



Workshop 04 - Social Media and Online Safety

SLQ Wiki Fabrication Lab 2025/07/04 15:34

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.



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)



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.



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

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



Keep Bluetooth off or hidden if not in use.



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



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.



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

Secure your Connection

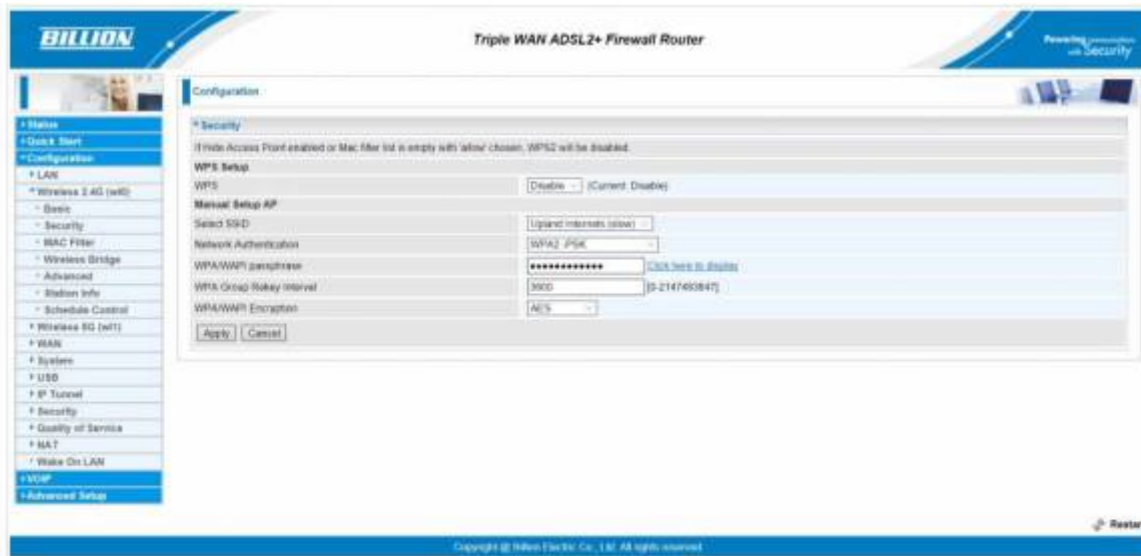
Home Wifi

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.



- **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.



