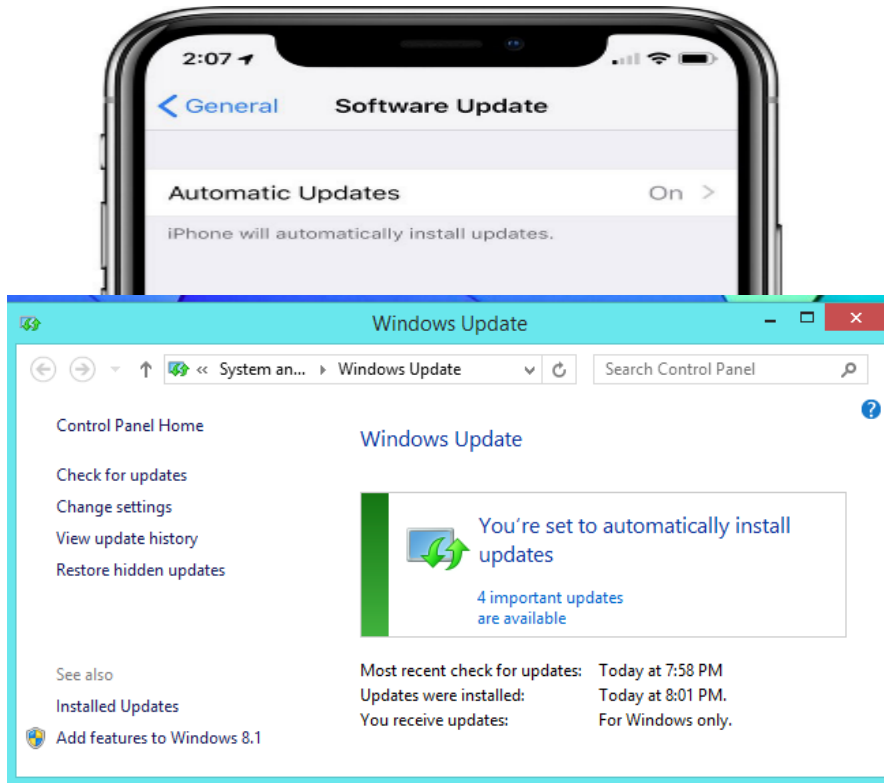
Case study - Business Email Compromise (BEC)

Invoice scams



What are the most effective ways for businesses to protect themselves??

- Automatic updates
- Multi Factor Authentication
- Passphrases



Automatic Updates

What?

Automatic software updates

Why?

Safer, faster and better protection

When?

As often as possible

Multi-factor authentication (MFA)

What?

A security measure that requires two or more proofs of identity to grant you access

Why?

Significantly more powerful security



Passphrases and Password Manager

A phrase or sentence
instead of a single word.

Effective when they are
unique, long, complex and
use some numbers or
special characters.

PASSWORD/ PASSPHRASE	TIME TO CRACK		EASY TO REMEMBER	COMMENTS
	Brute Force Attack	Dictionary Attack		
password123	Instantly Less than AU\$0.01	Instantly Less than AU\$0.01	Very Easy (too easy)	One of the most commonly used passwords on the planet.
Spaghetti95!	48 hours AU\$587.50	Less than half an hour AU\$6.10	Easy	Some complexity in the most common areas, and very short length. Easy to remember, but easy to crack.
5paghetti!95	24 hours AU\$293.70	Less than 1 hour AU\$12.20	Somewhat Easy	Not much more complexity than above with character substitution, and still short length. Easy to remember, but easy to crack.
A&d8j+!l	2.5 hours AU\$30.60	2.5 hours AU\$30.60	Very Difficult	Mildly complex, but shorter than the above passwords. Hard to remember, easy to crack (against BFA).
I don't like pineapple on my pizza!	More than 1 Year More than AU\$107,222.40	More than 40 days More than AU\$11,750.40	Easy	Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very difficult to crack.



