Workshop 04 - Social Media and Online Safety

SLQ Wiki Fabrication Lab 2024/04/26 20:01

Workshop 04 - Social Media and Online Safety

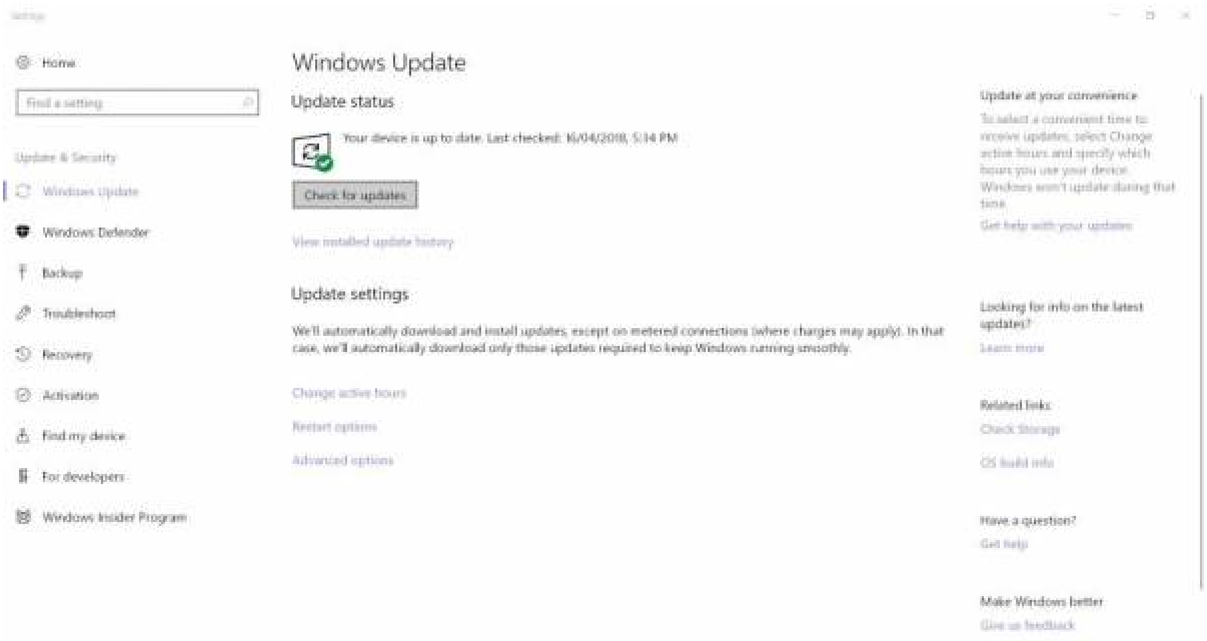
Here we will:

1. Secure your devices, connection, browser and accounts
2. Identify risky situations
3. Understand online privacy

Secure your Devices

Computer

- **Install only reputable software.** Do research first (especially if free).
- **Use secure passwords** and lock your device when unused.
- **Don’t leave it unattended in public.** Even if locked, it can be stolen.
- **Keep software updated** - security patches reduce vulnerabilities.


Windows Update

Update status

Your device is up to date. Last checked: 16/04/2018, 5:14 PM

Update settings

We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

Update at your convenience

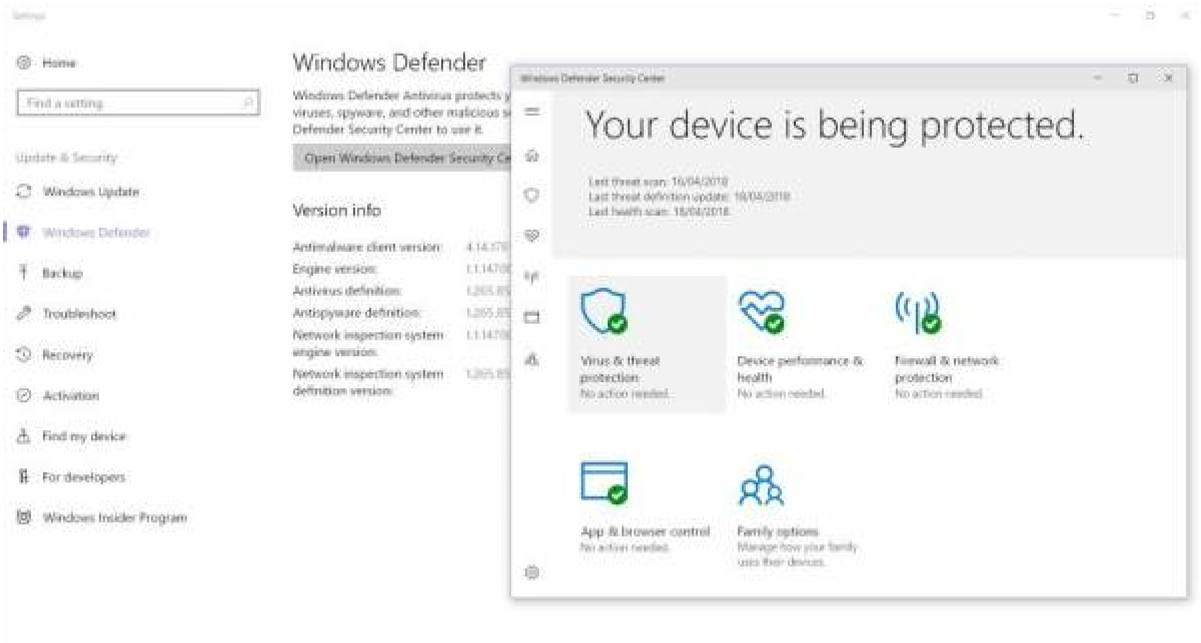
To select a convenient time to receive updates, select Change active hours and specify which hours you use your device. Windows won't update during that time.

Install a firewall. It's a barrier between your computer and others. You can authorise/deny access attempts.

Install anti-virus software (and anti-spyware if not already included). Examples of viruses and malware are:

- Keyloggers (records keystrokes)
- Ransomware (holds your system or details hostage)
- Worms (viruses that copies themselves to infect other devices)

- Trojan Horses (software that misleads about malicious intent)
- Rootkits (provides unauthorised system access)



Windows Defender

Windows Defender Antivirus protects y
viruses, spyware, and other malicious s
Defender Security Center to use it.

Version info

Antimalware client version: 4.14.17
Engine version: 1.1.1470
Antivirus definition: 1.265.85
Antispyware definition: 1.265.85
Network inspection system engine version: 1.1.1470
Network inspection system definition version: 1.265.85

Your device is being protected.

Last threat scan: 16/04/2018
Last threat definition update: 18/04/2018
Last health scan: 18/04/2018

Virus & threat protection
No action needed.

Device performance & health
No action needed.

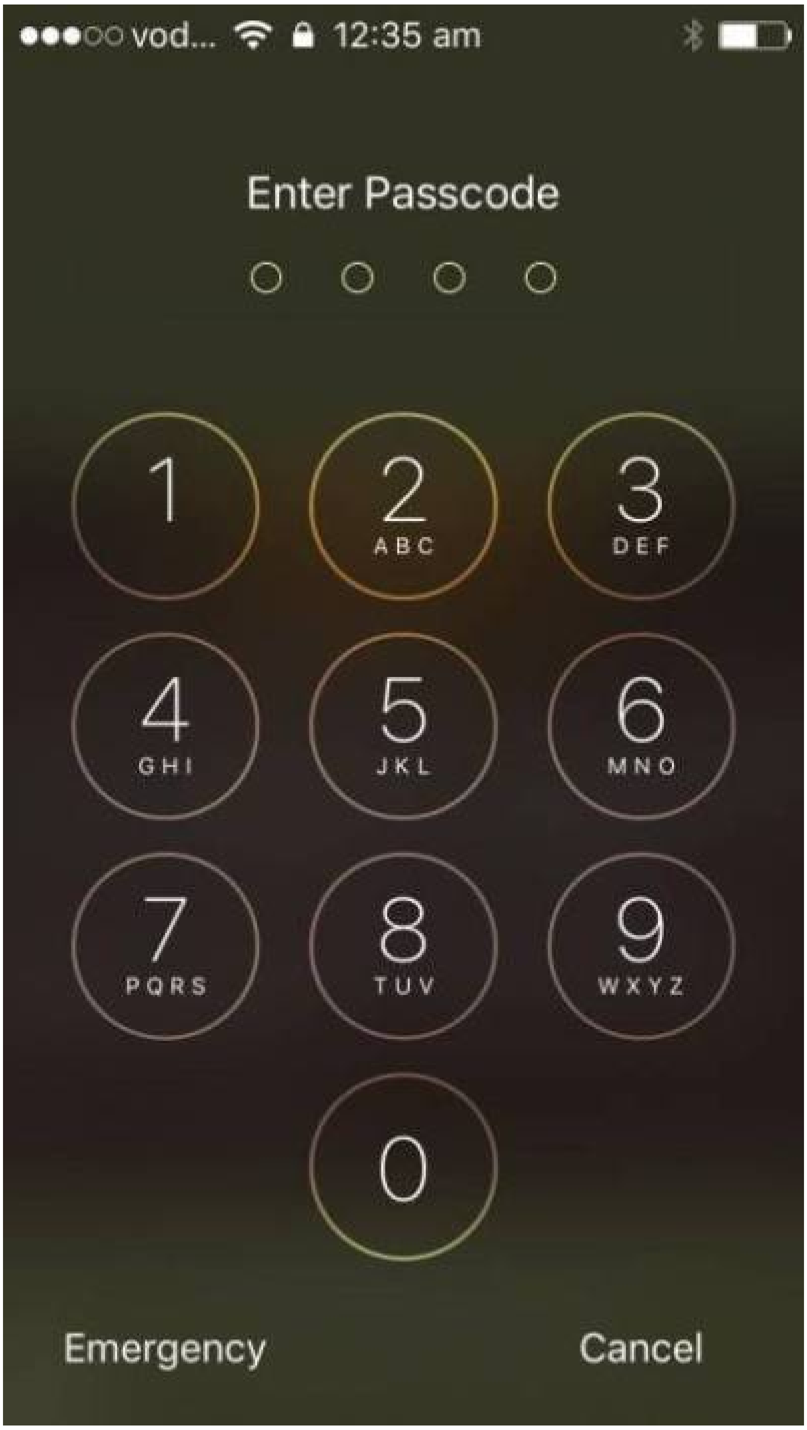
Firewall & network protection
No action needed.

App & browser control
No action needed.

Family options
Manage how your family uses their devices.