- **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



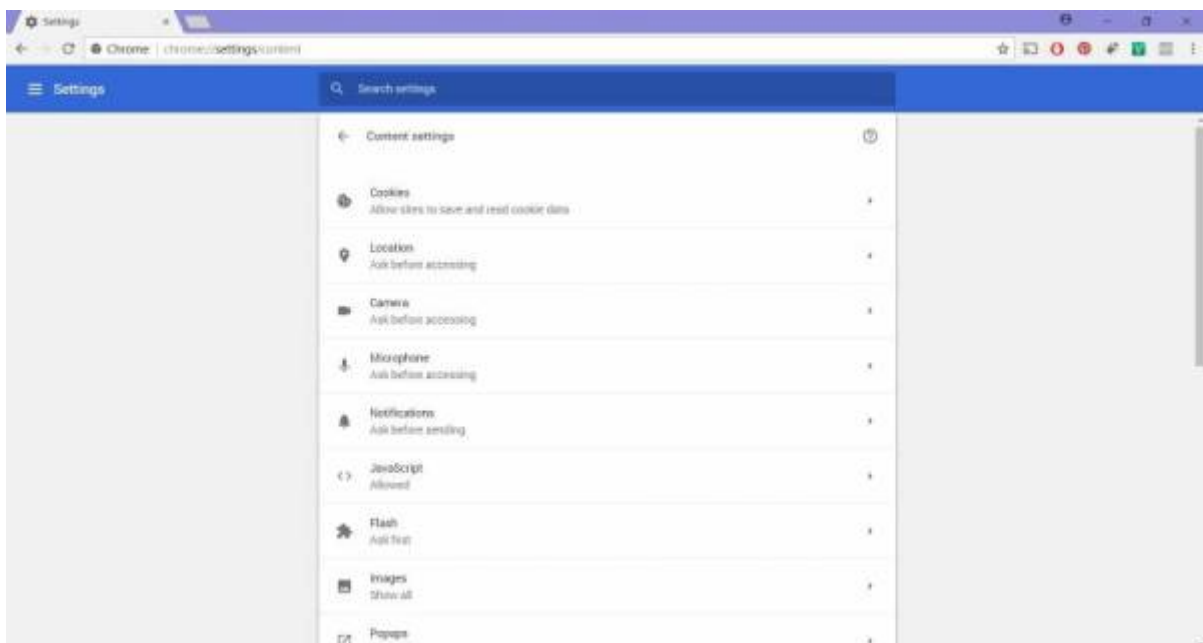
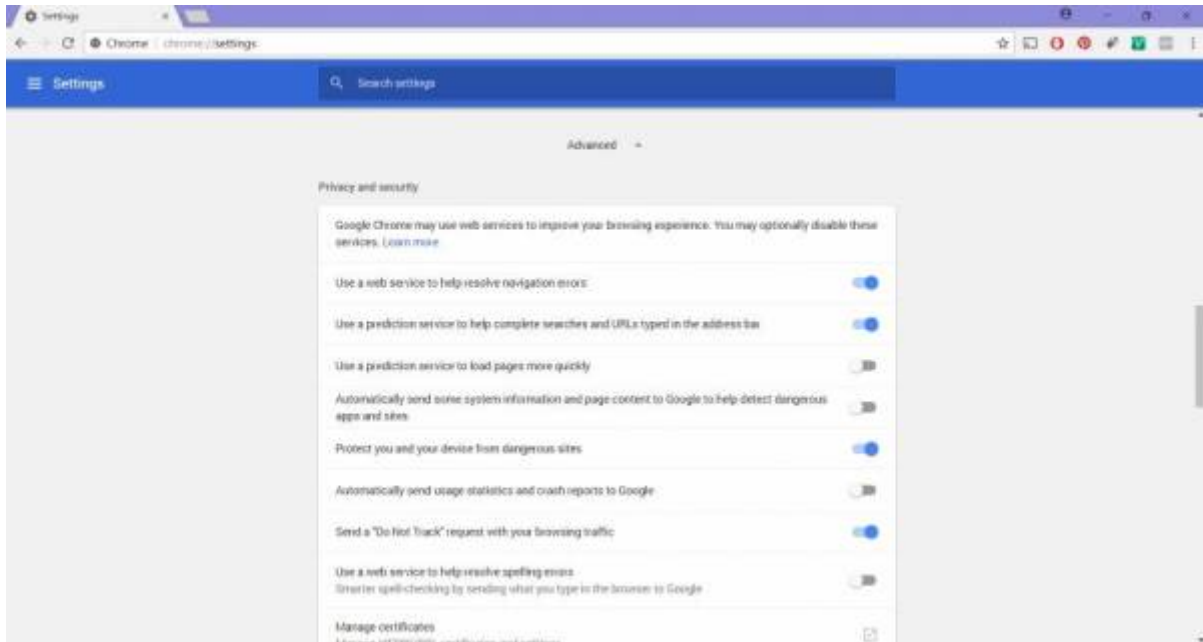
Free wifi can have security risks.

- **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.



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 your 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: 'ilove interiordesign'.
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.

