Stay Safe Online

✓ 1 Use a unique and strong passphrase on every account

✓ 2 Always set up multi-factor authentication

✓ 3 Install all software updates to keep your device secure

4 Check and update your privacy and location setting regular

5 Be cautious when using public Wi-Fi

6 Talk about how to be cyber secure with family and friends

7 Report Cyber attacks and incidents

Passwords & Passphrases:

To prevent password breaches:

- Do not reuse the same password
- Avoid sequential keyboard paths - **qwerty** or **password**
- Choose passwords or passphrases that are long (minimum 14 characters) with a combination of numbers, symbols, and uppercase and lowercase letters
- Four or more random words
- Different passphrase on every account

To create a strong passphrase:

- Think of a sentence that you can remember – To be or not to be (for shakespear’s fans)
- Add some uppercase letters – To Be Or Not To Be
- Remove the spaces: ToBeOrNotToBe-Hamlet
- Substitute numbers and symbols for some other letters - 2b0rNot2b-H@m!et

A password manager can help with creating or storing unique passphrases

Test your password hygiene

Test your password hygiene

- Attacks to gain personal and sensitive information are widespread and sophisticated. Every person could be a potential victim to a breach of their password. However, some are more at risk than others purely based on their password practices.

https://www.nsw.gov.au/id-support-nsw/be-prepared/passwords

Stay secure: update your device.

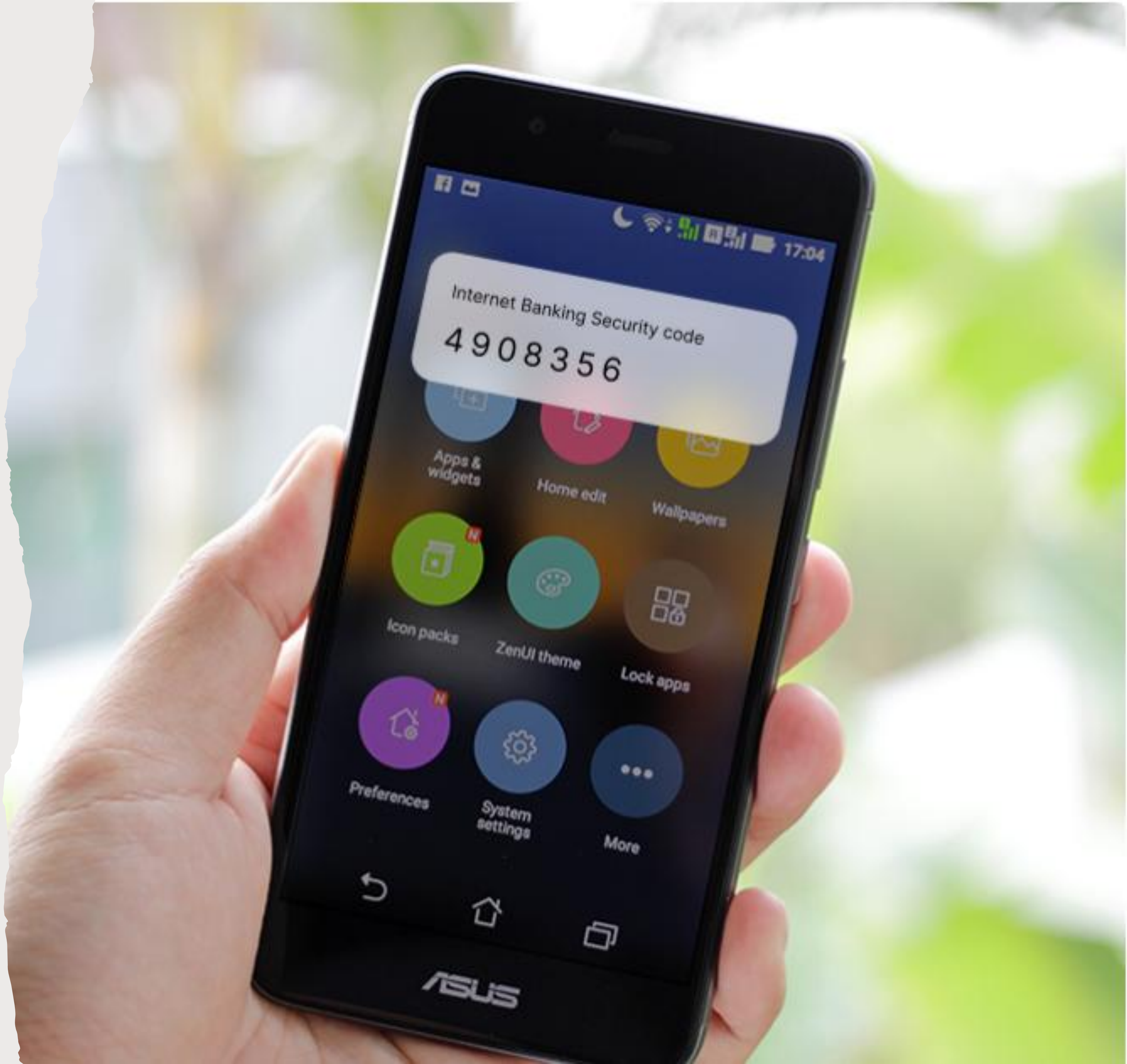
Install software updates as soon as they are available to keep your internet-connected devices secure.

