

Cyber Security Fundamentals

While waiting for the session to start, please:

1. go to kahoot.it & enter the PIN 659 2370

2. go to menti.com & enter the code 2720 8690

TLP: AMBER

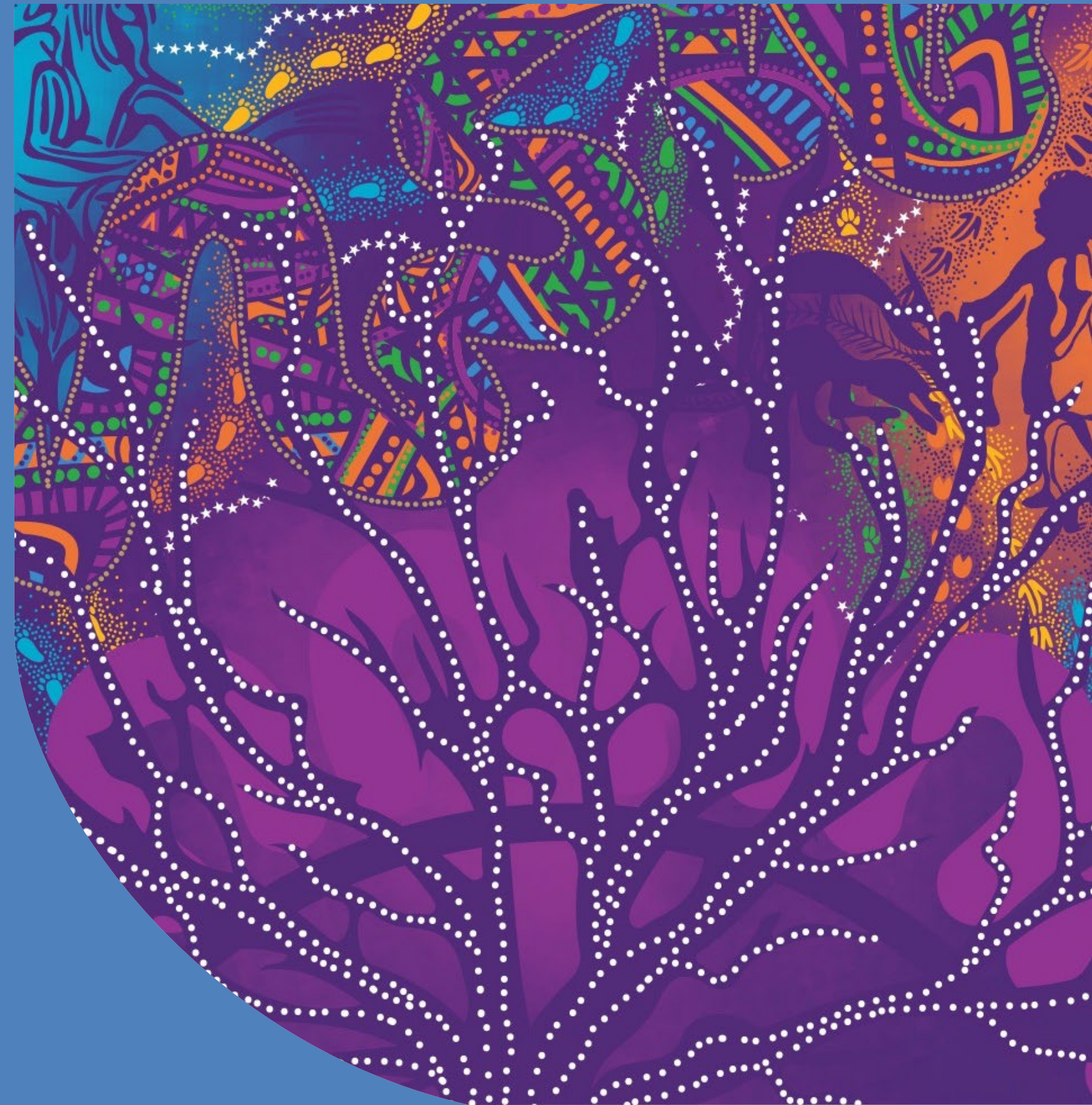


Acknowledgment of Country

AUSCERT through the University of Queensland (UQ) acknowledges the Traditional Owners and their custodianship of the lands on which we meet.

We pay our respects to their Ancestors and their descendants, who continue cultural and spiritual connections to Country.

We recognise their valuable contributions to Australian and global society.