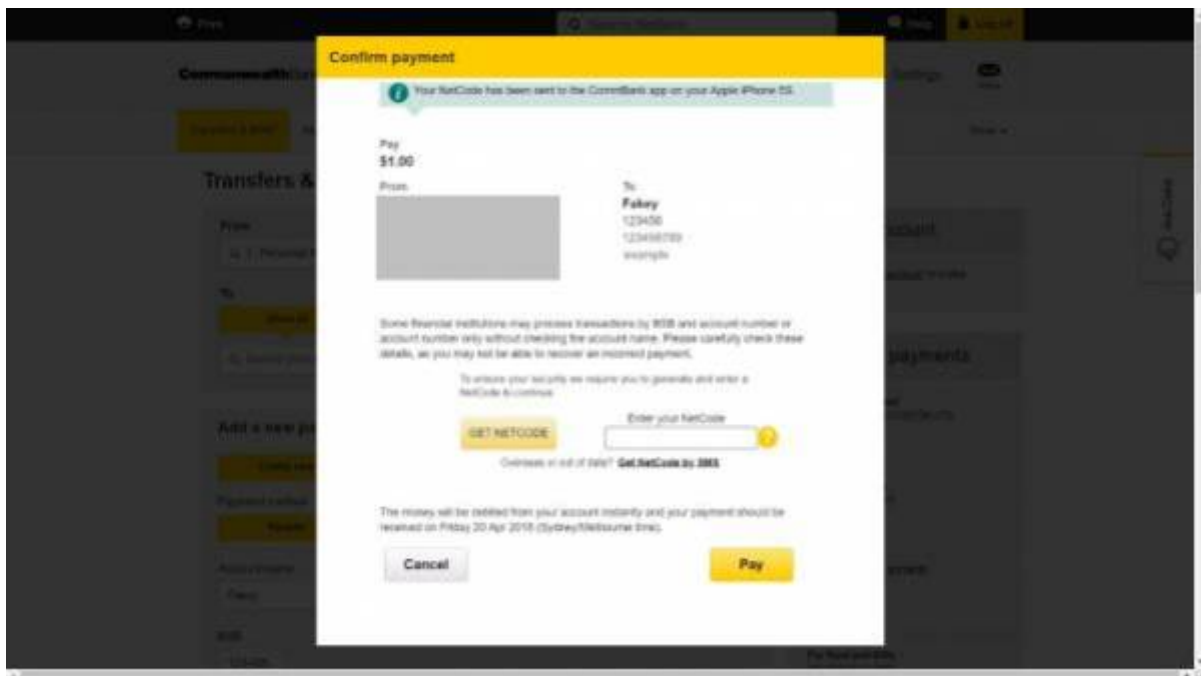
Using 2FA

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

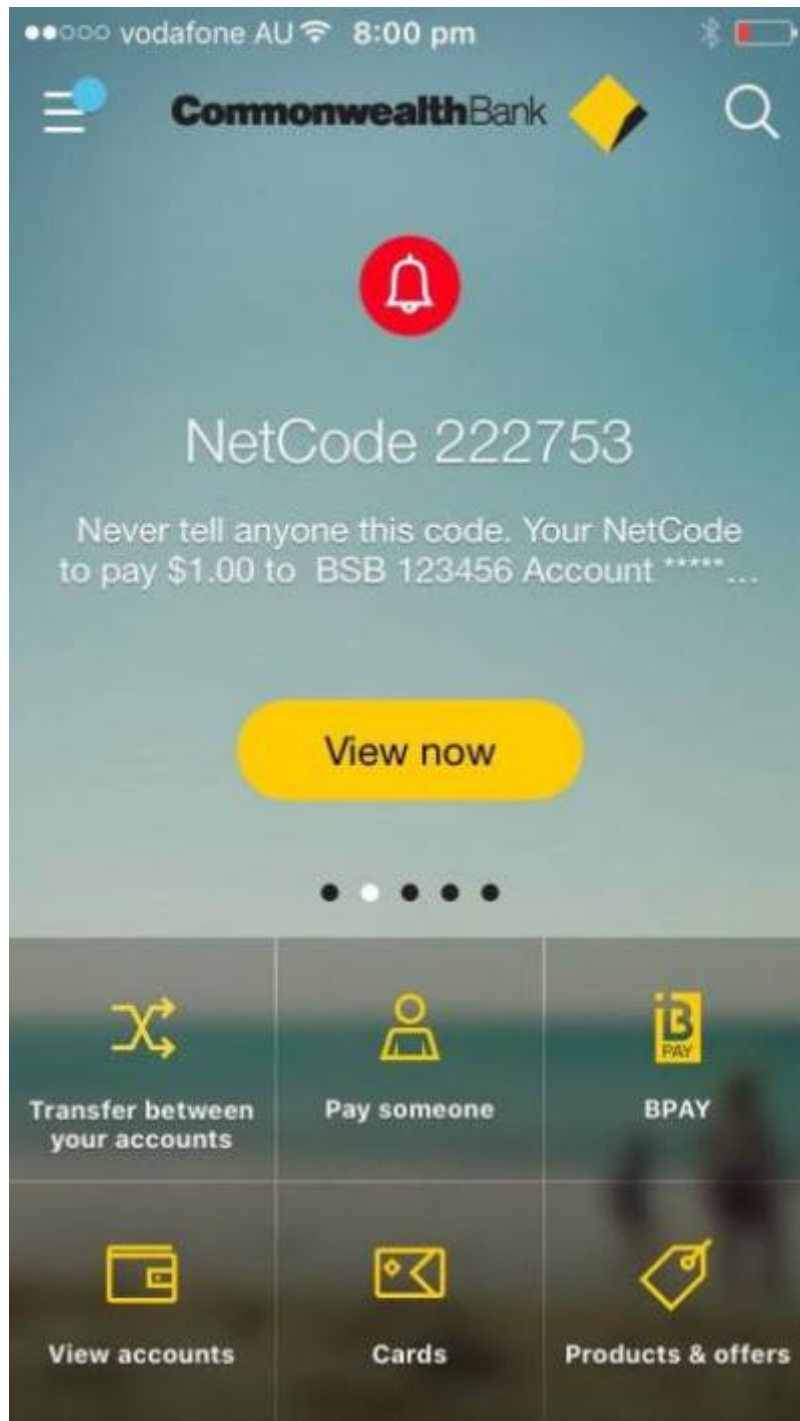
- something you **know** (eg a pin or password)
- something you **have** (e.g. a bank card or a mobile phone)
- something you **are** (e.g. a fingerprint)

Your accounts and transactions are more secure with 2FA.

Eg. This website sends a token via Push Notification:



You must enter the code to continue the transaction:



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=3lluT4jo4f8>
- 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.