Australian Government
Department of Home Affairs

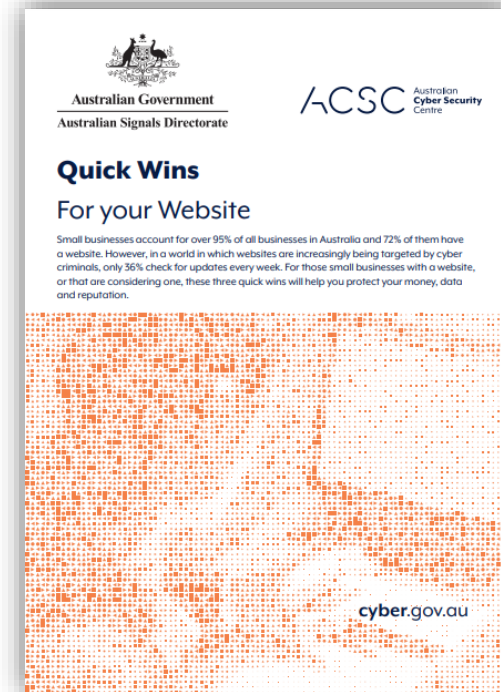
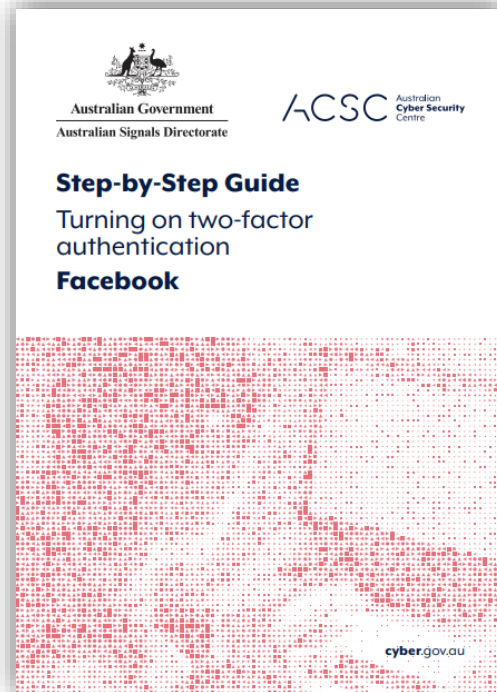
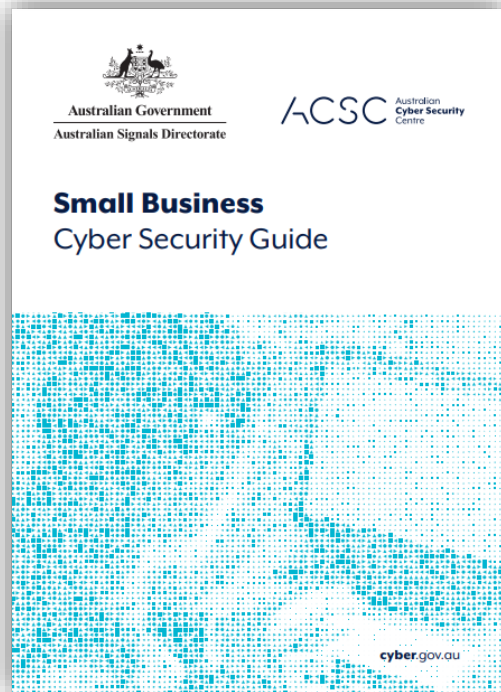


CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

ACSC Australian
Cyber Security
Centre

Australian Cyber Security Centre Resources

www.cyber.gov.au

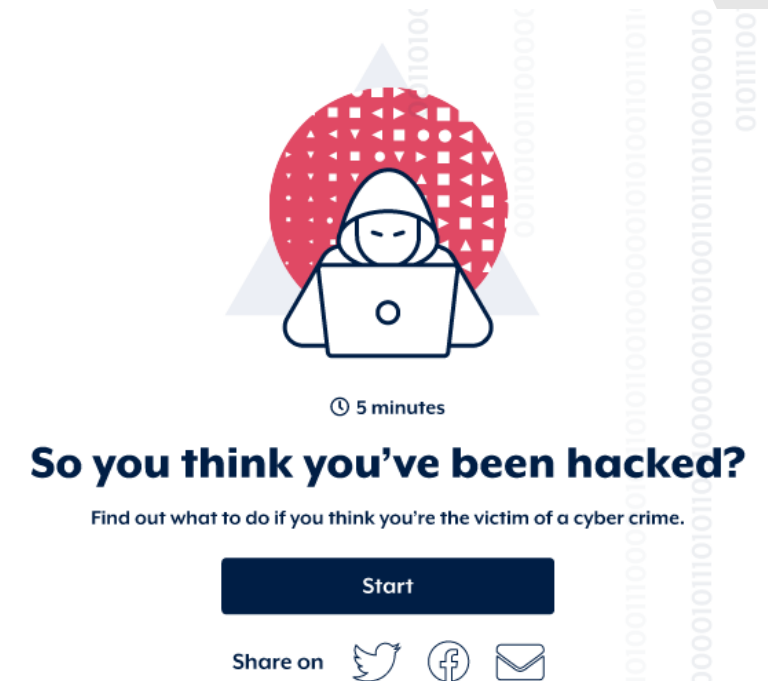


Have you been hacked?

'Have you been hacked?' steps potential victims through a series of scenarios to help assess if they've been hacked, and guide them on how to respond.

Scenarios include ransomware attacks, malware, email compromise and identity theft, as well as phishing and fake website scams accessed via sms and mobile devices.

Tool can be found on cyber.gov.au





Assess your level of cyber security

[Cyber Security Assessment Tool | Cyber.gov.au](https://www.cyber.gov.au/cyber-security-assessment-tool)

Your assessment and recommendations

Based on your responses, your cyber security maturity and knowledge level is: **Starter**.



Your business is in the early phase of its cyber security journey. You should be focusing on putting in place some basic measures to have a more effective approach to cyber security.