A little about me – Mark Carey-Smith





alobe
alone

cepume

dloire

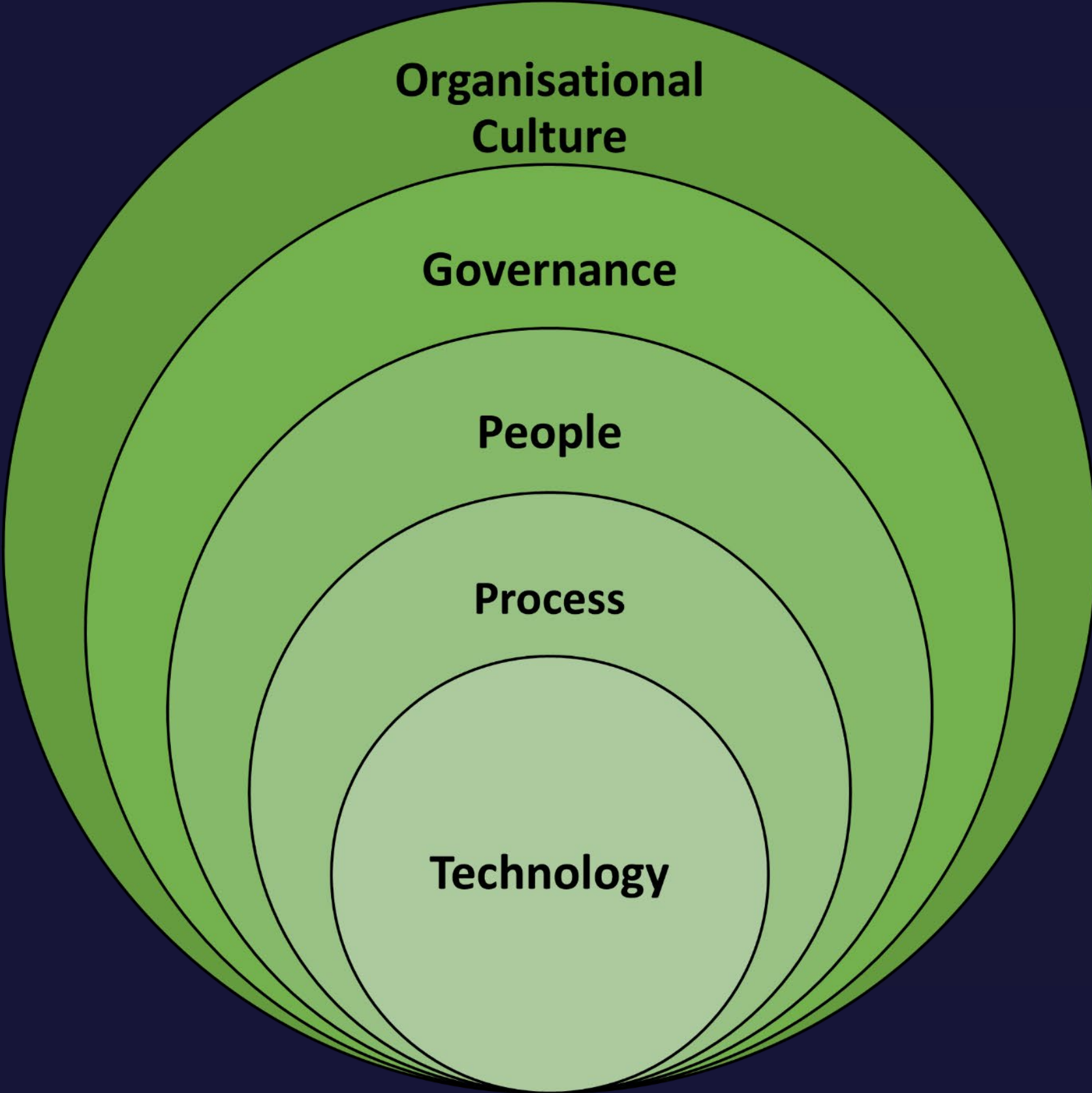
cure

oit

cloure

clube

What will you gain from today's information session?



Expectations

I will do my best to be entertaining and informative

I ask that you try hard to be curious, contribute your point of view and respect the opinions of others

If you have any questions please ask them at any time



Who is responsible for cyber security?

Let's do a quiz!

Technology can do amazing things but it can't do everything, the last line of defence is often you

Back to the quiz





Cyber hygiene – Situational awareness



TLP: AMBER



Cyber hygiene – Social Engineering

Back to the quiz!

Attackers are increasingly targeting people, rather than technology.

Phishing

Vishing?