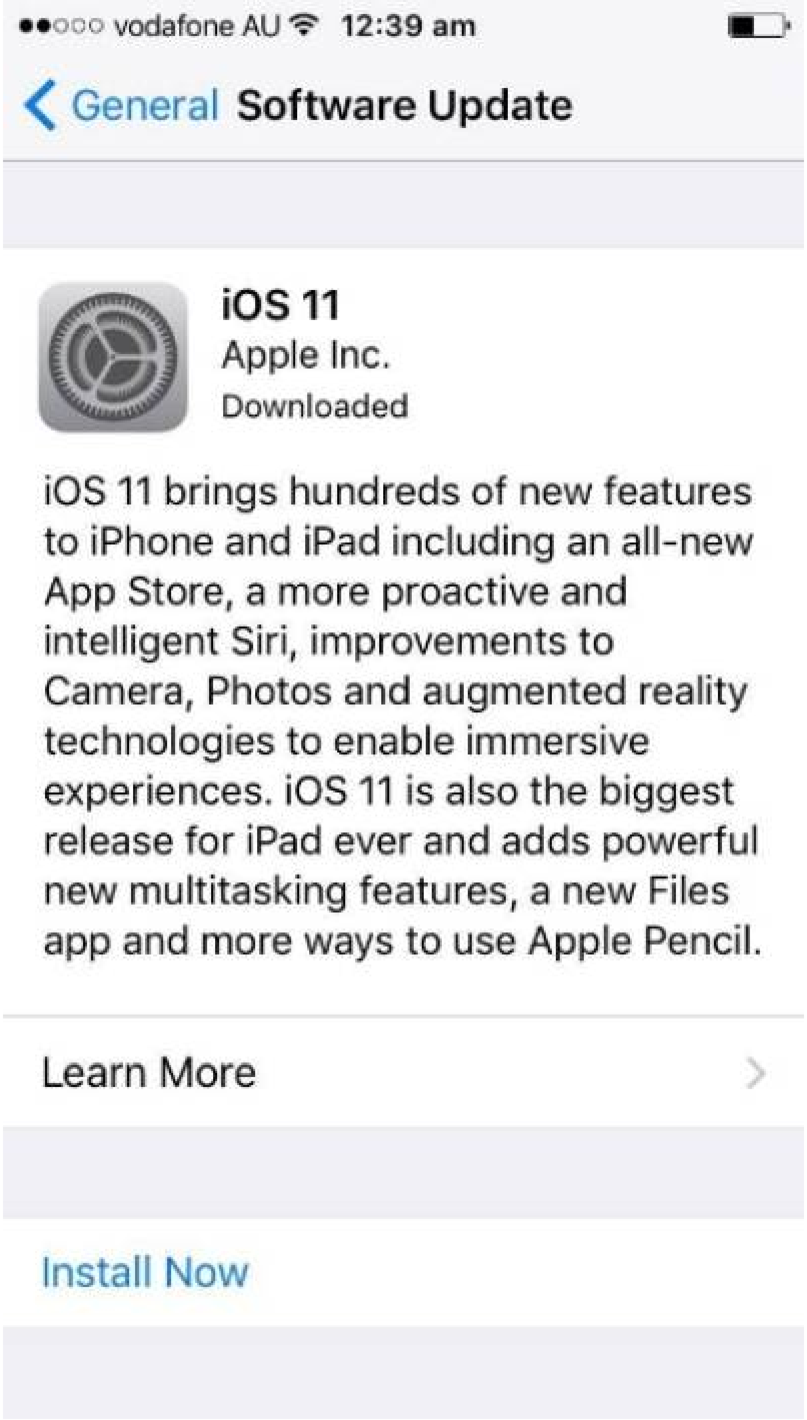
Phone

Use a password, pin or biometric data to lock your device when unused. Consider enabling device locking after a set time unused.



Don’t leave it unattended in public. Even if locked, it can be stolen. Do not lend it to others unless needed, and don't let it out of your sight if you do.

Keep software updated - security patches reduce vulnerabilities.

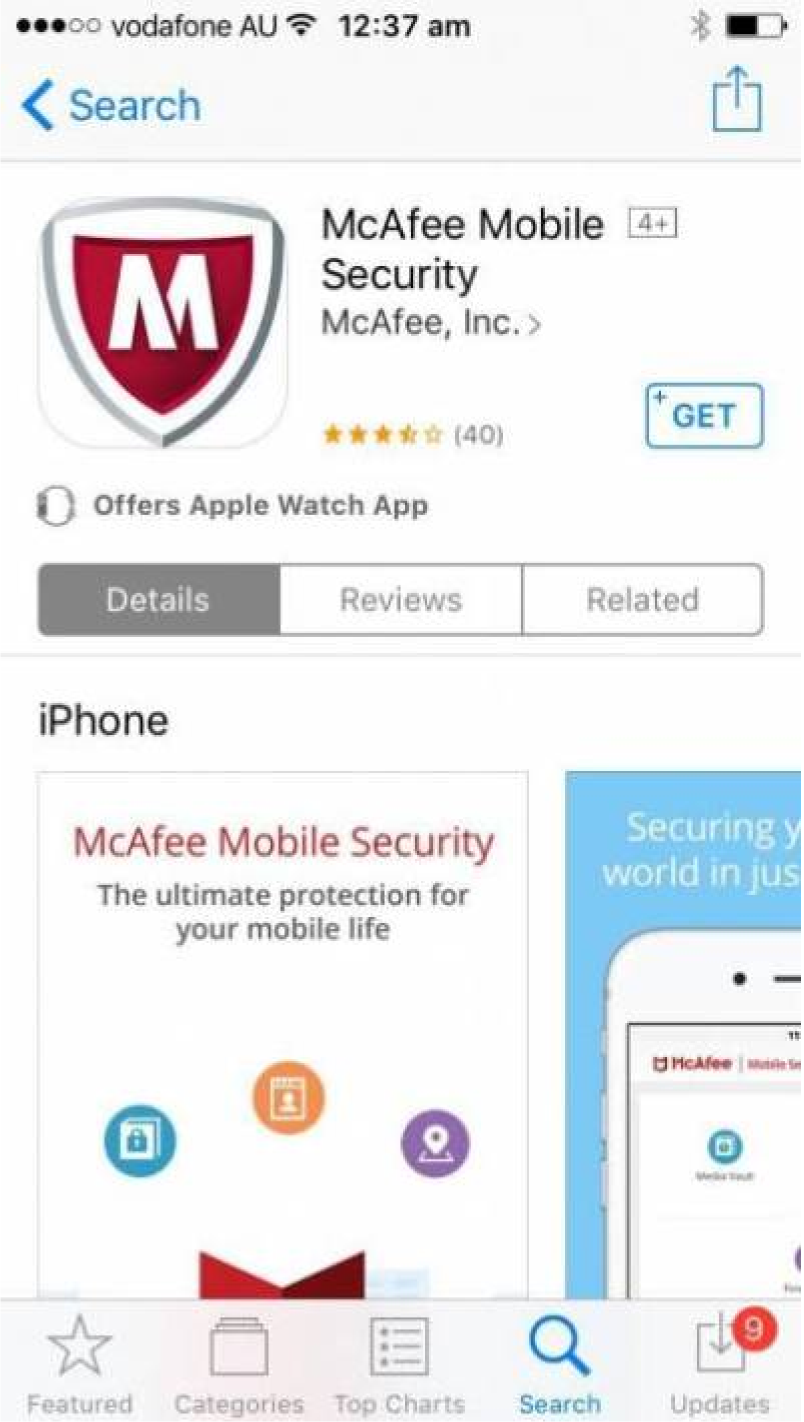


iOS 11
Apple Inc.
Downloaded

iOS 11 brings hundreds of new features to iPhone and iPad including an all-new App Store, a more proactive and intelligent Siri, improvements to Camera, Photos and augmented reality technologies to enable immersive experiences. iOS 11 is also the biggest release for iPad ever and adds powerful new multitasking features, a new Files app and more ways to use Apple Pencil.

Download reputable apps from trusted sources, eg. Google Play.

Install reputable security software with anti-virus and anti-loss capabilities.



●●●○○ vodafone AU 12:37 am

Search

McAfee Mobile Security 4+

McAfee, Inc. >

★★★★☆ (40)

