

LET'S TALK CYBER AWARENESS



Leah Armand
Chief Information Security Officer (A/g)
Federal Court of Australia



OVERVIEW

- » Welcome
- » Forming a Cyber Awareness Plan
- » Set the plan in motion
- » Understand your people- Learning Styles
- » Awareness Initiatives
- » Mind the GAP; Stakeholder Engagement



About

- A/g Chief
- Bachelor
- Mother of

Former Ro

- Assistan
- Australia
- Cyberse
- WA Poli
- Regiona
- Super Re

BRACE YOURSELF



makeameme.org

stralia
ECU

court of

or the

and,

CYBER AWARENESS

PLAN



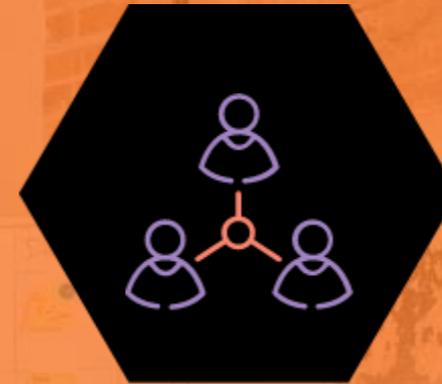
WHY?

Creates a coordinated, considered and streamlined approach which aligns and supports the broader objectives of the Cyber Strategy.
Executive buy in!



WHAT?

Awareness methodology, key stakeholders and their responsibilities, time frames.



WHO?

Stakeholder engagement, who else within the organisation can help with the implementation. Bring others on the journey!



WHERE?

Embed the roadmap and stick to it. This plan should become a part of BAU within the Cyber or GRC function.

DON'T REINVENT THE WHEEL



Online Resources

Google....

Search engines- Google Images

Open-source intelligence

LinkedIn



Government Agencies

ACSC- Australian Cyber Security Centre

ASD- Australian Signals Directorate

eSafety Commissioner



In-house or procured software

Use YOUR people!

Not just IT Communications/Digital Teams,
Media Cyber Awareness Platforms which
provide content, and can be personalised to
your organisation.

JUST RE-ALIGN IT



“If an individual can’t learn the way we teach, ~~maybe~~ we should teach the way they learn”

UNKNOWN

THE SOLUTION

ENSURE YOUR AWARENESS PLAN INCLUDES STRATEGIES WHICH ALIGN WITH THE FOUR MAIN LEARNING STYLES



VISUAL
LEARNERS



READ/WRITE
LEARNERS



AUDITORY
LEARNERS



KINAESTHETIC
LEARNERS

TIMELINE

RESPONSIBILITY

ACCOUNTABILITY

SUCCESS

JANUARY 2022

FEBRUARY 2022



Cyber Theme:
Working Remotely



Release newsletter
content



Monthly Lockscreen
Design deployment



Prepare Feb theme:
Ransomware



Cyber Theme:
Ransomware



Release Newsletter
Content



Monthly Lockscreen
Design deployment



Prepare March
Theme content:
Passwords

Cyber Awareness Initiatives

Connect directly with your employees

- Posters
- Computer lockscreens
- Cyber in your pocket guides
- Internal Newsletters
- Knowledge Sessions
- Learning Management System
- Table Top Exercises
- Company Intranet
- Phishing Campaigns
- Brain Teasers

PRIVACY

Always ask why, how and who

- Why am I being asked for this information
- Is how the information being sought credible
- Do I know this person

Protect yourself online, commit to sharing less and don't leave your personal information lying around.

Protect what matters most

- Safeguard your privacy and security. Every small action counts.
- 2FA
- Passwords/paraphrases
- Software updates

Start small and take it one step at a time. Make cyber a lifestyle.

If you receive any suspicious emails, calls or sms immediately contact the [redacted]

SOCIAL ENGINEERING:

The art of manipulation used to gain access to information and/or devices

Cyber criminals look for information about their victims online, prior to attempting to 'hack' them. Remain vigilant and **do not share** personal details online such as date of birth, phone numbers, holiday plans etc.

