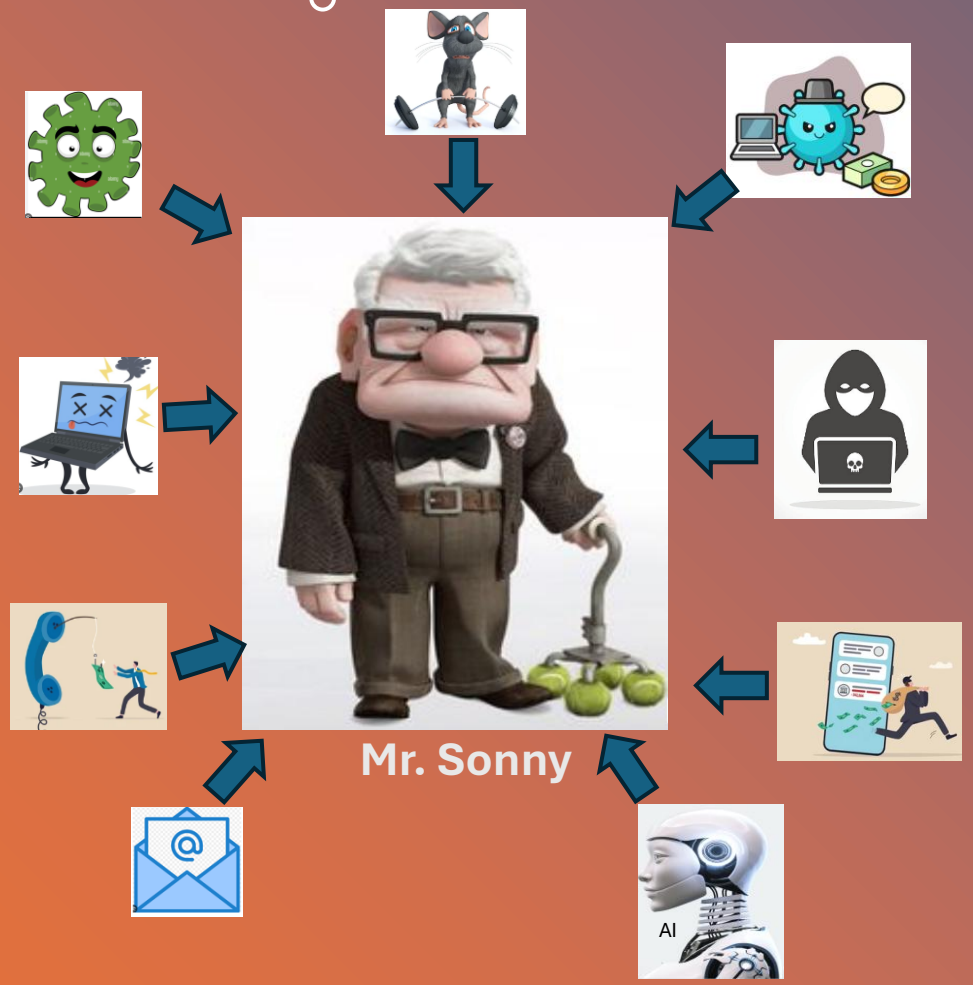
Cybersecurity & Artificial Intelligence

Awareness For Senior Citizen Presentation



- **Inspiration for Seniors**
- **Cyber Threats**
- **Vulnerability**
- **Impact to our Life**
- **Self Assessment**
- **Resilience**
- **Maturity**
- **Getting Help**

Presented By: Abelardo (Sonny) Gomez

15 June 2026





Educational and Work Achievements

- **BS Electrical Engineering (National University)**
- **Electronic Engineering (Victoria University)**
- **Master of Engineering (Swinburne University)**
- **PhD in Systems Engineering- 2nd Year (RMIT)**
- **Professional Cooking (William Angliss)**

Retirement

- **Postgraduate in Cybersecurity- Honor (RMIT)**
- **Presently-Master in Artificial Intelligence (Scholarship with La Trobe University)**