GET

Offers Apple Watch App

Details | Reviews | Related

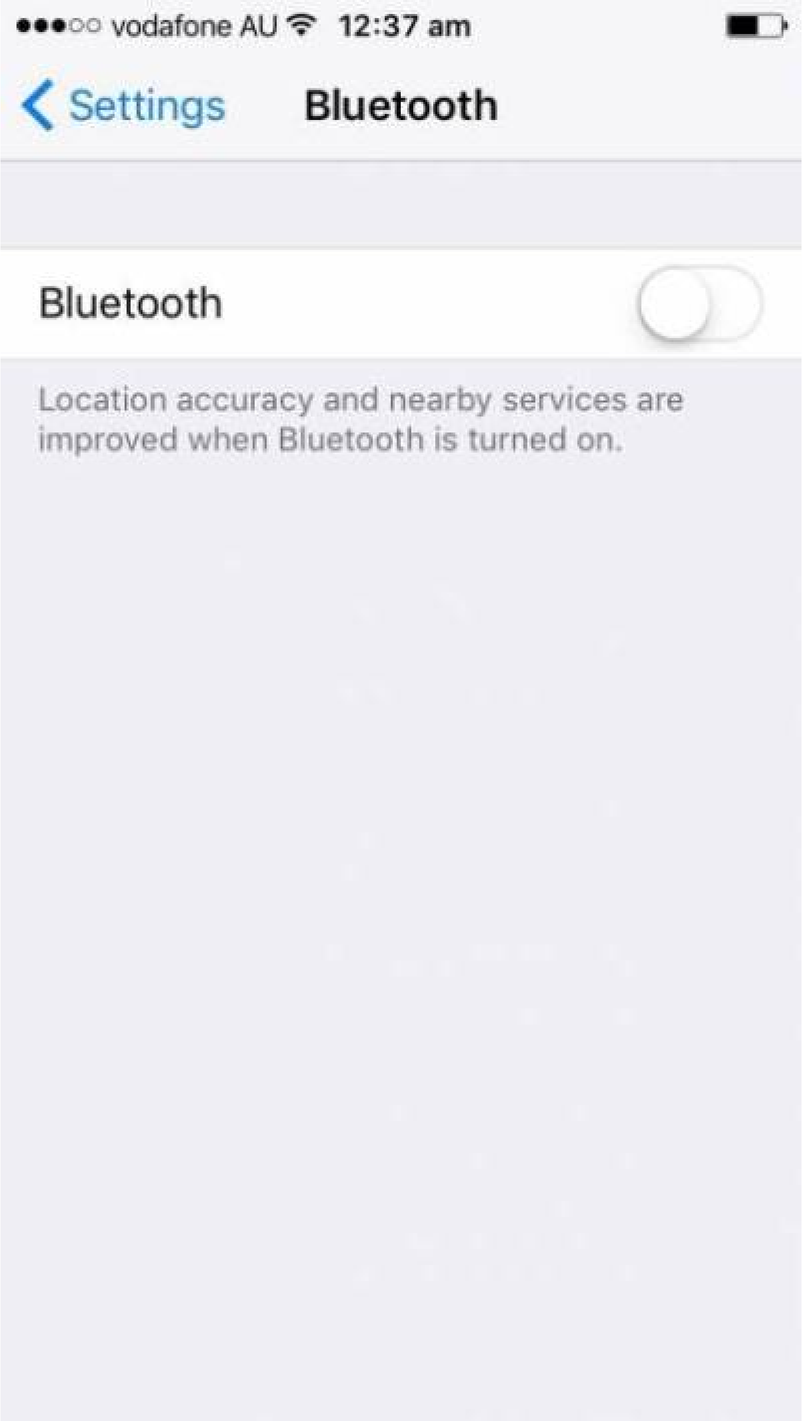
iPhone

McAfee Mobile Security

The ultimate protection for your mobile life

Securing y world in jus

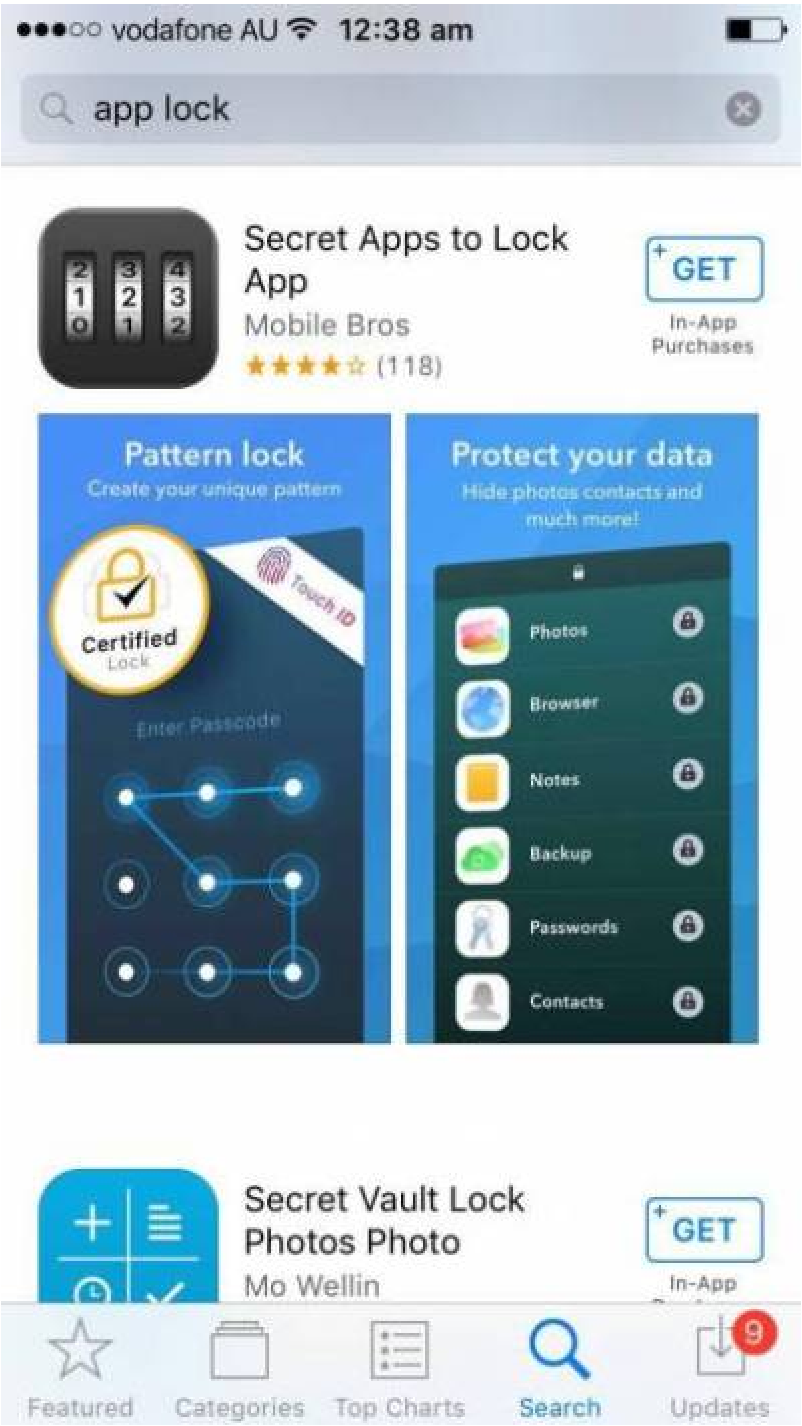
Keep Bluetooth off or hidden if not in use.



Bluetooth ○

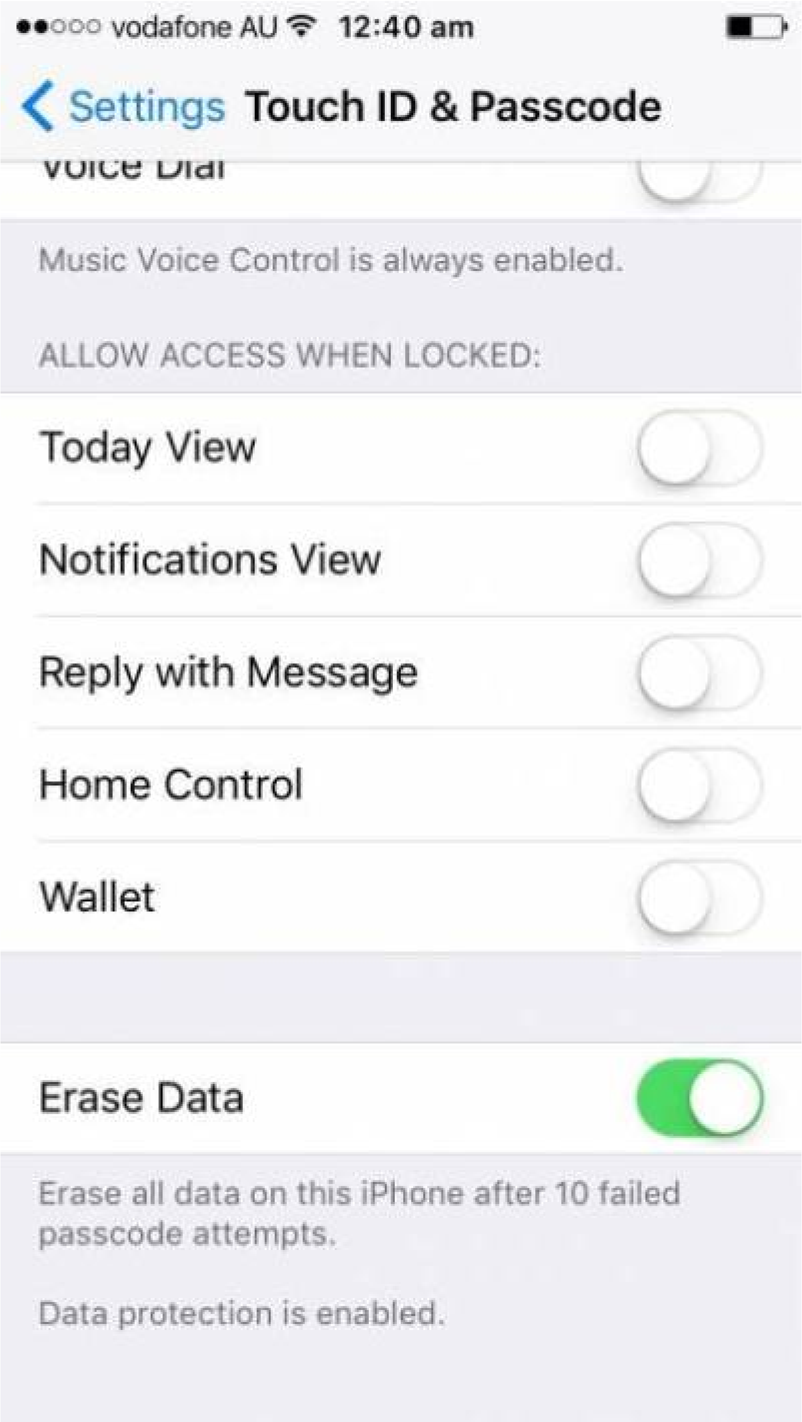
Location accuracy and nearby services are improved when Bluetooth is turned on.

Consider app-lock applications to protect unlocked access to apps with sensitive information.



app lock

Consider enabling remote locking and wiping so you can lock/wipe your phone from afar. Auto-wiping can remove data after a number of incorrect login attempts.



Voice Dial ○

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Today View ○

Notifications View ○

Reply with Message ○

Home Control ○

Wallet ○

Erase Data ●

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

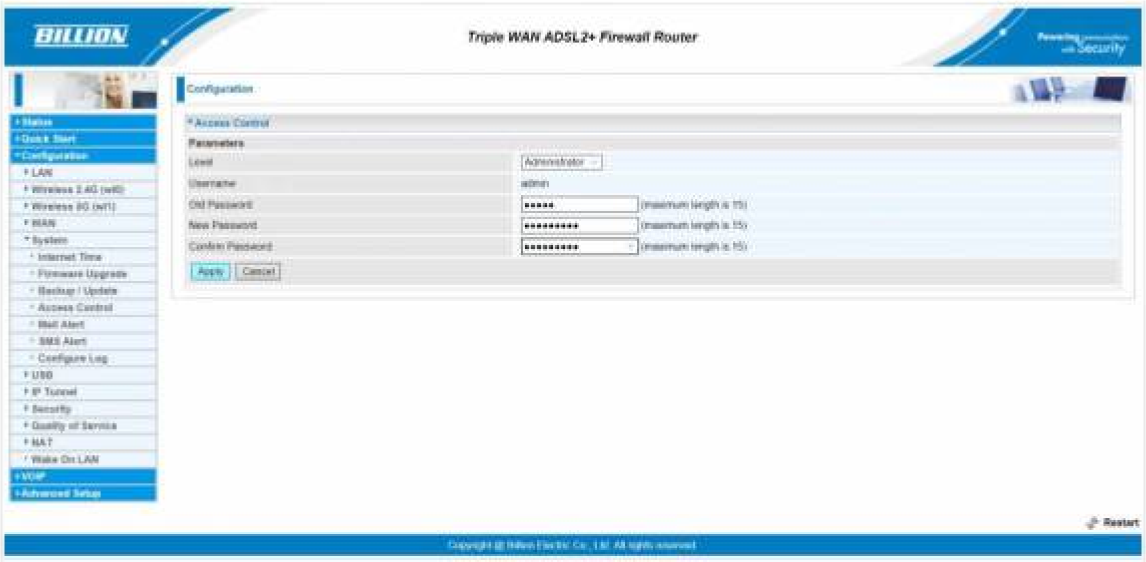
Consider adding emergency information to your lock screen. This could help it be returned if lost.

Secure your Connection

Home Wifi

Unsecured connections allow access to your devices/connection without permission.

Change the default administrator password on your router. - default passwords can sometimes be found online. Choose something strong instead.

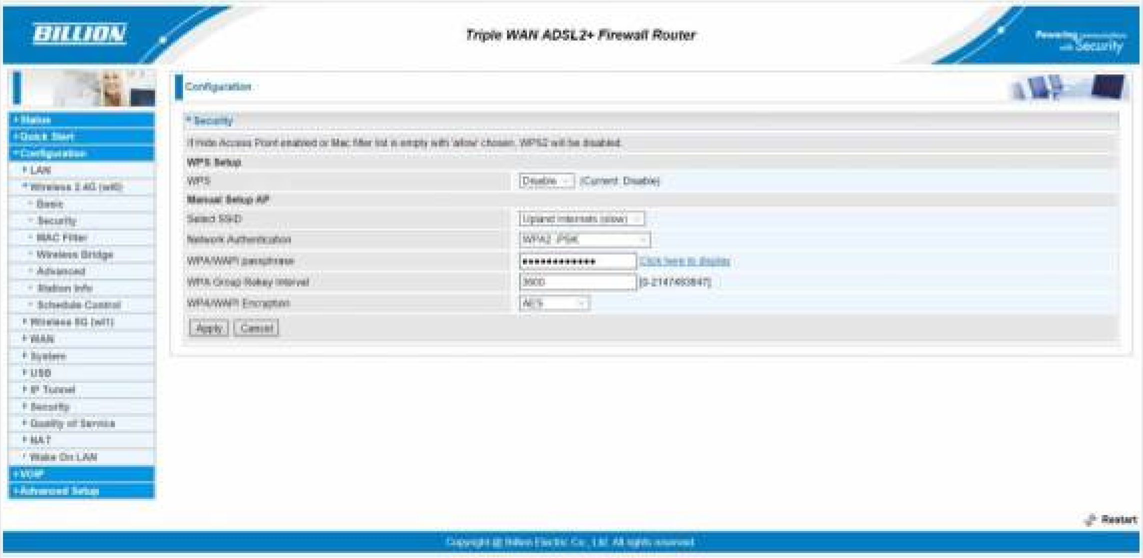


Access Control

Parameters

Level	Administrator	
Username	admin	
Old Password	•••••	(maximum length is 15)
New Password	••••••••••	(maximum length is 15)
Confirm Password	••••••••••	(maximum length is 15)

- **Disable remote router management** as this makes it easier for others to access.
- **Use strong encryption.** WPA2 is currently the strongest encryption protocol.
- **Give your SSID (Service Set Identifier) a unique, non-identifying name.** Eg, not ‘Billion7800N’ (default) or ’John Doe's Internet’ (personal information)
- **Set a strong Network Key** (your wifi password). To disable for existing users, change your SSID or Network Key.



Configuration

Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.

WPS Setup

WPS: Disable (Current: Disable)

Manual Setup AP

Select SSID: Upland Internats (slow)

Network Authentication: WPA2 -PSK

WPA/WAPI passphrase: ••••••••••••• Click here to display

WPA Group Rekey Interval: 3600 [0-2147483647]

WPA/WAPI Encryption: AES

Apply Cancel

- **Turn off open Guest Networks** - Only give access to trusted people.
- **Activate your router's firewall**.
- **Keep your router firmware updated.**
- **Disable WPS (Wifi Protected Setup) and remove access to router** as devices can be paired with some routers by pressing a router button.