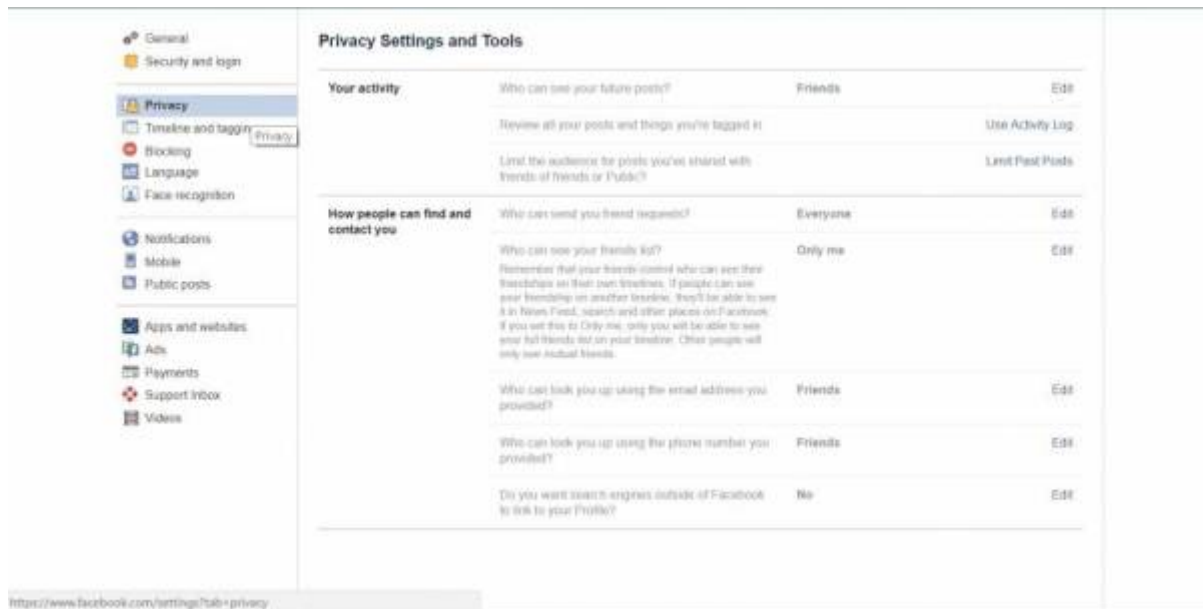
Social Media Privacy

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

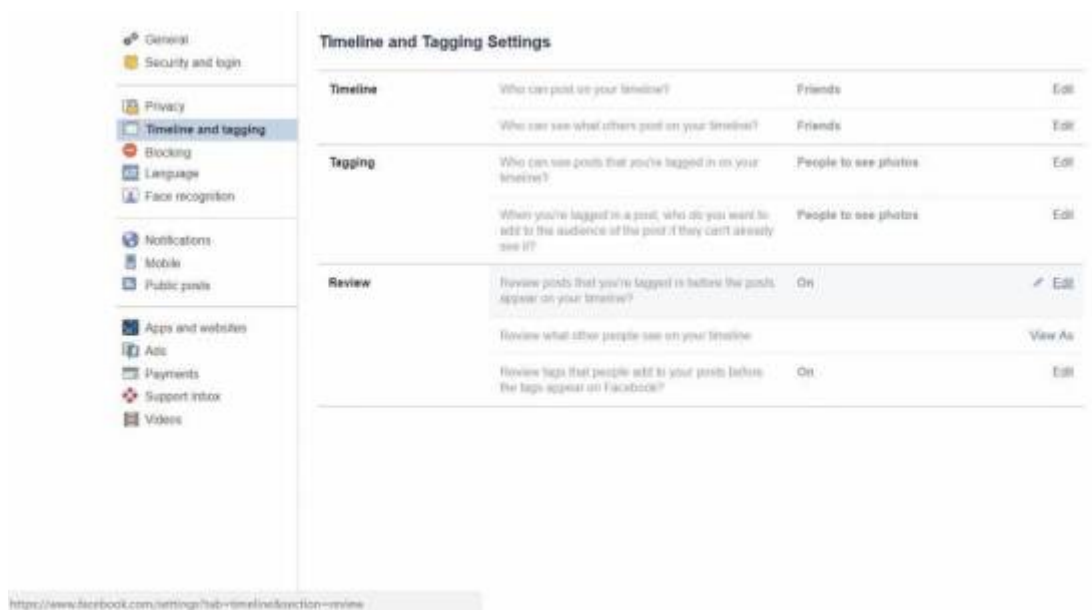
You can often Google guides on how to navigate privacy on each platform. We'll look at Facebook's settings today.