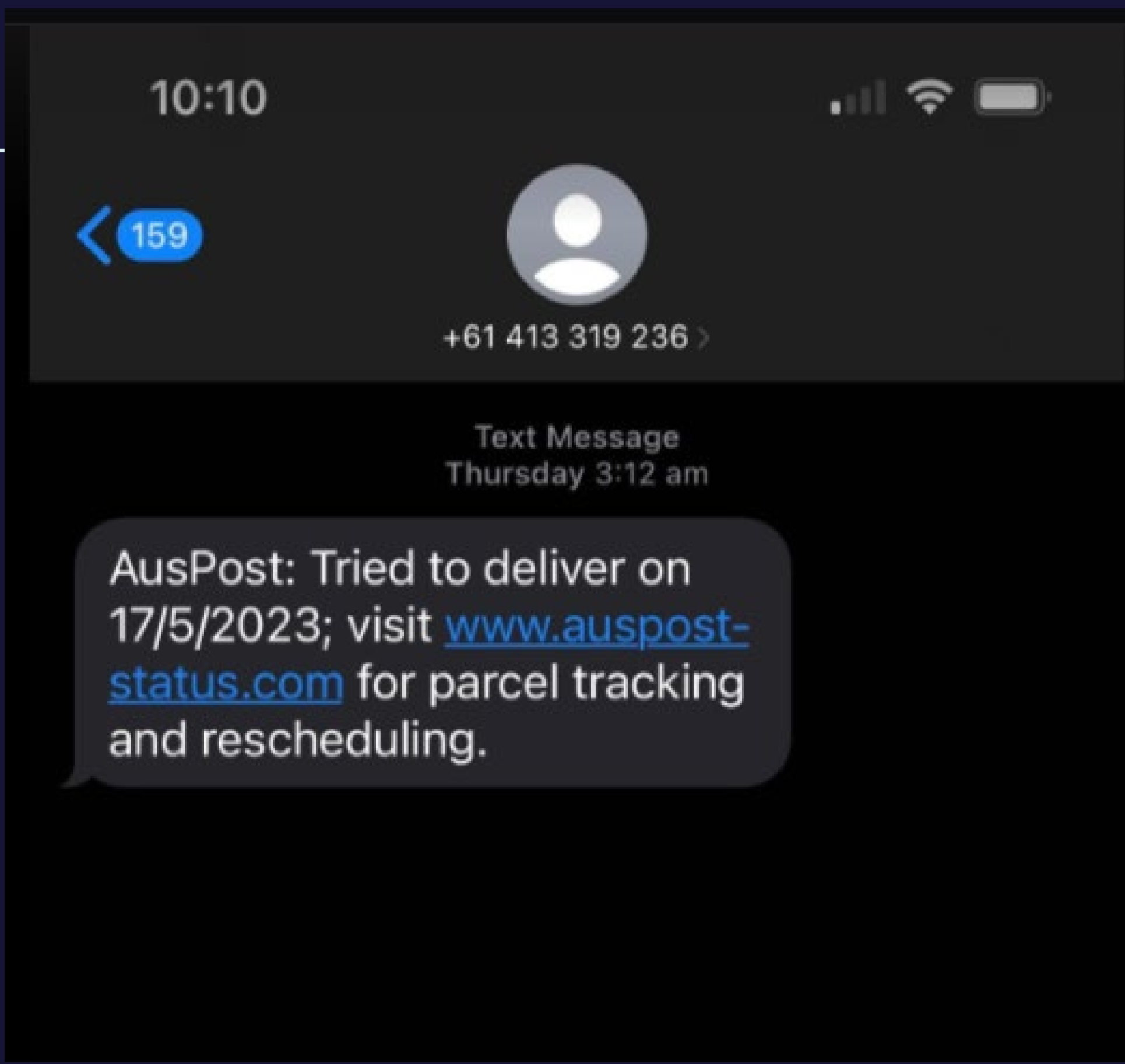
Smishing?

Quishing?

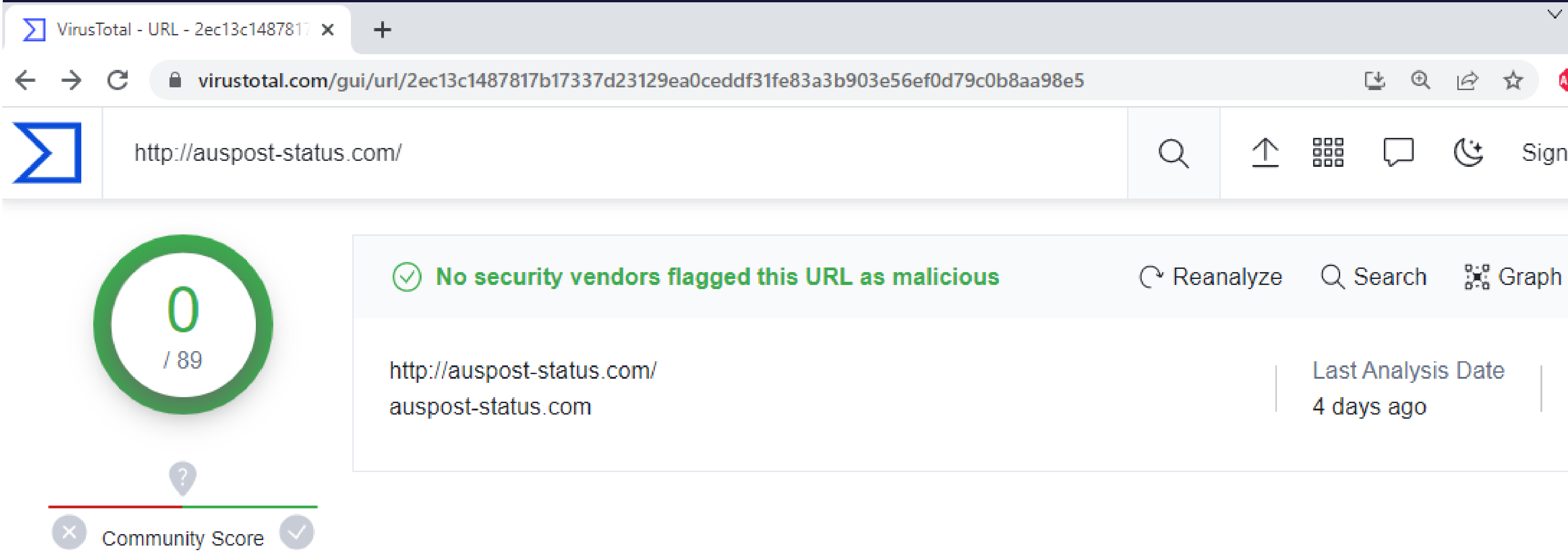
Dishing?