41 years

Senior Electrical Engineer and Hazard Dust Specialist

Nestle Australia

Wonka Factory

As Rotarian my Objective: Share Knowledge, Protect People & Industry









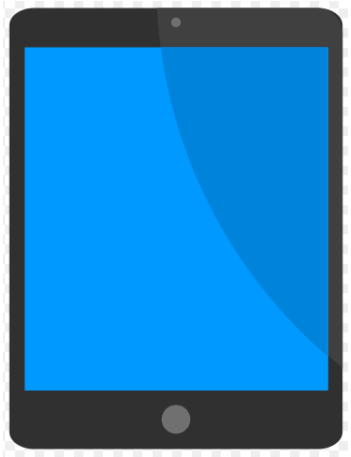


Our Senior Now Spoiled of Electronic Gadgets











We are expose to :

Application, Facebook,

Tic Tok & Online Shopping







CURRENT REALITY

⚠ The Modern Hazard Cyber Threats:

1 Every 10 Mins

A new cyber attack is reported to the Australian Cyber Security Centre (ACSC).
That is 1 in every 4 people affected annually.

It is no longer a question of IF it happens, but WHEN.

My Main Objective is to protect the Industrial Automation

CORE FRAMEWORK

The 5 Elements of Cybersecurity

1. Human

Behaviors & awareness.

2. Cyber Threat

Scams & malicious intent.

3. Vulnerability

Weaknesses in defense.

4. Impact

Financial & stress cost.

5. Resilience

Behavioral adaptivity.

ATTACK VECTORS

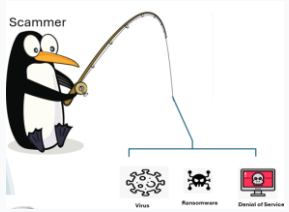
Common Digital Threats





Malware

Ransomware, viruses, and unauthorized access tools.



Phishing

Deceptive calls and fraudulent messages stealing credentials.



Social Engineering

Deceiving individuals into revealing private passwords.



IoT ,AI & Voice Clones

Synthetic voice scams and hyper-realistic fraud.

Scammers are very Resourceful



Dark Web



Mr. Sonny

No.	Behavior Description
1	Behaviour:NoWorriesItShouldBeOkay.
2	Behaviour:MistakenBelieve.
3	OpeningFakeEmails.
4	WeakPasswork.
5	LackAwareness.
6	LackTraining.
7	SharingTooMuchSocialMedia.
8	DiscussConfidentialInfo.
9	EasyTrustBrand/Logo.
10	UsingUnsecureWIFI.
11	ConnectUSBUnknownSource.
12	NotBackingUpData.
13	ImproperlyDisposingData.
14	NotLockingScreen.
15	SensitiveUnencrypted.
16	NotUpdatingApplication.
17	IgnoringCybersecurityProtocol.
18	UsingPersonalEmailForWork
19	Behaviour:Laziness.
20	Trust UnknownCaller.

How Do We Protect Ourselves from Cybersecurity Risk?

1. Identify Our Vulnerabilities and Behavior.
2. Identify Our Financial Impact
3. Identify Our Metric Score Risk
4. Identify Our Maturity Acceptance
5. How Do We Build Resilience?