Facebook

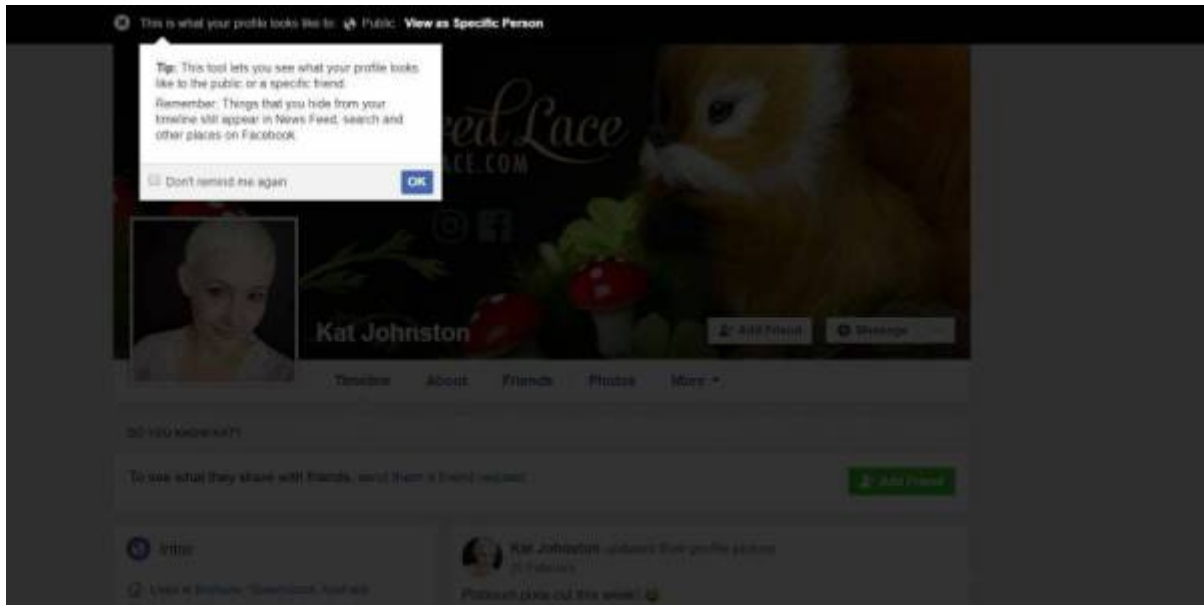
Facebook's account privacy options can be adjusted in 'Settings':