Public Wifi

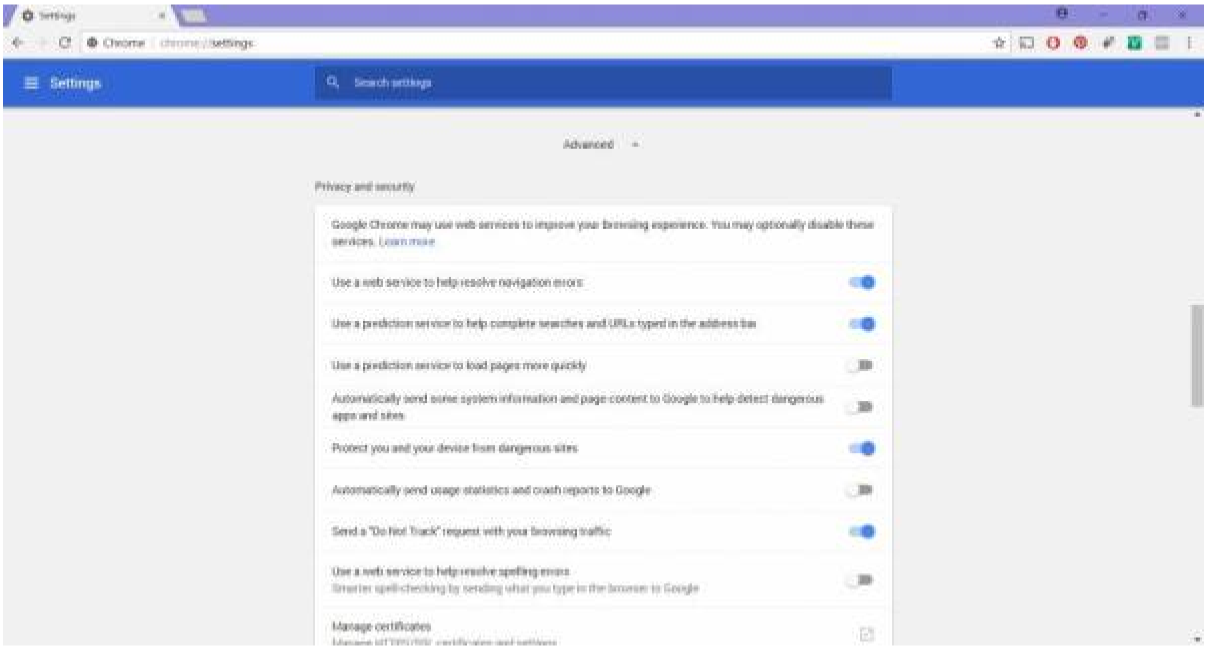
Free wifi can have security risks.

- **Only use wifi on networks you trust.** Eg, SLQ wifi. Avoid unknown networks. Verify network with staff first, if unsure.
- **Use password protected public wifi** over fully open networks.
- **If wifi use has a terms of service, read them.** Note how they use your data, content restrictions, etc.
- **Avoid sensitive data on public wifi**, eg. logging onto internet banking, etc.
- **Identify the network as 'public' on your device**. Turn off file sharing/location services.
- **Turn off wifi when not in use.**
- **Consider avoiding public wifi.** You can set up a 'hotspot' to use mobile data on other devices. Mobile hotspot setup varies by device.

Secure your Browsing

Internet Explorer is an identified security risk. Consider another browser where possible.

Browsers offer a number of security settings to configure. Sometimes these are under ‘advanced’ options.

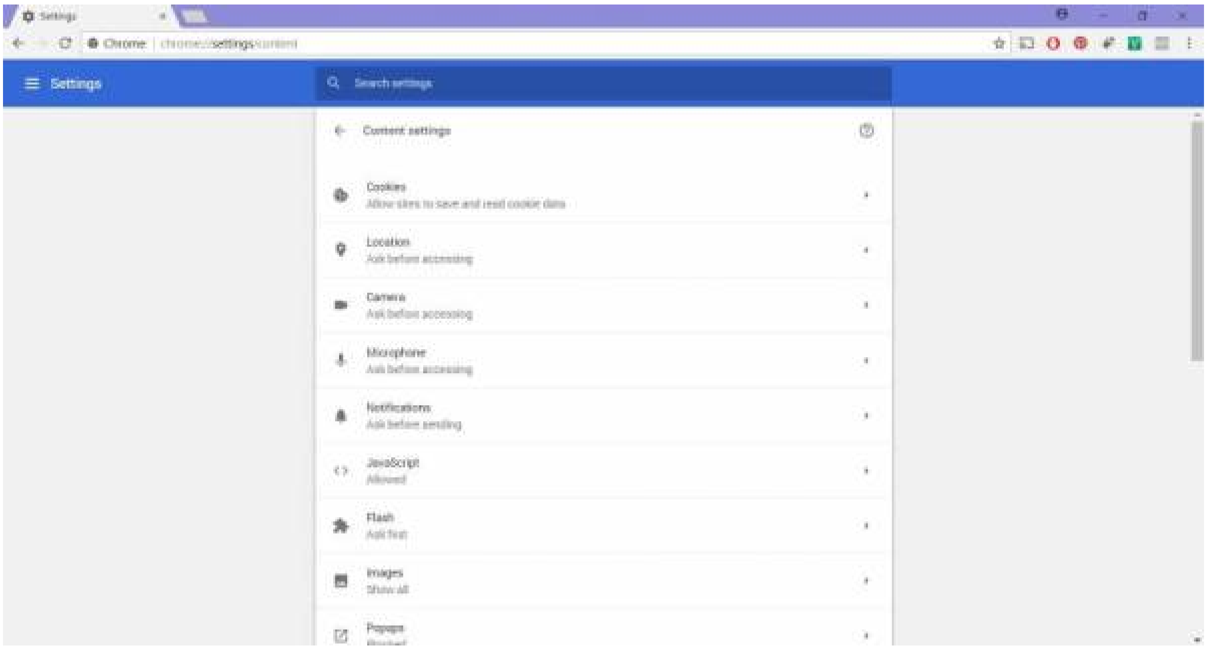


Advanced

Privacy and security

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

- Use a web service to help resolve navigation errors ●
- Use a prediction service to help complete searches and URLs typed in the address bar ●
- Use a prediction service to load pages more quickly ○
- Automatically send some system information and page content to Google to help detect dangerous apps and sites ○
- Protect you and your device from dangerous sites ●
- Automatically send usage statistics and crash reports to Google ○
- Send a "Do Not Track" request with your browsing traffic ●
- Use a web service to help resolve spelling errors ○
  Smarter spell-checking by sending what you type in the browser to Google
- Manage certificates
  Manage HTTPS/SSL certificates and settings



Content settings

- Cookies
  Allow sites to save and read cookie data
- Location
  Ask before accessing
- Camera
  Ask before accessing
- Microphone
  Ask before accessing
- Notifications
  Ask before sending
- JavaScript
  Allowed
- Flash
  Ask first
- Images
  Show all
- Popups
  Blocked

Some features may introduce vulnerabilities. You can turn these off, or turn them on only sometimes. Eg:

- **Cookies** store data for websites - eg, sites you visit or login credentials. If intercepted, attackers may access the information communicated.
- **Java** is used for active content on websites. Java applets usually have limited access to your system. Vulnerabilities could allow it to ignore these restrictions. Signed Java applets can ignore restrictions, but users often need to authorise them beforehand.
- **JavaScript** helps make websites interactive. JavaScript standards usually restrict features such as accessing local files.

Install only reputable browser plugins/extensions. Do you research first.

Always keep your browser updated. Security patches reduce vulnerabilities.

Don't enter sensitive information into a website without 'HTTPS:'. HTTPS: means it has a SSL (Secure Socket Connection) Certificate installed to encrypt traffic, so it is more secure.

- **Consider using a VPN (Virtual Private Network)** to encrypt your internet traffic.

Always pay attention to what you allow or restrict, including access to camera, microphone, location, etc.

Secure your Accounts

Strong passwords are your first line of defense. Consider reputable password manager software or make your own strong passwords.

Cyber-criminals can crack weak passwords easily:

- Brute force attacks test password combinations quickly
- Dictionary-based attacks test common words
- They can guess from personal information

Also pick a unique username. E.g. ‘admin’ is a very common username (so easy to guess).

Pick Passwords

Do use:

- Numbers, letters (upper and lower case), and symbols
- Something memorable, or use a password manager
- Long passwords – at least 8 characters

Don’t Use:

- Common words
- Easy to guess passwords (e.g. dog's name, your birthday)
- Repeated characters or predictable combinations (eg, 1234)

Easy Password Generation

1. Think of a sentence
2. Use part of each word
3. Substitute numbers, symbols and capitals.

E.g.:

1. Sentence: ‘**ilo**ve **int**erio**rd**e**s**i**gn**’.
2. Sentence fragments: **ilointrdsgn**
3. Substitution: **!lo1nTRdsgN**

Try it in a different language too!

Password Security

Make your passwords different If you use the same password everywhere, your information is more vulnerable.

This can be easy! Use extra letters to make them different. E.g.

- Gmail Password: 18**GIL**6SunD@e5
- Facebook Password: **FOK**186SunD@e5
- Twitter Password: 186SunD@e5**TW**

Do:

- Consider a password manager - paid software often has more options.
- Always log out after using accounts on shared computers.
- Use Two Factor Authentication.

Don't:

- Share passwords with others.
- Keep passwords in emails or easily found files.
- Use passwords on public networks/computers.
- ‘Save’ passwords unless you are the only device user.
- Enter your passwords through unsolicited emails/communication.
- Enter passwords on unsecured sites

If your account is used by someone else change your password/s immediately and/or perform a password recovery.

Password Recovery

When setting a password, you may need to provide a secret question and answer for password recovery. Eg:

- Your mother’s maiden name?

Use information only you know. If password recovery is weak, you are still vulnerable - especially if your email is compromised.

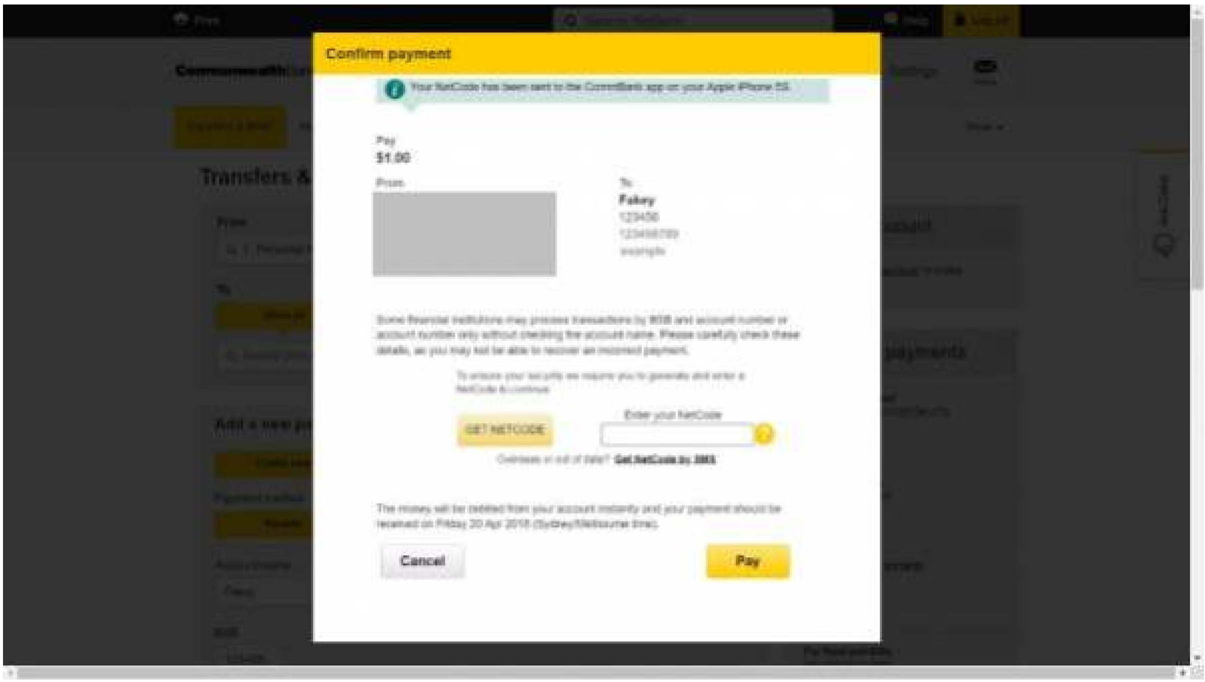
Using 2FA

2FA is Two Factor Authentication. Instead of one verification method (eg Username/Password), 2FA adds security with a second. Eg:

- something you **know** (eg a pin or password)
- something you **have** (e.g. a bank card or a mobile phone)
- something you **are** (e.g. a fingerprint)

Your accounts and transactions are more secure with 2FA.