Cybersecurity Self Risk Assessment

			Vulnerability / Weakness				Financial Impact			
No.	Behavior Description	Include	Low	Medium	High	ExtremeHigh	Low Greater < $5K	Medium Greater $20K	High Greater $50K	ExtremeHigh Greater< $100K
1	Behaviour:NoWorriesItShouldBeOkay.	Yes	.	.	.	1				$110,000
2	Behaviour:MistakenBelieve.	Yes	.			1				$100,000
3	OpeningFakeEmails.	Yes		1			$5,000			$5,000
4	WeakPasswork.	Yes			1			$20,000		
5	LackAwareness.	Yes				1				$55,000
6	LackTraining.	Yes				1				$55,000
7	SharingTooMuchSocialMedia.	Yes		1				$25,000		
8	DiscussConfidentialInfo.	Yes			1				$54,000	
9	EasyTrustBrand/Logo.	Yes		1				$20,000		
10	UsingUnsecureWIFI.	Yes		1				$21,000		
11	ConnectUSBUnknownSource.	Yes			1			$25,000		
12	NotBackingUpData.	Yes		1			$3,234			
13	ImproperlyDisposingData.	Yes		1			$2,234			
14	NotLockingScreen.	Yes	1		.	.	$1,000			
15	SensitiveUnencrypted.	Yes			1				$55,000	
16	NotUpdatingApplication.	Yes		1		.				$60,000
17	IgnoringCybersecurityProtocol.	Yes			1		$5,445			
18	UsingPersonalEmailForWork	Yes				1			$50,000	
19	Behaviour:Laziness.	Yes			1					$75,000
20	Trust UnknownCaller.	Yes		1				$20,000		

Designed by: Abelardo (Sonny) Gomez 26 July 25

When Priority is Clear, Decision is easy.





Need Support

Cybersecurity is **everyone's responsibility**.

a. Everybody from the family using the gadgets.

b. Understanding

c. Preparing

d. Adapting is key to staying safe in today's digital world.

Build Our Resilience

By Changing our Behavior

RESILIENCE TIP #1



Strong Key Passwords

WEAK (DO NOT USE)

Violette123

Short 10 Characters, predictable word combinations.

1.6 Million Combinations

Cracked instantly by standard tools.

Tip:

Melbourne$3000_G25

14+ characters, mixed case, numbers, symbols.

17 Quadrillion Combinations

Resistant to brute-force attacks.

Password Resilience

RESILIENCE TIP #2

Card & Payment Protection

Master Card

Block tapping capability for high-value accounts. Use strictly for trusted, verified vendors.

Travel Card

Enable tapping with a low limit ($200 max). Top up $100 as needed for public transit & coffee.

Debit Card

Remove tap option. Require PIN verification always to prevent unauthorized contactless drain.

Activate Your Multi Factor Authentication (MFA)

Use Bank Application with Transaction Notification

RESILIENCE TIP #4

Mobile Device Hardening

Device Security

Android Hygiene

Open-source architecture requires active user defense:

- Disable third-party app installations
- Review permission access frequently

iOS Security

Closed ecosystem with centralized controls:

- More Operating System Secure
- Enforce biometric authentication

Update all the time Mobile Operating Software

RESILIENCE TIP #5

Phone Etiquette & AI Voice Attacks

Voice Clone Defense

11 Seconds to Clone

Modern AI requires as little as 10 seconds of audio to synthesize your voice convincingly for scam calls to family or banks.

Safe Phone Protocol

- **Resistant to brute-force attacks**.
- **Refuse:** "I do not provide details over the phone."
- **Hang up:** Terminate suspicious calls immediately.

Do not Mention the word “Yes”



Resilience:

- **Prevent using QR Code in downloading any information to your Devices.**



Resilience:

Prevent using Unsecure WIFI Network in downloading any information to your Devices.

Resilience Tip





Risk of Online Shopping in Facebook or Tik-Tok and Emails

Buying through **Facebook** or **TikTok** comes with real **cybersecurity and fraud risks**, especially because these platforms are not traditional e-commerce stores — they **host sellers, but don't verify all of them**. Beware of Emails. Using Voice Clone. **Fake Sales**

⚠️ Main Risks in Facebook and TikTok :



1. Fake Sellers / Pages
Scammers often create f ams to sell non-existent or low-quality items. Once payment is r uyer.

2. No Buyer Protection
Unlike Amazon or eBay, F ps may not offer robust refund or dispute systems. If you're scamm er your money.