Cyber hygiene -



Cyber hygiene – Social Engineering



The screenshot shows a web browser window with a single tab titled "VirusTotal - URL - 2ec13c1487817". The address bar displays the URL "virustotal.com/gui/url/2ec13c1487817b17337d23129ea0ceddf31fe83a3b903e56ef0d79c0b8aa98e5". The main content area shows the analysis results for the URL "http://auspost-status.com/". A large green circle on the left contains the number "0" and the text "/ 89", representing the community score. To the right, a green checkmark icon is followed by the text "No security vendors flagged this URL as malicious". Below this, the URL "http://auspost-status.com/" is listed, and the "Last Analysis Date" is shown as "4 days ago". At the bottom left, there is a "Community Score" label with a close button (X) and a checkmark icon.

VirusTotal - URL - 2ec13c1487817 x +

virustotal.com/gui/url/2ec13c1487817b17337d23129ea0ceddf31fe83a3b903e56ef0d79c0b8aa98e5

http://auspost-status.com/

0 / 89

Community Score

✓ No security vendors flagged this URL as malicious

Reanalyze Search Graph

http://auspost-status.com/
auspost-status.com

Last Analysis Date
4 days ago

Cyber hygiene – Social Engineering – Attacker Techniques

D.A.N.C.E

Distraction - Attackers pull your focus in one direction so you don't notice or think about the thing they want you to miss

Appearance - Attackers 'blend in' and appear to be normal and trustworthy - and scam emails look legitimate

Need - The attack will make you want something and then provide the solution from a position of power or authority

Context - Attackers prefer places/situations/times of day when you are busy or stressed, and your guard is down

Emotion - Attackers rely on creating an emotional state such as panic or gratitude in their victim because emotions override rational thinking



Cyber hygiene – Social Engineering

Back to the quiz!

There are some great resources from [Scamwatch](#) and from [IDCare.org](#)

Phishing comes via any messaging app

If in doubt, don't open it, then report it

If you lose a device, report it



Cyber hygiene – Passwords

Let's watch a video:

<https://www.youtube.com/watch?v=x9LIqdUV09M>



Cyber hygiene – Passwords

What do you think are the most common passwords?

Now let's have a look at [a common password list](#)