Eg. This website sends a token via Push Notification:



Confirm payment

Your NetCode has been sent to the CommBank app on your Apple iPhone 5S

Pay
$1.00

From
[redacted]

To
Fakey
123456
123456789
example

Some financial institutions may process transactions by BSB and account number or account number only without checking the account name. Please carefully check these details, as you may not be able to recover an incorrect payment.

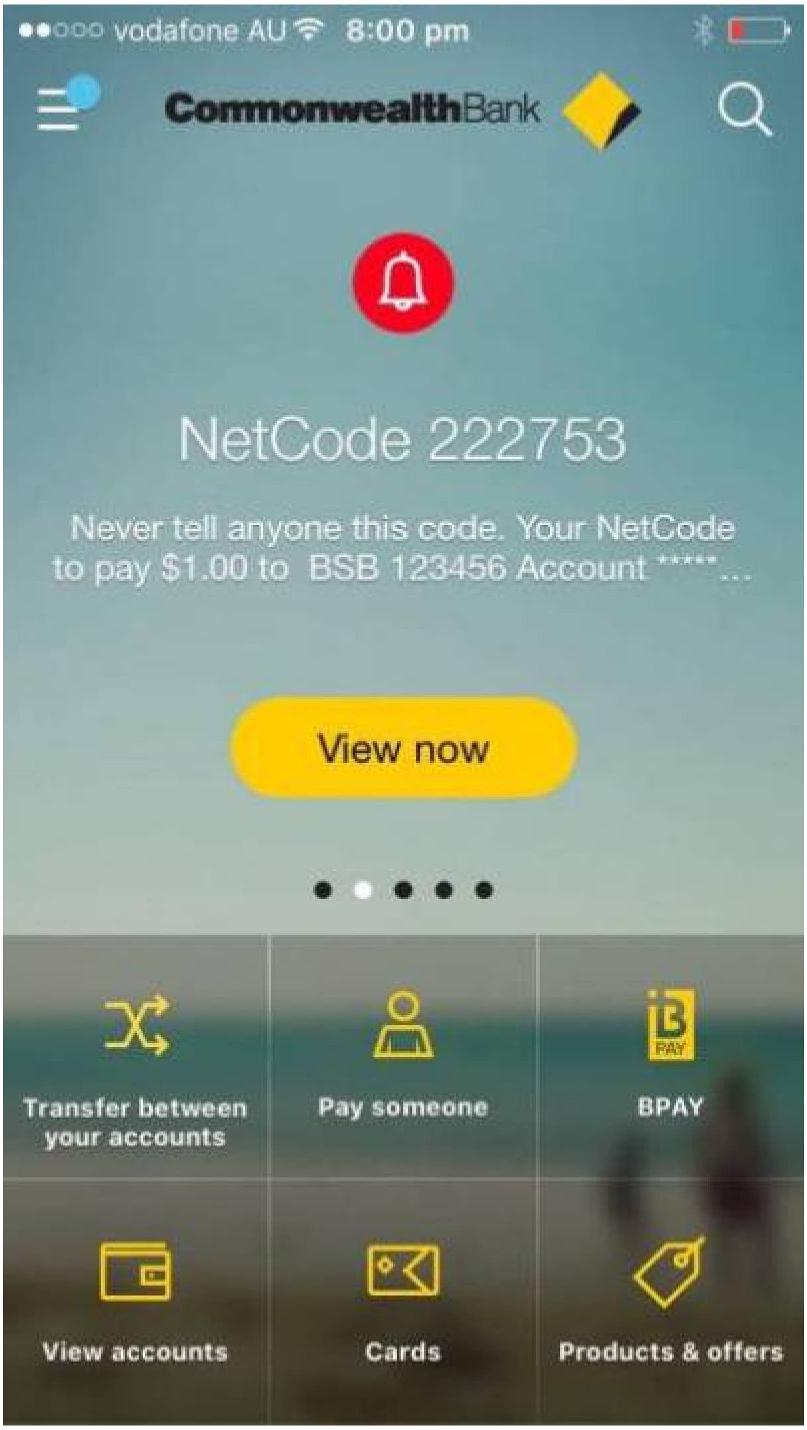
To ensure your security we require you to generate and enter a NetCode to continue.

Enter your NetCode

Overseas or out of date? Get NetCode by SMS

The money will be debited from your account instantly and your payment should be received on Friday 20 Apr 2018 (Sydney/Melbourne time).

You must enter the code to continue the transaction:



NetCode 222753

Never tell anyone this code. Your NetCode to pay $1.00 to BSB 123456 Account *****...

Two Factor Authentication reduces risk, but not entirely.

- Tokens sent by **push notifications** (from an app) are more secure than **SMS**.
- If you can't access to your phone/connection, you **can't access your accounts** that use phone 2FA.
- Your phone could be **lost or stolen**. Whoever has your unlocked phone could use your logged in accounts and phone 2FA methods.

Spot Risks/Scams

Scams cheat people out of information (for identity fraud), money, or other things. Learn about common scams at https://www.scamwatch.gov.au.

Example Video: https://www.youtube.com/watch?v=BL7WJM342Uc

Most importantly:

- Look for fakes (emails, calls, websites, etc)
- Don't click on untrustworthy links (websites, email attachments, shortened URLs, etc)
- Be cautious if asked for money, identity information, or account details

Premium Charge Scams

- Scammers text or call from unknown numbers and charge a premium rate if you text/call back.
- Random number generators can still contact your number (even if private)

Block problematic numbers. If compromised, contact your mobile provider - they might remove charges.

Remote Access Scams

Scammers call and claim to be from a company/tech service that needs to access your computer (often to 'fix' a non-existent problem or process a refund).

- Never give an unsolicited caller remote access to your computer. Real companies will not ask for this.
- Never give your personal or account details unless you made the call (or it's a verified legitimate call).

If compromised, seek help from a qualified computer technician, change account details and contact your payment method to reverse charges if possible.

Phishing

Phishing scams try to gain personal information (eg. login/credit card details/etc) often by pretending to be a trusted source.

Eg, **calls or emails** claiming to be from a bank or other institution asking for details to secure your account.

They are often designed to scare (eg. 'Centrelink' asking to confirm details or they'll stop payment). Others might pretend to offer a prize or similar.

- Check to see if calls are from verifiable numbers and emails are from official addresses (should be listed on website)
- Check emails against real ones. Are there formatting, grammar or spelling errors? Don't click suspicious links or open unknown attachments.
- Check website addresses. Are they different from normal? (eg. commmbank.com vs commbank.com.au)
- Never provide personal details to unsolicited contact claiming to be from banks, ATO, etc.
- **Real companies and institutions will not threaten or verbally abuse you.**

If compromised, change your account information immediately, and contact the real company/institution to secure your details.

Buying/Selling

When buying from individual sellers:

- If something seems too good to be true, **it usually is**. Eg, low cost cars or property you cannot inspect before purchase.
- See items in person, check seller reviews, and use payment methods with fraud protection (e.g. Paypal Goods and Services).

When buying from stores:

- Fake online stores easy for scammers to create, as seen here: https://www.youtube.com/watch?v=3IluT4Jo4f8
- Check that their business registration and contact details are real before transacting.
- Check that privacy/refund/returns policies comply with local laws.
- If prices are 'too' good, you may receive imitation products (or nothing at all).
- If a credit card gateway is used, is it trusted/secure? Only use payment methods including fraud protection.

When selling:

- Document items thoroughly and send **with** tracking (in case disputes are raised seeking refunds through Paypal etc).
- Don't send until payments have cleared.
- Do not delete original advertisement until well after transaction date.
- Do not accept overpayment for item and 'refund' the difference (it's a common scam).

If compromised while using a payment method with fraud protection (eg, credit card or Paypal), you may be able to arrange a charge-back. Also contact your Consumer Protection Agency (eg, the Office of Fair Trading: https://www.qld.gov.au/law/fair-trading)

Socialising Online

Some social media memes ask **personally identifying questions** that can be used for **identity fraud** - eg, 'name creators' that use your birthdate/street you grew up on to make a name).

Be cautious of **'catfishing'** (fake profiles to take advantage of you, often on dating sites). ACCC example video: https://youtu.be/YDt0F7ETmRU

- They seem to develop strong feelings quickly, and want you to trust them.
- Often ask for gifts, money or personal details (sometimes with a sad story).
- Do a 'reverse image search' – they often use random pictures to build ‘real’ looking profiles.

They may also pretend to be family or friends with fake profiles or compromised accounts. Eg:

- May claim to need money while stuck overseas (which seems real because it's from a 'trusted person')
- Confirm facts using a different method – e.g. telephoning them.
- **If in doubt, say no.**

What if I'm scammed?

- Contact your financial institution, affected account providers and/or local consumer protection agency
- Change your passwords
- Recover your stolen identity
- Report scams to the authorities
- Get help from Australian agencies

More Information: https://www.scamwatch.gov.au/get-help/where-to-get-help

Privacy Controls

Privacy controls where your information is displayed and who sees it.

Some information you give intentionally. Eg, Your details to open an account. This is **Personally Identifying Information**.

Other information you might not realise you’re sharing – Eg, shopping habits or search history. This **Non-Personally Identifying Information** is connected to 'someone’, but not specifically you.

Who Owns your Data?

Video explanation: https://www.youtube.com/watch?v=y1txYjoSQQc

Information may be *about* you, but it is not owned *by* you.

1. Check **terms and conditions** and **privacy policies** before using a service.
2. Check how your data is used.
3. Often we **give our data** to **get a service**. Eg. Facebook receives permission to use data for advertising when you join.

Secure your data

- **Limit information you share online.**
- **Birthdates are often used in 2FA** so **don't tell everyone**
- **Secure your connection and browsing** – see steps above.
- **Review and amend your privacy settings as needed**.
- **Think before accepting cookies.** Cookies can track information like login details or browsing history.
- Consider **deleting data** and accounts you no longer need.

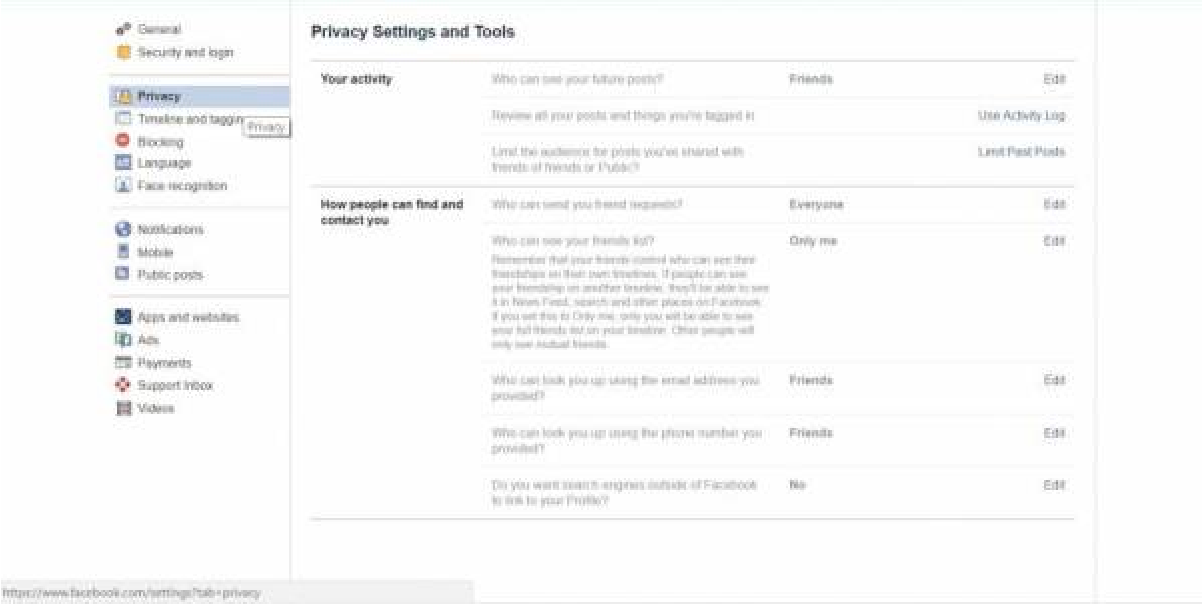
Social Media Privacy

Each social media platform has its own terms of service and privacy options. Review these before **and during** use of these platforms.