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



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



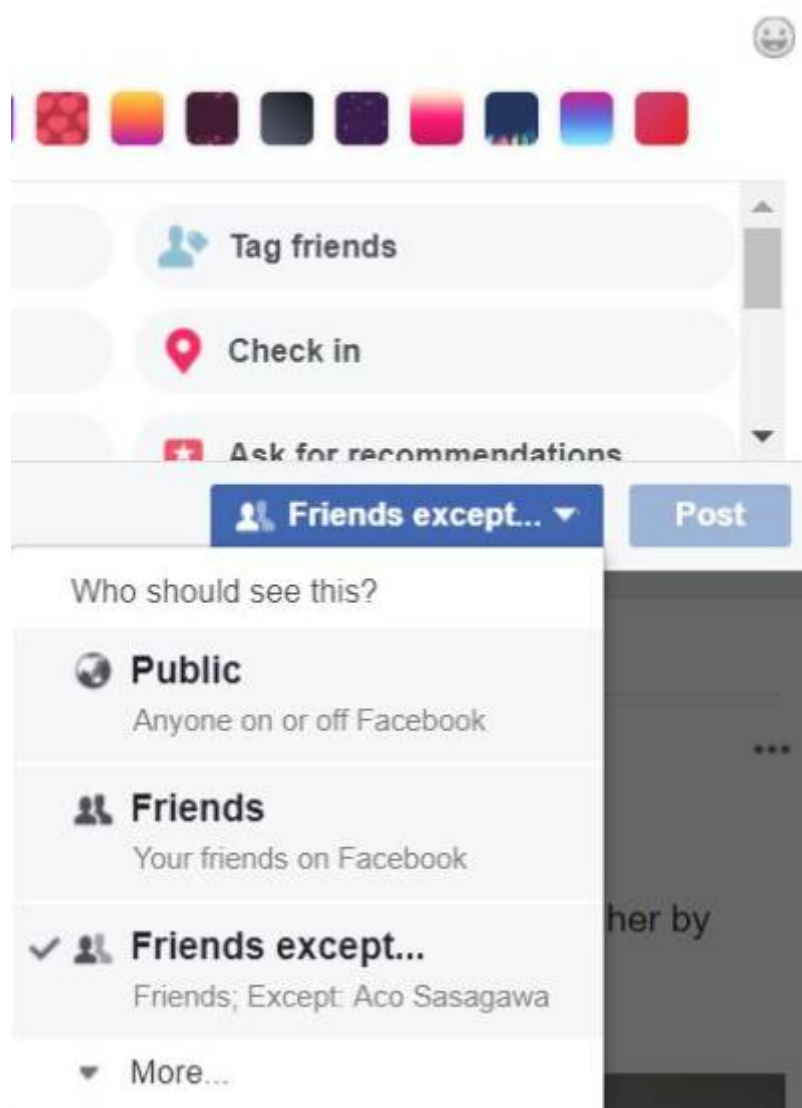
Friend lists

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.**

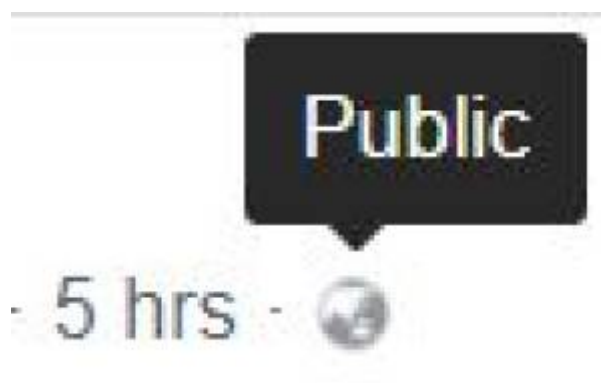


You (and others) can **change the privacy** of a post later.

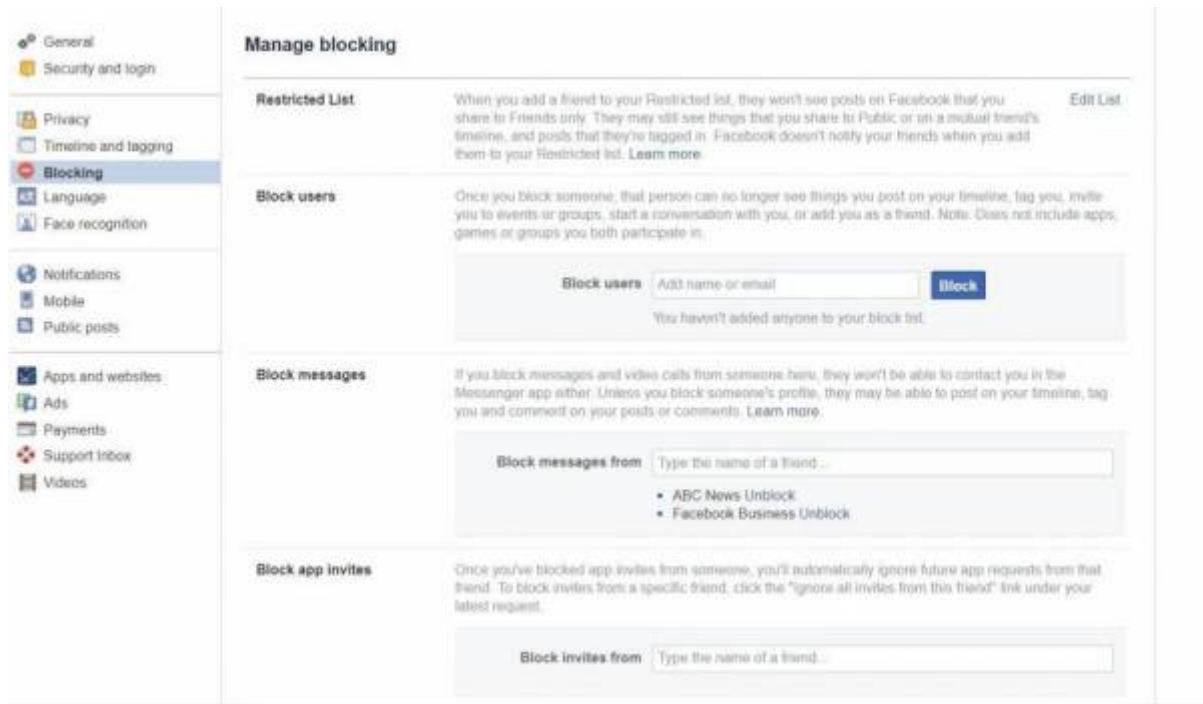


Comments inherit privacy settings of original posts. Eg, **if a post is public, so are your comments.**