Malware Baiting Phishing Pretexting Shoulder surfing Dumpster diving

How can socially engineered messages be identified?

Is the sender asking you to open an attachment or access a website?	Is the sender asking for information they wouldn't necessarily need to know?
Is the sender asking you to perform a specific activity?	Is the message suspiciously written?

If you receive any suspicious emails, calls or sms immediately contact the [redacted]

TIPS TO PROTECT YOUR PRIVACY

Keep up to date with current scams. Always think: Who? Why? How?

Delete unused applications

Use security software on all devices

Don't give out your personal information unless you're sure how it will be used

If you receive any suspicious emails, calls or sms immediately contact the [redacted]

DID YOU KNOW

that a foreign USB memory stick can download malicious code and steal data directly from your computer?

NEVER plug in any unknown media devices such as USB's, hard-drives and/or mobile phones.

If you receive any suspicious emails, calls or sms immediately contact the [redacted]

SECURITY IS NOT COMPLETE WITHOUT U



SECURITY ALERT- LOCK IT BEFORE YOU LEAVE IT
Windows Key + L
You never know who is watching you!
If you have any security concerns, contact _____ immediately
1300 --- ---



SECURITY ALERT- LOCK IT BEFORE YOU LEAVE IT
Windows Key + L
You never know who is watching you!
If you have any security concerns, contact _____ immediately
1300 --- ---



SECURITY ALERT- LOCK IT BEFORE YOU LEAVE IT
Windows Key + L
You never know who is watching you!
If you have any security concerns, contact _____ immediately
1300 --- ---



SECURITY ALERT- LOCK IT BEFORE YOU LEAVE IT
Windows Key + L
You never know who is watching you!
If you have any security concerns, contact _____ immediately
1300 --- ---

POSTERS

HOW RANSOMWARE WORKS AND HOW TO PROTECT THE ENTITY



1. Ransomware starts with an unsolicited email that tries to lure you (the victim) into clicking a link or downloading an attachment.
2. Ransomware takes advantage of a glitch in the operating system or software to run an infecting code.
3. Ransomware code encrypts the data/information within the system.
4. The attacker will demand the ransom (cryptocurrency, \$) to release the data/information.

HOW TO KEEP SAFE:



Refrain from visiting suspicious websites.



Do not open suspicious emails or links.



Store data/information in appropriately secured file servers.



Do not use public Wi-Fi.

If you receive any suspicious emails, calls or sms immediately contact the IT Service Desk or cybersecurity@fedcourt.gov.au

LOCK UP BEFORE YOU GET UP



When leaving your desk, don't forget to lock your computer.

If you receive any suspicious emails, calls or sms immediately contact the IT Service Desk or cybersecurity@fedcourt.gov.au

WOULD IT BE BAD IF YOU LOST YOUR DOCUMENT? THEN PLEASE DO NOT SAVE IT LOCALLY.

Saving files only on your computer not only makes collaboration harder, it significantly increases the risk of data loss and data leak.

Save it on OneDrive instead.



If you receive any suspicious emails, calls or sms immediately contact the IT Service Desk or cybersecurity@fedcourt.gov.au

DO YOUR PART, BE CYBER SMART



Be careful of suspicious looking emails.



Don't use public Wi-Fi.



Don't leave your screen unlocked.



Use a strong unique password/passphrase.



Don't let anyone tailgate you into the building.



Don't plug in any unknown media devices (USBs).

If you receive any suspicious emails, calls or sms immediately contact the IT Service Desk or cybersecurity@fedcourt.gov.au

TRACTION

THE MORE, THE MERRIER
INVOLVE YOUR EMPLOYEES



General feedback;
Negative and Positive.



What would you like
to see more of?