You can often Google guides on how to navigate privacy on each platform. We'll look at Facebook's settings today.

Facebook

Facebook's account privacy options can be adjusted in 'Settings':

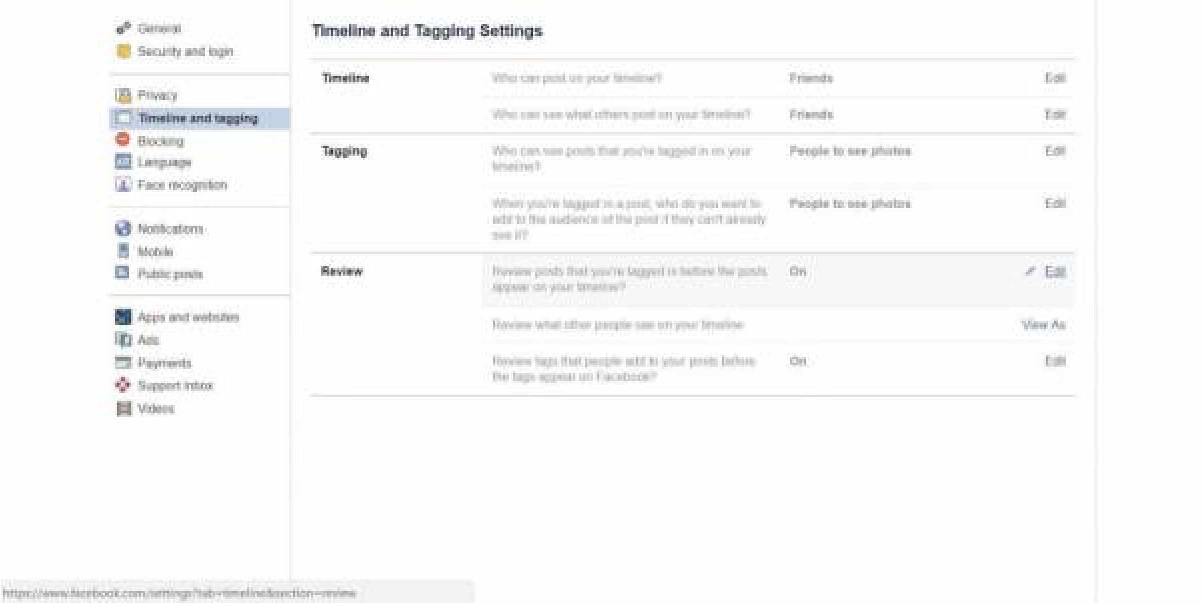


Privacy Settings and Tools

Your activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How people can find and contact you	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list? Remember that your friends control who can see their friendships on their own timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will only see mutual friends.	Only me	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit

https://www.facebook.com/settings?tab=privacy

Timeline and tagging restricts who sees your content or can 'tag' you. Lists allow you to restrict these to specific people.

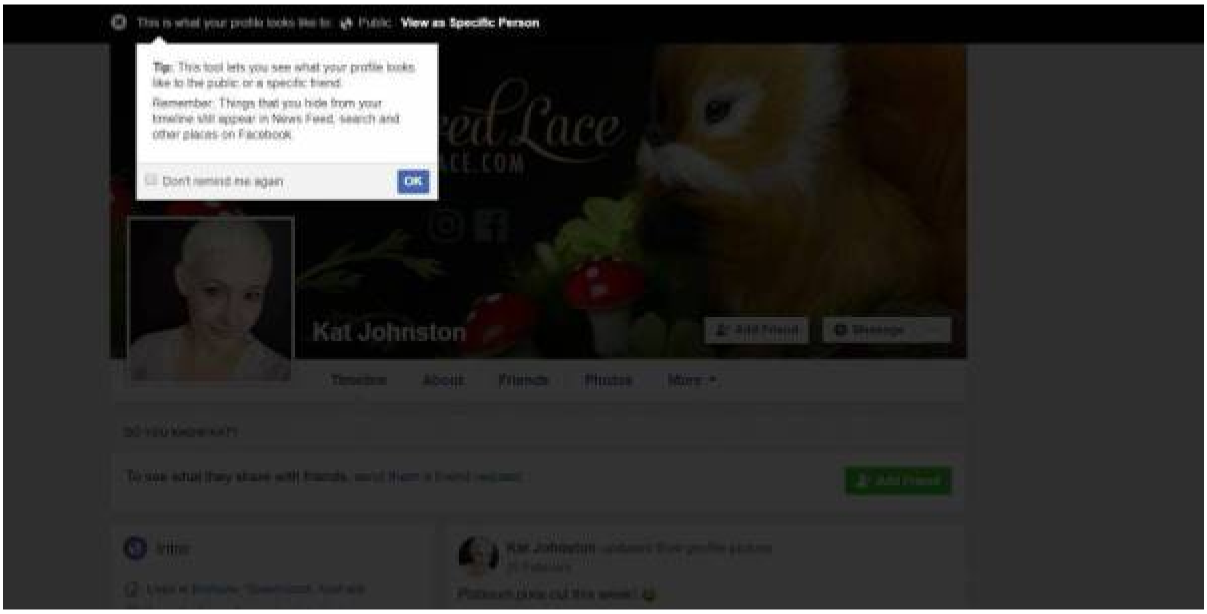


Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
Tagging	Who can see posts that you're tagged in on your timeline?	People to see photos	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	People to see photos	Edit
Review	Review posts that you're tagged in before the posts appear on your timeline?	On	Edit
	Review what other people see on your timeline		View As
	Review tags that people add to your posts before the tags appear on Facebook?	On	Edit

https://www.facebook.com/settings?tab=timeline&section=review

Review what other people see on your timeline: view as a general user, or specific person.



This is what your profile looks like to: Public View as Specific Person

Tip: This tool lets you see what your profile looks like to the public or a specific friend.

Remember: Things that you hide from your timeline still appear in News Feed, search and other places on Facebook.

□ Don't remind me again OK

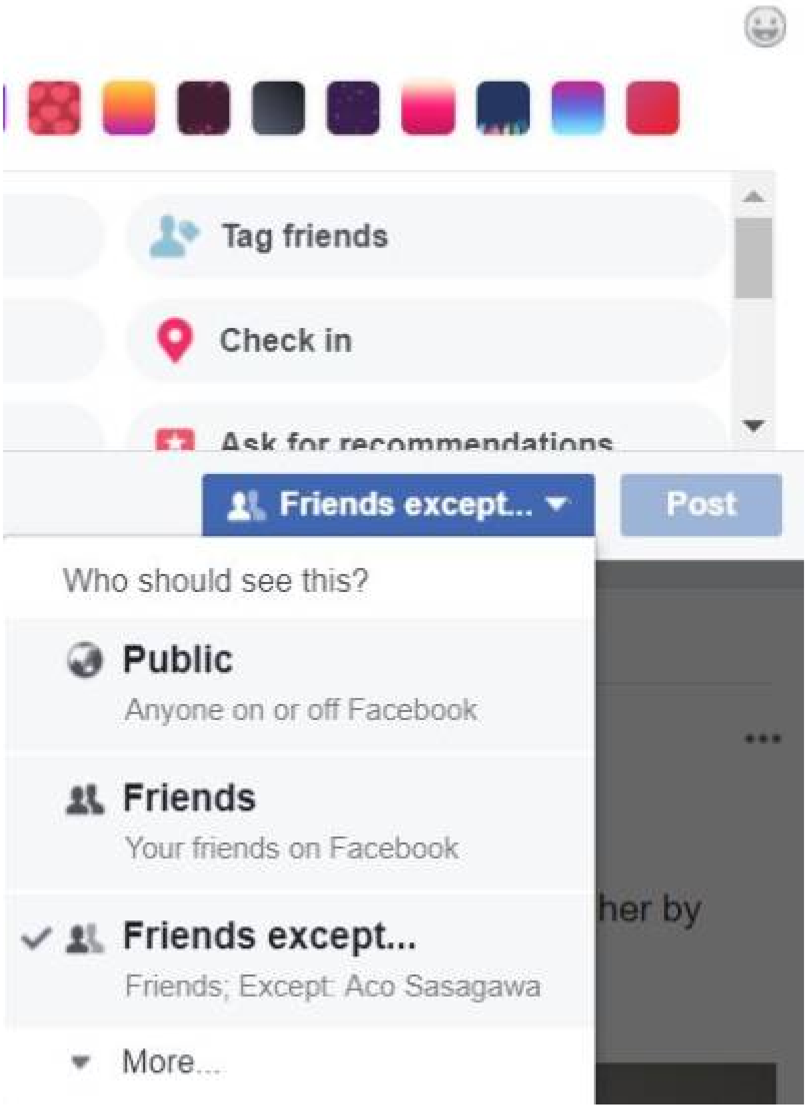
Friend lists

Create lists to easily share with only specific people.

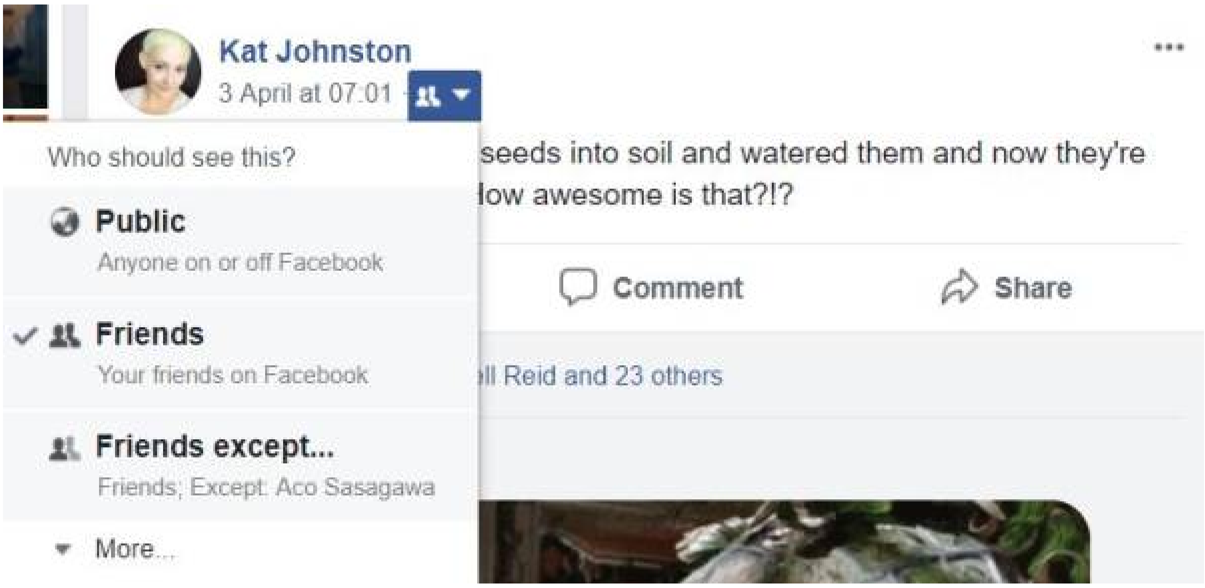
1. In News Feed, click 'Friend Lists' on the left. You may need to click 'See More' first.
2. Click '+ Create List'.
3. Create list name and add friends to the list. You can add/remove people at any time.
4. Click Create.