Software updates are new, improved, or fixed versions of software or apps that can fix weak spots in security.

Make sure your device has **automatic updates** turned on so that you are notified when an update is available - don’t delay or ignore prompts to update.

Multi-factor authentication - MFA

- Sometimes strong passwords aren't enough. Multi-factor authentication (MFA) strengthens security by adding factors like biometrics, authenticator apps and email and SMS verification.
- Multi-factor authentication (MFA) combines something you know, have and are. For example:
  - **Know:** username and password
  - **Have:** mobile phone to receive a code by SMS
  - **Are:** Biometrics - facial recognition, voice recognition, retina scans, and fingerprint mapping.



MFA - ServiceNSW

SMS.

A one-time code , often referred to as a ‘one time PIN, is sent via SMS as part of Multi-Factor authentication (MFA). For Example, Service NSW may send you an SMS code that you must enter before logging, adding an extra layer of security to your account

ServiceNSW App.

Adds an extra layer of security when accessing government service online. After entering your username and password, a notification is sent to your registered ServiceNSW App, prompting you to approve the login.

Authenticator app.

A mobile application that generates a random one-time PIN or password. These can be stand-alone mobile apps or part of existing apps. The Google Authenticator or Microsoft Authenticator mobile apps are examples of these.

Pros and Cons

+	−
Easy to set up and use – no app installation required	**Less secure** than other methods – SMS can be intercepted via SMS swapping or other attacks
Works on any mobile phone that can receive text message	Requires mobile network coverage to receive code
Familiar to most users	May be delayed or undelivered in some areas or under poor signal conditions

+	−
More secure than SMS, using push notifications and app-based confirmation	Requires a smartphone and installation of the **Service NSW app.**
Integrated with the NSW Government ecosystem for a seamless user experience	Limited to services that support the app-based authentication
Fast and convenient—approve logins with a single tap.	App must be kept updated and notifications enabled.

+	−
Strong security—uses time-based one-time passwords (TOTP) that change every 30 seconds.	*Setup can be slightly **more technical** for non-technical users.
Does not rely on mobile network or SMS; works offline.	
Compatible with many online services beyond just Service NSW.	

eSafety Tip

Lost or stolen mobile phone

If your device is lost or stolen, call us on 13 77 88 or go to a service centre (https://www.service.nsw.gov.au/service-centre)

Contact

If you need help or have questions, call us on 13 77 88 or go to a service centre (https://www.service.nsw.gov.au/service-centre)

THANK YOU

Australian Government

Perhimpunan Indonesia - The Indonesian Association of NSW Inc.

WWW.ACTNOWSTAYSECURE.GOV.AU

PI_NSW@OUTLOOK.COM

WWW.MULTICULTURALINTEGRATIONNSW.ORG