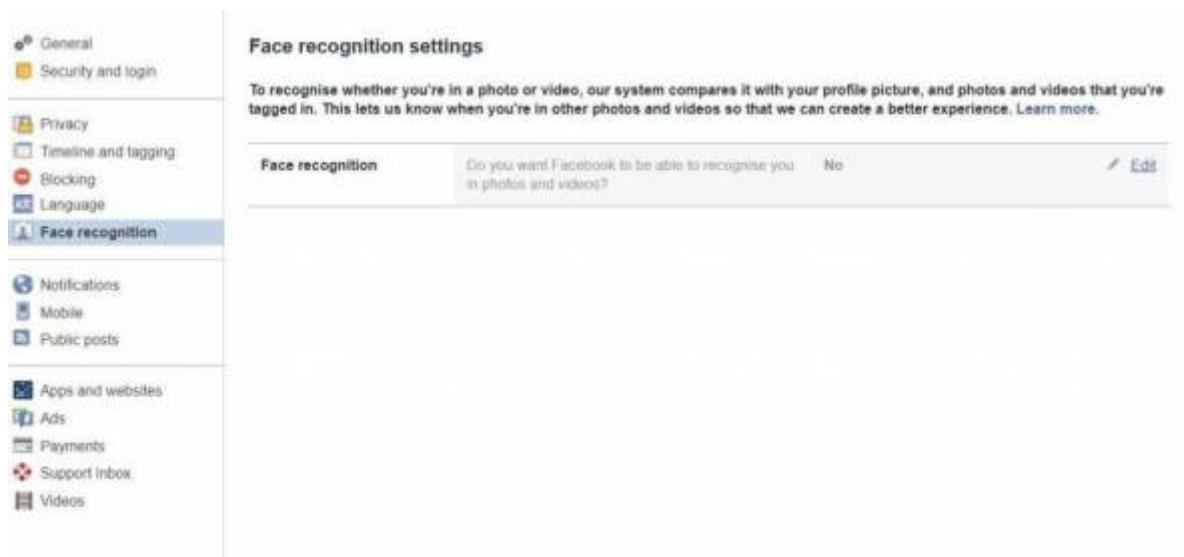
Facebook Pages and most **Facebook groups** have public posts. 'Account privacy' does not cover content on something marked as public.



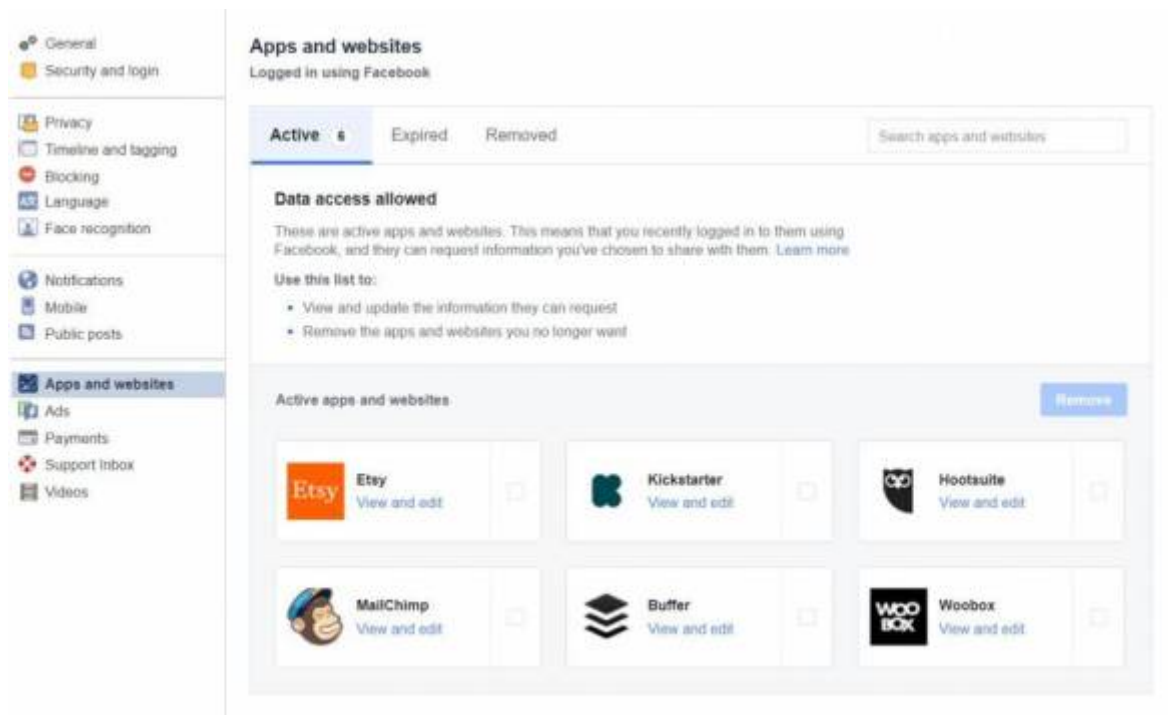
You can **block** people if someone is harassing or bullying you (located under 'settings'). You can also report behavior on individual posts.