Set privacy on posts

Select from the drop-down menu - you can select a friends list here too. **Check this setting every time you post.**



You (and others) can **change the privacy** of a post later.



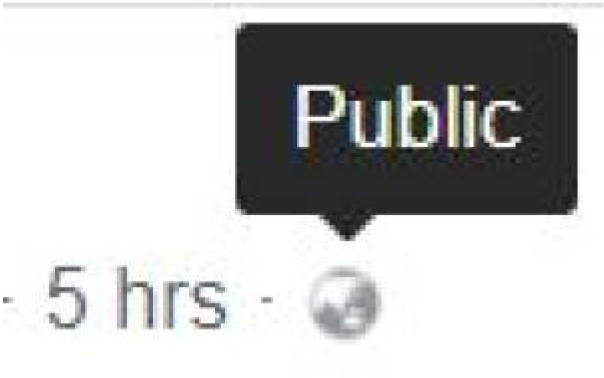
Kat Johnston
3 April at 07:01

Who should see this?

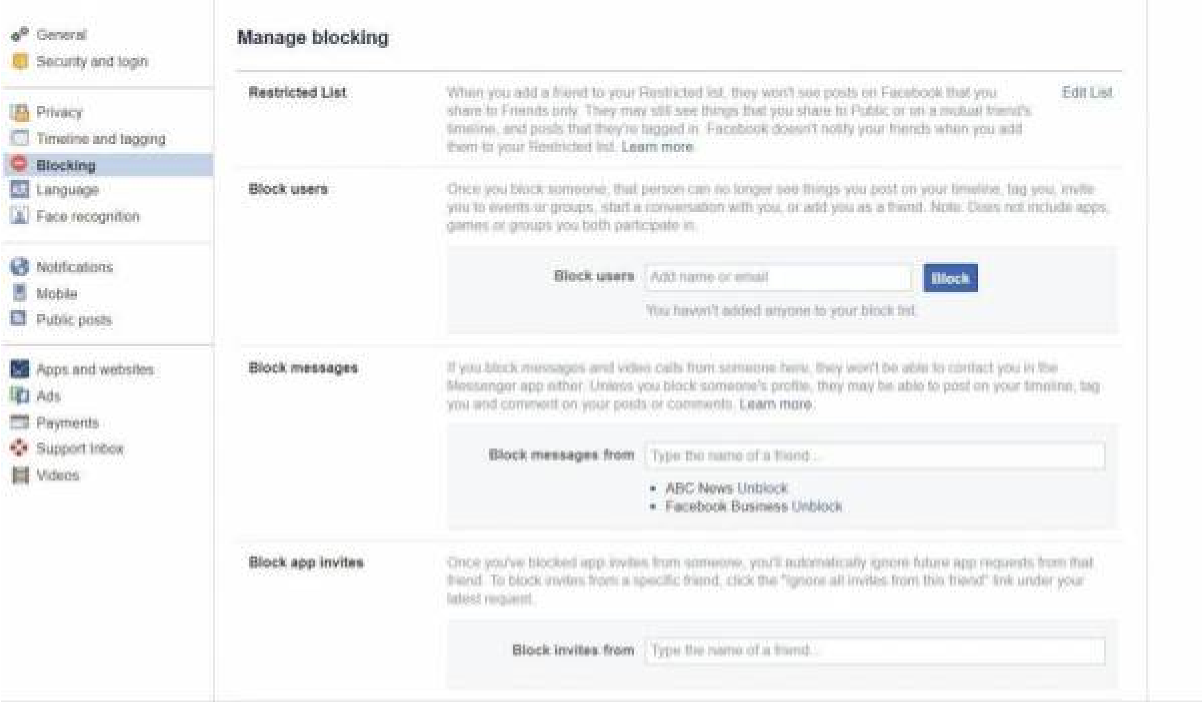
seeds into soil and watered them and now they're
low awesome is that?!?

Comments inherit privacy settings of original posts. Eg, **if a post is public, so are your comments.**

Facebook Pages and most **Facebook groups** have public posts. 'Account privacy' does not cover content on something marked as public.



You can **block** people if someone is harassing or bullying you (located under 'settings'). You can also report behavior on individual posts.



Manage blocking

Restricted List When you add a friend to your Restricted list, they won't see posts on Facebook that you share to Friends only. They may still see things that you share to Public or on a mutual friend's timeline, and posts that they're tagged in. Facebook doesn't notify your friends when you add them to your Restricted list. Learn more Edit List

Block users Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users: Add name or email [Block]

You haven't added anyone to your block list.

Block messages If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your timeline, tag you and comment on your posts or comments. Learn more.

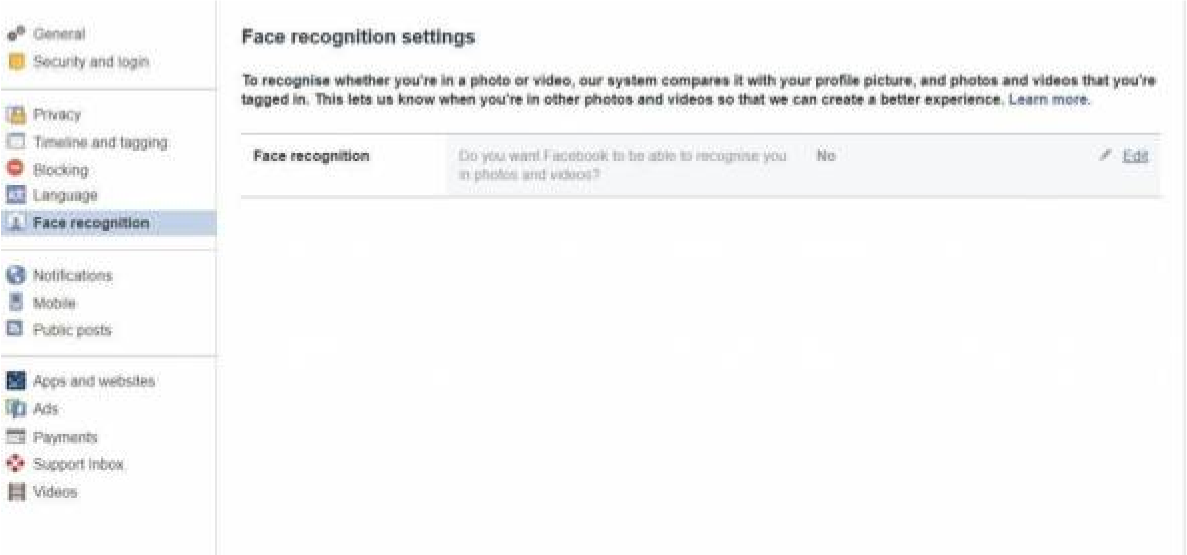
Block messages from: Type the name of a friend...

- ABC News Unblock
- Facebook Business Unblock

Block app invites Once you've blocked app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore all invites from this friend" link under your latest request.

Block invites from: Type the name of a friend...

Consider disabling **facial recognition** to maintain privacy.

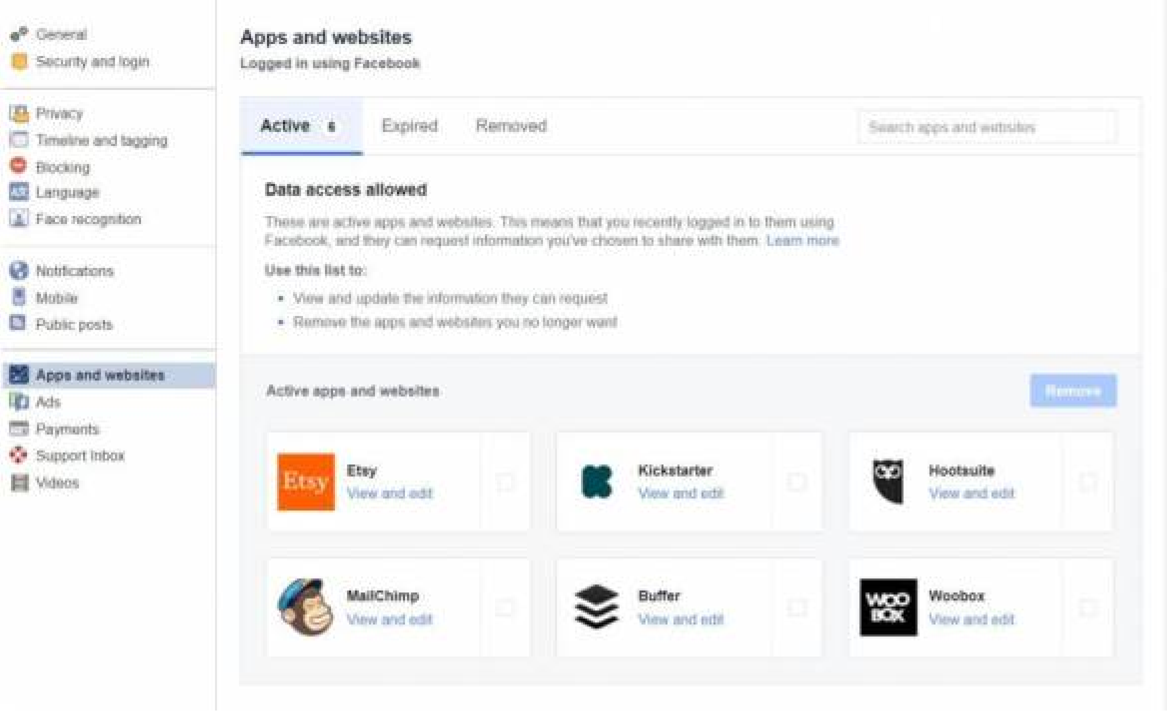


Face recognition settings

To recognise whether you're in a photo or video, our system compares it with your profile picture, and photos and videos that you're tagged in. This lets us know when you're in other photos and videos so that we can create a better experience. Learn more.

Face recognition Do you want Facebook to be able to recognise you in photos and videos? No Edit

View and edit the accounts you've logged into using Facebook. Logging in with Facebook allows sites to access certain information. Regularly check and adjust information being shared.



Apps and websites

Logged in using Facebook

Data access allowed

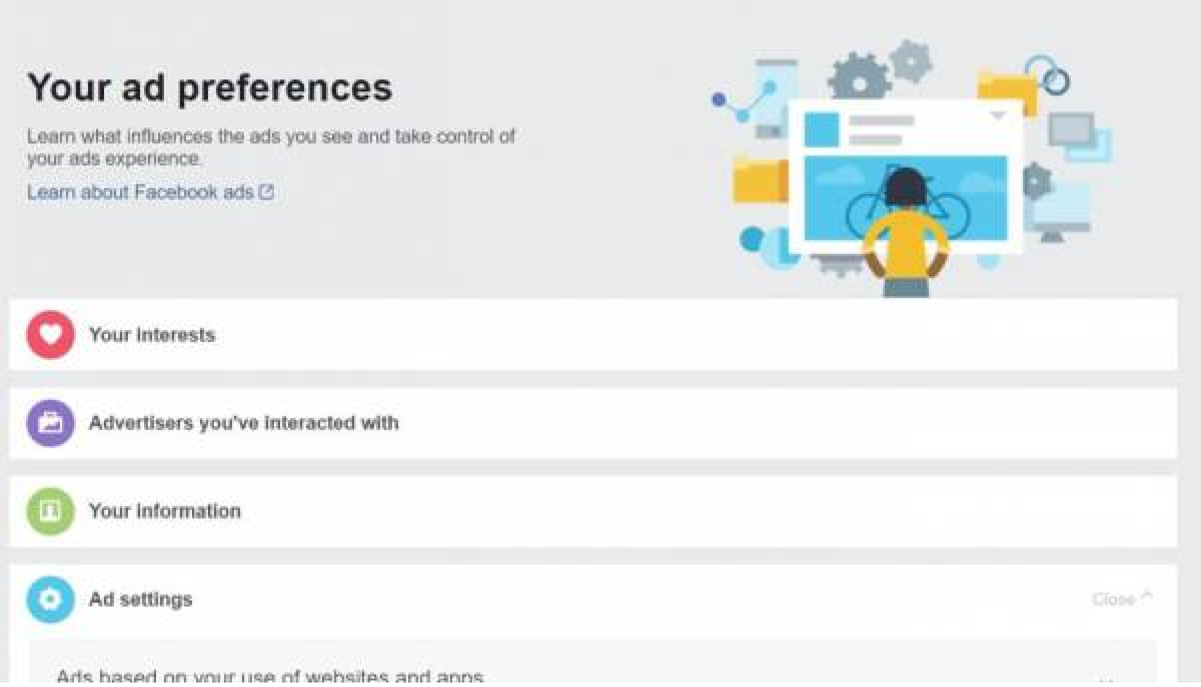
These are active apps and websites. This means that you recently logged in to them using Facebook, and they can request information you've chosen to share with them. Learn more

Use this list to:

- View and update the information they can request
- Remove the apps and websites you no longer want

Active apps and websites

Facebook advertisers use your data to show targeted content.