The [haveIbeenpwned web site](#) is useful



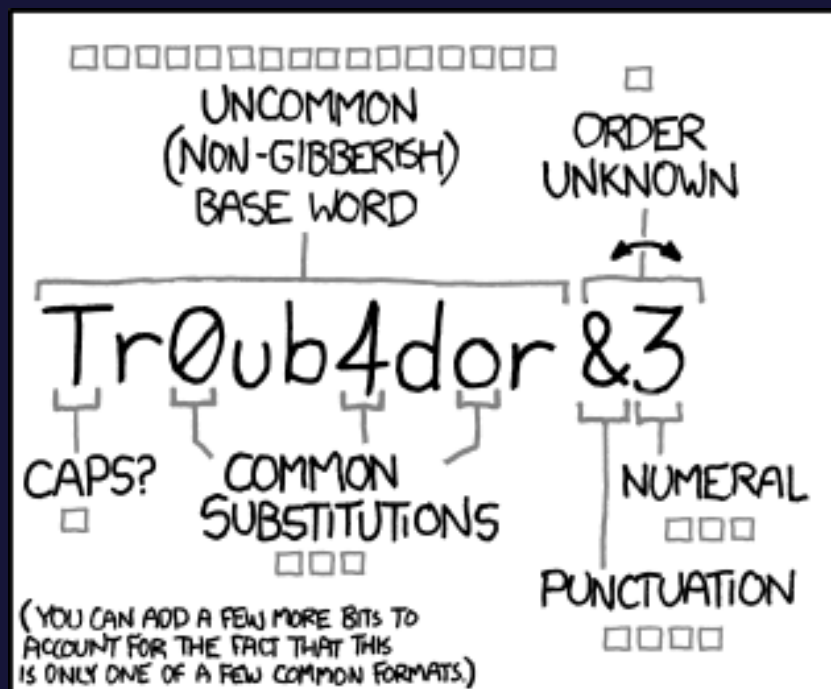
Habits and Switching Cost

Habits

Switching cost



Cyber hygiene – Passwords



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

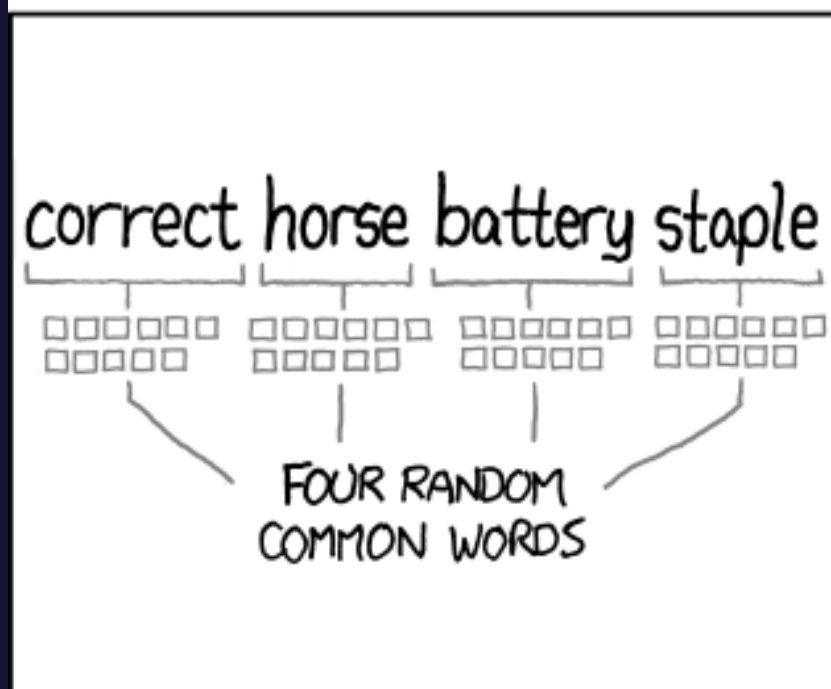
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Cyber hygiene – Passwords

Reducing the number of passwords to remember makes life easier, but...

What's an unsafe way to do that?

Back to the quiz



Cyber hygiene – Passwords

A safe and convenient solution to better passwords is to use a password manager

Used on computers and mobile devices

iOS devices have Keychain

TLP: AMBER



Cyber hygiene – Passwords – 2FA or MFA

MFA is not a panacea

Use caution when responding to prompts

TLP: AMBER

A login was detected, is this
you?

[REDACTED] ID

Browser

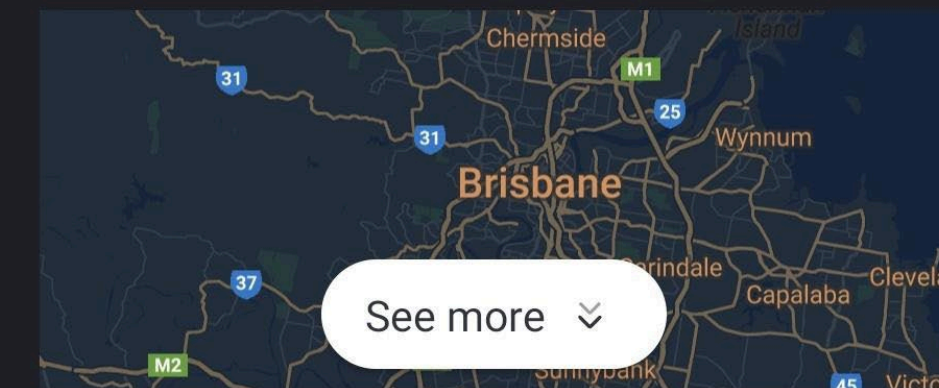
Chrome

Date and time

06 Sep 2024 02:43pm AEST

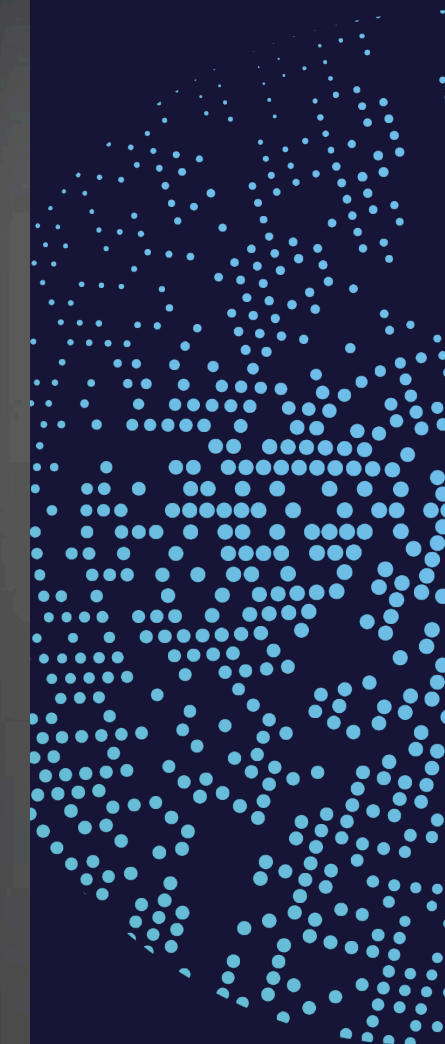
Near

Saintlucia, QLD, Australia



Yes, it's me

No, it's not me



Personal privacy - managing your digital footprint

Let's watch a video -

<https://www.youtube.com/watch?v=yvjT8m0hcKU>

What's going on here, why are the customers so surprised?