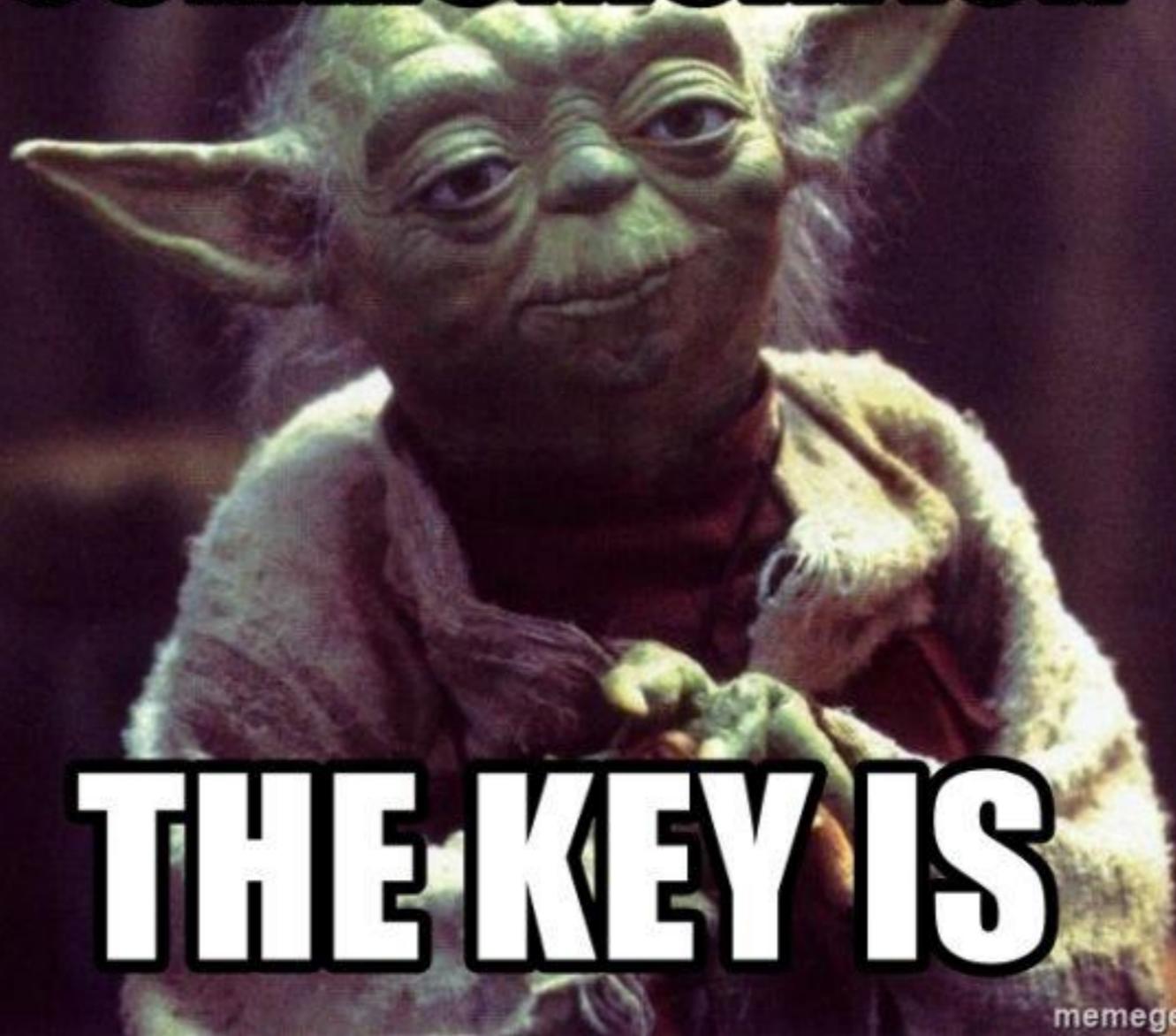


How can we help you
learn and become more
cyber aware?



Just like a PIR,
review your awareness
plan at least annually.

COMMUNICATION



memegenerator.net

Sp

Creat
engag
and b

pres
staff a



FEDERAL COURT
OF AUSTRALIA



THANK YOU