3. Counterfeit or Mislea
Photos or videos may sh what arrives (if anything) is often fake, damaged, or completely

4. Phishing Links
Some sellers send links (") that lead to phishing websites designed to steal your credit card,

5. Malware Traps
Clicking unfamiliar ads o an sometimes lead to malware-infected sites, especially on Andr

6. Payment Scams
If a seller insists on direc a red flag. These are hard to trace and offer zero protection if someth

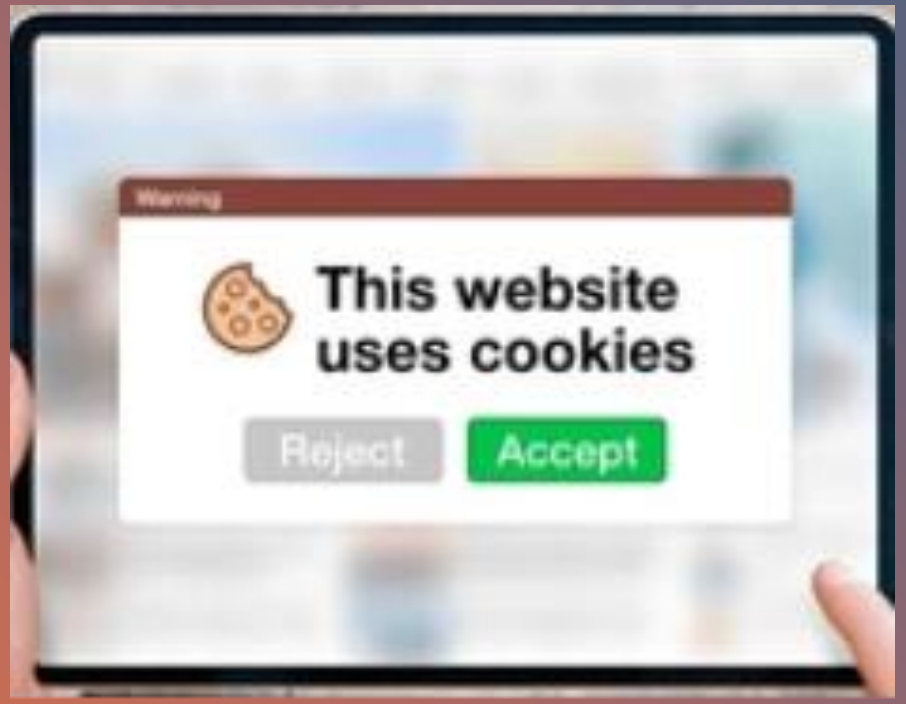
Resilience Tip No. 8

How to Identify AI-Generated Information



- If the information you receive seems unrealistic, too good to be true, or doesn't match what's possible in our current time, there's a high chance it was generated by AI. These types of messages or content can often be misleading—and in some cases, they may be part of a scam.
- Always verify the source of the information. If it lacks human context, includes strange wording, or offers unbelievable claims (like guaranteed money, miracle cures, or secret tech), be cautious—it might be AI-generated and designed to trick or deceive.
- **Ignore it right away**

Beware of Web Browser cookies



Resilience Tip

- Safety Rating



- Governments are now preparing legislation to introduce a **Cybersecurity Star Rating System** for smart appliances.
This system will show how well a device protects your privacy and data from hackers.
- **What You Should Do:**
- **Watch for this rating** in stores and online.
- **Only buy appliances with a high cybersecurity star rating.**
- Protect your home by making smart, safe choices.

Cybercrime getting help:

End

ASD Australian Signal Directorate
1300 CYBERI (1300 292 271)



Triple Zero - 000

Call 000 immediately if the incident is life-threatening, needs immediate police attendance, a crime is happening now, or an offender is (or may be) still in the area.

Crime Stoppers Victoria

Police Assistance Line - 131 444

To report non-urgent crimes and events.

To report COVID breaches.

Crime Stoppers Victoria

Crime Stoppers - 1800 333 000

To report crime information anonymously.

Note: Crime Stoppers is unable to offer emergency response services or assist victims of crime

Crime Stoppers Victoria

Any Question ?

Abelardo (Sonny) Gomez
Cybersecurity and AI Engineer
Gomeson Tech
Email: abelardosonnygomez@gmail.com
Mobile: 0401 134 359