Personal privacy - managing your digital footprint

Personal privacy is about protecting the information that others collect about you

We can't stop it but we can reduce it:

- Assume everything posted is public

- Consider if you need to tell the truth

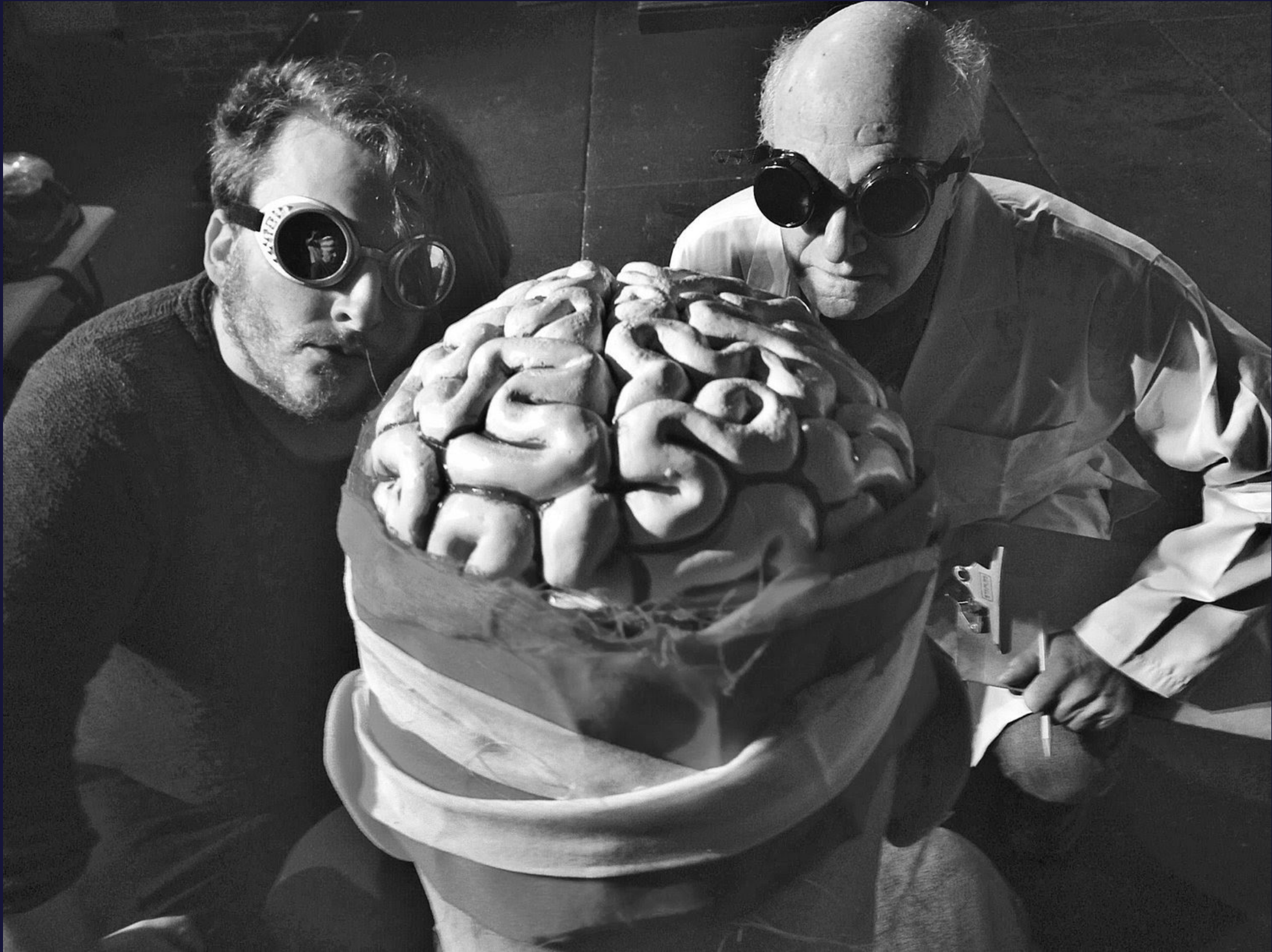
- Vote with your feet

- Be very careful with apps

- Review your apps every few months



We need to talk...about your brain



We need to talk...about your brain

Let's watch a video -

<https://www.youtube.com/watch?v=vJG698U2Mvo>

The video is an example of selective attention

Busy people notice fewer red flags

Slow down and stay safe

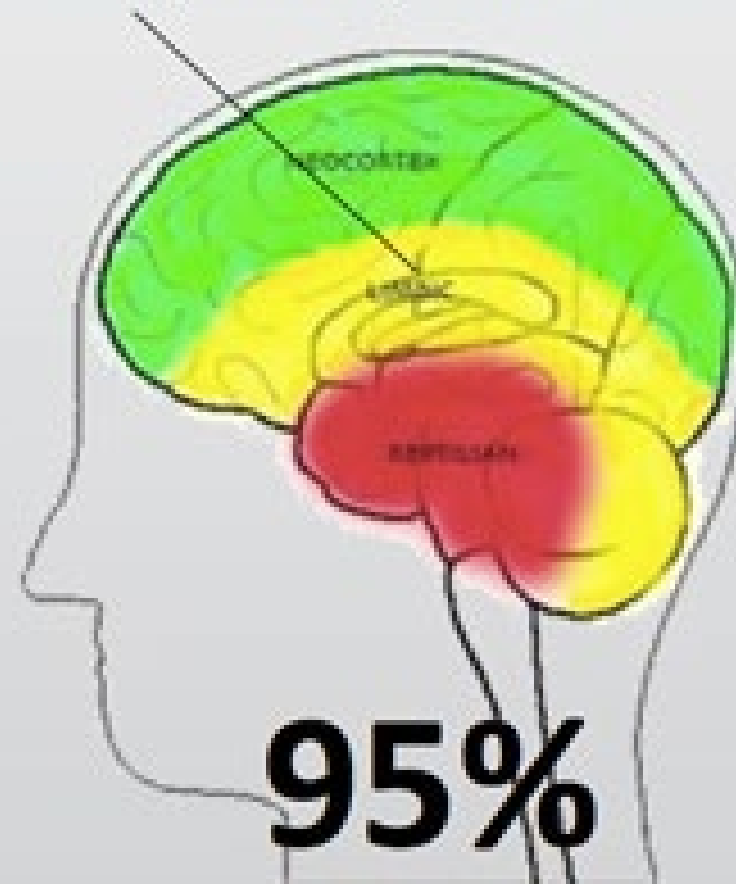


We need to talk...about your brain

SYSTEM 1 AND SYSTEM 2 PROCESSING

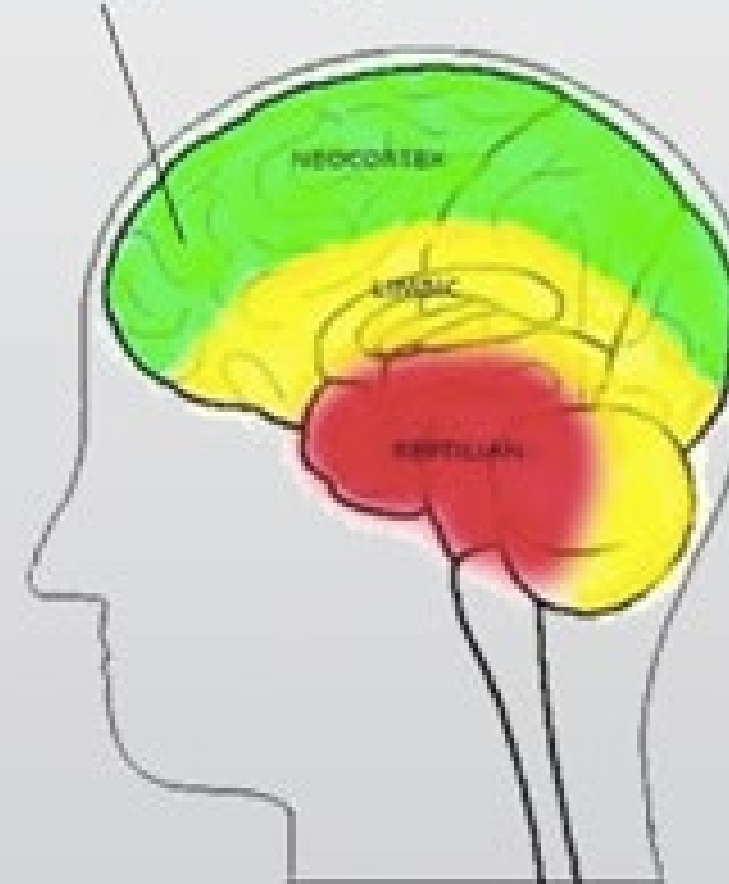
"FIRST REACTIONS"

System 1 = fast, automatic, impulsive, associative, **emotional**, and unconscious processing = limbic.



"THINKING"

System 2 = slower, conscious, reflective, deliberative, analytical, rational, logical processing = neocortex.



We need to talk...about your brain

System 1 (automatic) thinking keeps us alive

Let's go back to the quiz!









Small group exercise - OSINT and phishing

You are an attacker

You plan to use OSINT to find actionable information about your target; the CFO of UQ

You will attack them via phishing



Small group exercise - OSINT and phishing

Your objectives:

1. Determine what OSINT is available on your CFO.
2. Decide what OSINT will be useful for you as an attacker.
3. Create ideas for at least 3 different phishing lures.