Your ad preferences

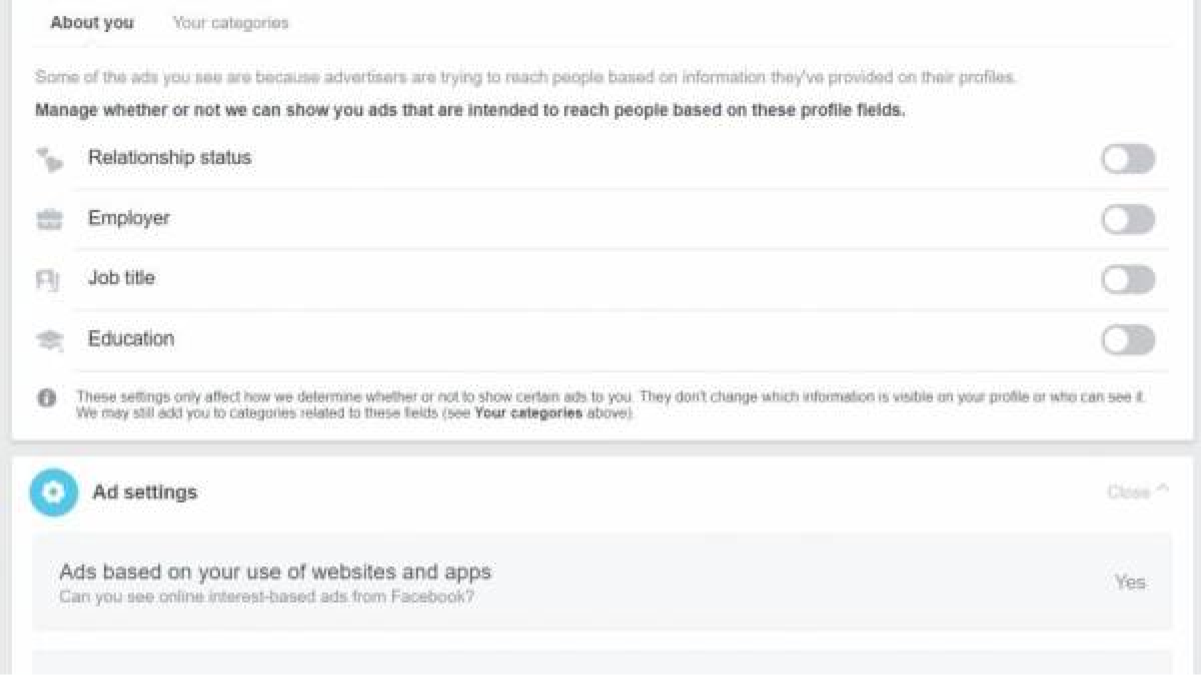
Learn what influences the ads you see and take control of your ads experience.

Learn about Facebook ads

Your interests
Advertisers you've interacted with
Your information
Ad settings
Close
Ads based on your use of websites and apps

A lot of data is stored here. You can remove information (e.g. your interests), but Facebook will continue collecting data to rebuild lists.

Permissions allow/deny advertiser access to certain information.



Some of the ads you see are because advertisers are trying to reach people based on information they've provided on their profiles.

Manage whether or not we can show you ads that are intended to reach people based on these profile fields.

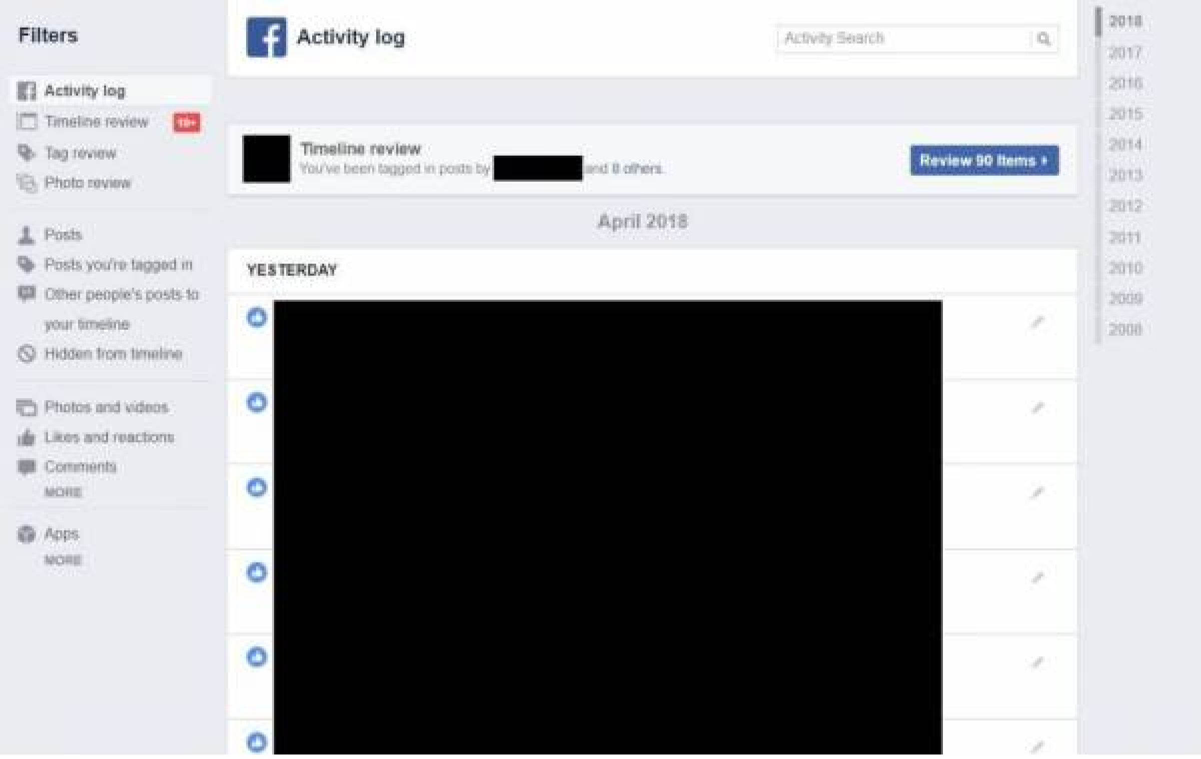
Relationship status
Employer
Job title
Education

These settings only affect how we determine whether or not to show certain ads to you. They don't change which information is visible on your profile or who can see it. We may still add you to categories related to these fields (see **Your categories** above).

Ad settings

Ads based on your use of websites and apps
Can you see online interest-based ads from Facebook? Yes

Regularly check your activity log and review your data. **Do you still need to share it?** Remove what you don't need.

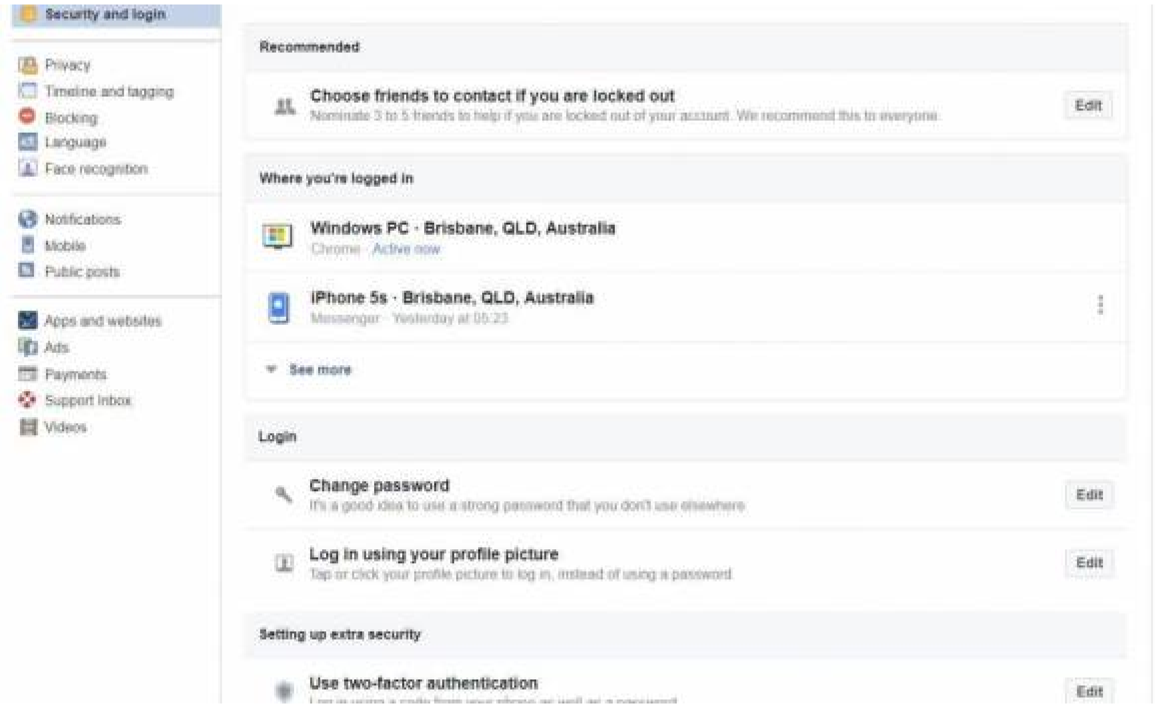


[redacted] Timeline review
You've been tagged in posts by [redacted] and 8 others.

[redacted]

Use the security and log-in screen to review your logins, and log out remotely. **If you left Facebook logged in somewhere accidentally, log out here.**

Turn on **Two Factor Authentication**, and consider nominating people to vouch for your identity if you're locked out.



Recommended

Choose friends to contact if you are locked out
Nominate 3 to 5 friends to help if you are locked out of your account. We recommend this to everyone.

Where you're logged in

Windows PC · Brisbane, QLD, Australia
Chrome · Active now

iPhone 5s · Brisbane, QLD, Australia
Messenger · Yesterday at 05:23

Login

Change password
It's a good idea to use a strong password that you don't use elsewhere

Log in using your profile picture
Tap or click your profile picture to log in, instead of using a password

Setting up extra security

Use two-factor authentication
Log in using a code from your phone as well as a password

Remember!

Privacy is not guaranteed even with strong settings:

1. **Screen-shots** can be shown to people who don't usually have access.
2. Your **copied/downloaded** information can be shared.
3. You may inadvertently **give access** to the wrong person.
4. **Security flaws** can make private information public.

To keep information 100% private, don't put it online.

Further Resources

https://www.staysmartonline.gov.au/

https://www.scamwatch.gov.au/

https://aifs.gov.au/cfca/publications/online-safety

https://www.esafety.gov.au/

https://www.opencolleges.edu.au/informed/cyber-safety/

https://www.facebook.com/help/325807937506242

https://help.instagram.com/196883487377501 https://help.twitter.com/en/safety-and-security