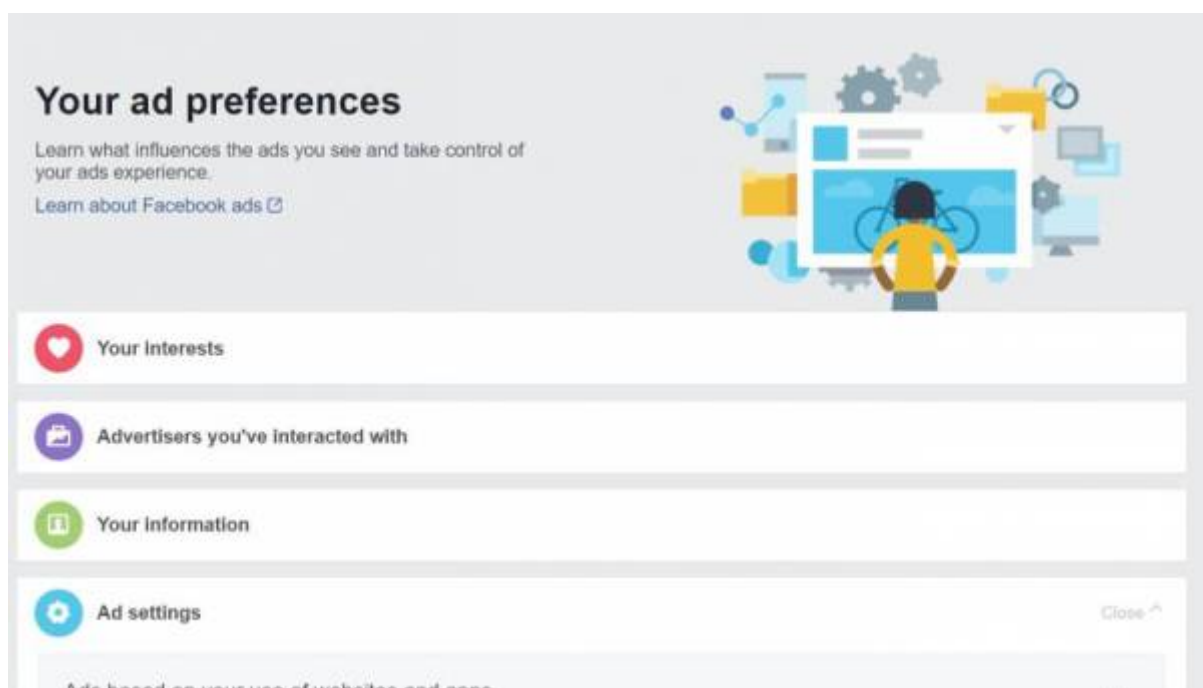
Consider disabling **facial recognition** to maintain privacy.



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.



Facebook advertisers use your data to show targeted content.



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.

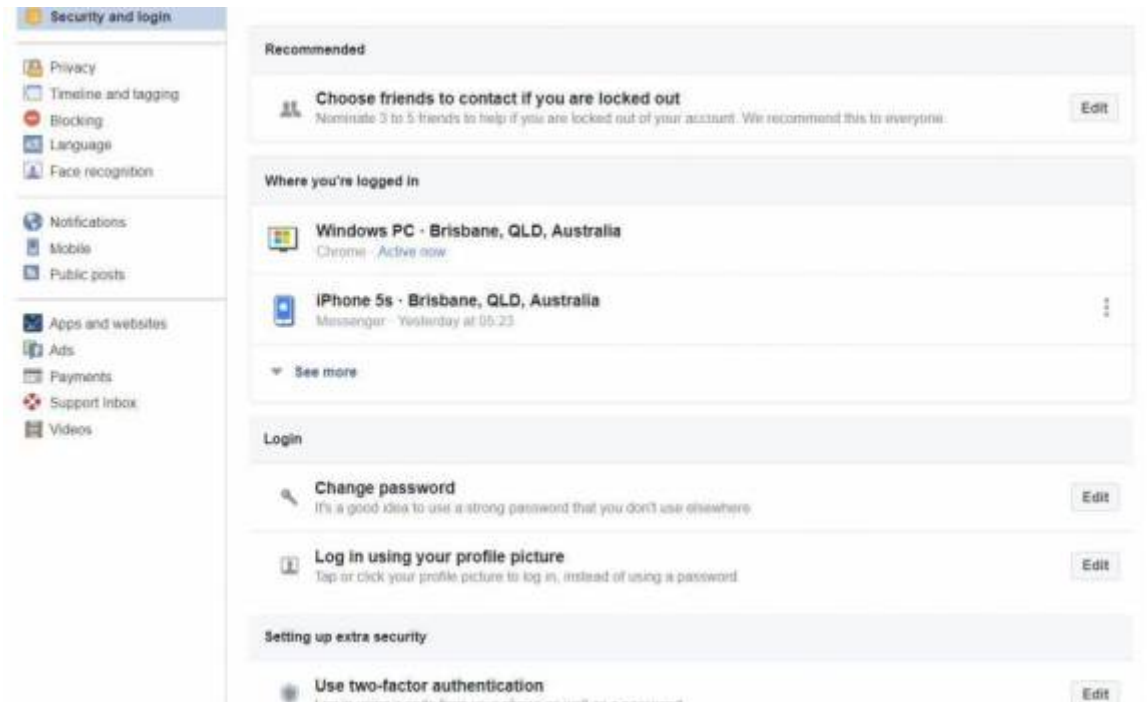


Regularly check your activity log and review your data. **Do you still need to share it?** Remove what you don't need.



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.



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>