You have 15 minutes, then we'll debrief as one group





Scam stats - Scamwatch

Reported losses

\$261,931,958.19

Reported scams

216,818

Top scams by loss



Investment

\$161,242,675



Romance

\$19,969,894



Phishing

\$15,093,998

Top contact methods



Email

75,144



Text message

72,370



Phone call

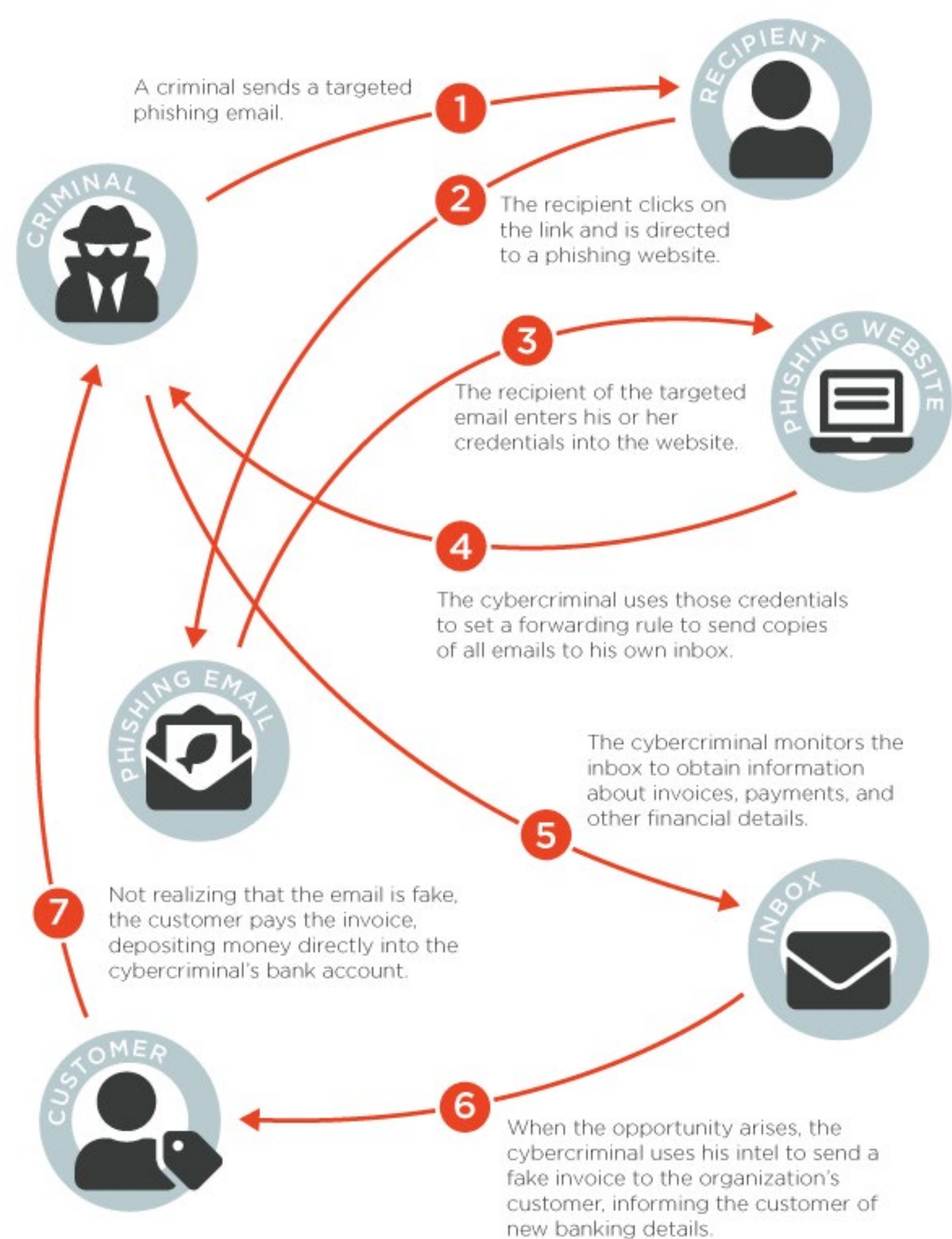
36,696

Business Email Compromise - BEC

BEC is a rapidly growing cyber crime

BEC scams target communications

Payment processes are a common target



Cyber hygiene – What does HTTPS actually mean?

🔒 <https://auscert.org.au>

80%



Subscribe for updates



Member Portal



Services ▾

Training ▾

Resources ▾

About Us

Contact

Become a member

Allies in Cyber Security



Incident
Support



Vulnerability
Management



Threat
Intelligence

membership inclusions



AFP

[Home](#)[Services](#)[About
us](#)[Crimes](#)[Jobs](#)[News
Centre](#)

28 JUNE 2024,
7:30AM

[Media Release](#)

Man charged over creation of 'evil twin' free WiFi networks to access personal data

Editor's note: [Footage of the man's arrest and on camera grabs by AFP Det-Insp Coleman available via Hightail](#)

The AFP has charged a West Australian man who allegedly established fake free WiFi access points, which mimicked legitimate networks, to capture personal data from unsuspecting victims who mistakenly connected to them.

The man, 42, is expected to appear in Perth Magistrates Court today (28 June, 2024) to face nine charges for alleged cybercrime offences.

Cyber Hygiene on the Move

Public WiFi is not safe (continued)

Use your phone as a hotspot instead

Set a PIN, or equivalent, on your phone



Cyber Hygiene at Home

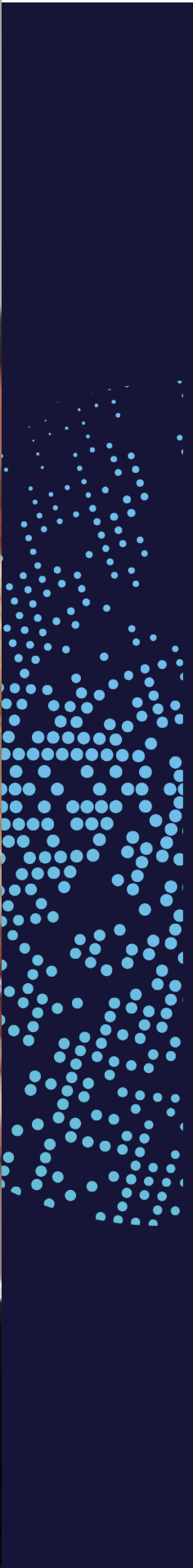
Change default passwords

Guests use the guest WiFi

Kids don't use your work device

There's smart and there's "smart"





Allies in Cyber Security



The University of Queensland | St Lucia, Q 4072 Australia

ABN: 63 842 912 684

t +61 7 3365 4417

e membership@auscert.org.au

w auscert.org.au

TLP: AMBER

