Workshop 04 - Social Media and Online Safety

SLQ Wiki Fabrication Lab 2024/05/23 01:22

~~REVEAL~~

Workshop 04 - Social Media and Online Safety

What is Online Safety?

The internet is an incredible resource to stay in touch with friends and family, and to connect with products, services and information all around the world.

There are, however, risks associated with being online, such as:

1. Scamming and phishing
2. Viruses and Malware
3. Fraud and Identity Theft
4. Gaining unauthorised access to personal/private information
5. Cyberstalking
6. Cyberbullying
7. Hacking

By the end of this session, you will be able to:

1. Secure your devices, connection, browser and accounts
2. Spot potentially dangerous or risky online situations
3. Lock down your privacy settings on social media

Step One - Secure your Devices

On your Desktop/Laptop

The more layers of defence you have, the harder it will be for cyber-criminals to gain access to your computer and its contents.

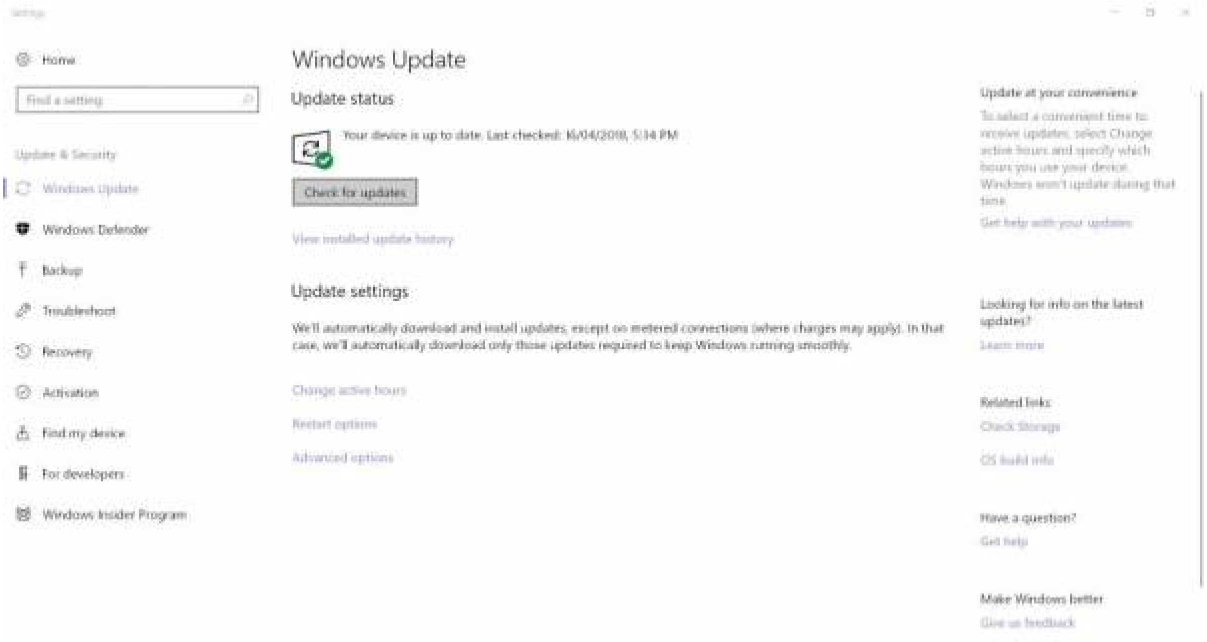
Some operating systems are more vulnerable to attack than others. Windows tends to be less secure than Mac and Linux, for example.

Only install reputable software. If something is free or seems too good to be true, do your research and make sure you're not accidentally downloading spyware or malware.

Use secure passwords to lock your device when not in use. Consider using a setting that locks the device after a set amount of time if not in use.

Don't leave your device unlocked and unattended in public areas, even for a short time. Even if it's locked, someone can still steal it if it's left alone.

Always keep your software up to date, as this will include security patches which help to reduce vulnerabilities. This includes your operating system, browsers, programs, plugins, etc.



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.

Looking for info on the latest updates?

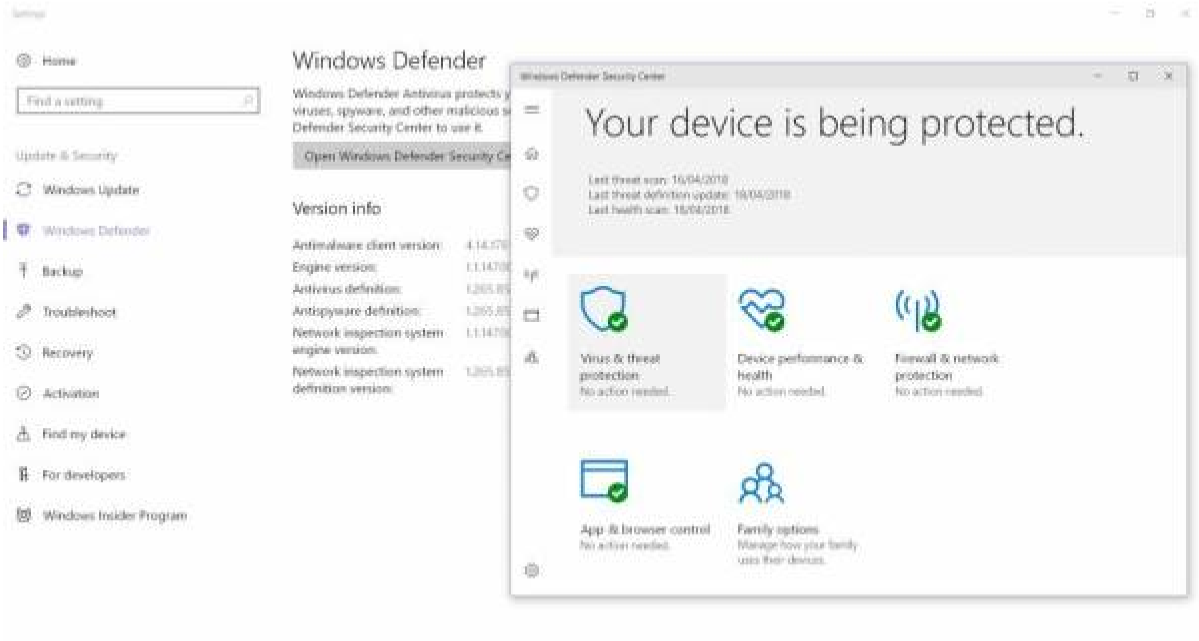
Install a firewall. A firewall acts like a barrier between your computer and any authorised programs trying to access it. If there are any attempts to access your system, it will tell you so that you can either authorise or deny access.

Install anti-virus software to protect against unauthorised software that can attack and compromise your system. Examples of viruses and malware (malicious software) include:

1. Keyloggers (records your keystrokes)
2. Ransomware (holds your system or details hostage in demand of payment)
3. Worms (causes harm and self-replicate to spread to other computers/devices)
4. Trojan Horses (software that misleads the user about its true intent)
5. Rootkits (designed to provide unauthorised access to a system)

And more.

Install anti-spyware if it isn't already included in your anti-virus software. Spyware is a type of software that collects information from you without your approval, which is then passed back to a third-party website. It is often difficult to remove by yourself.



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

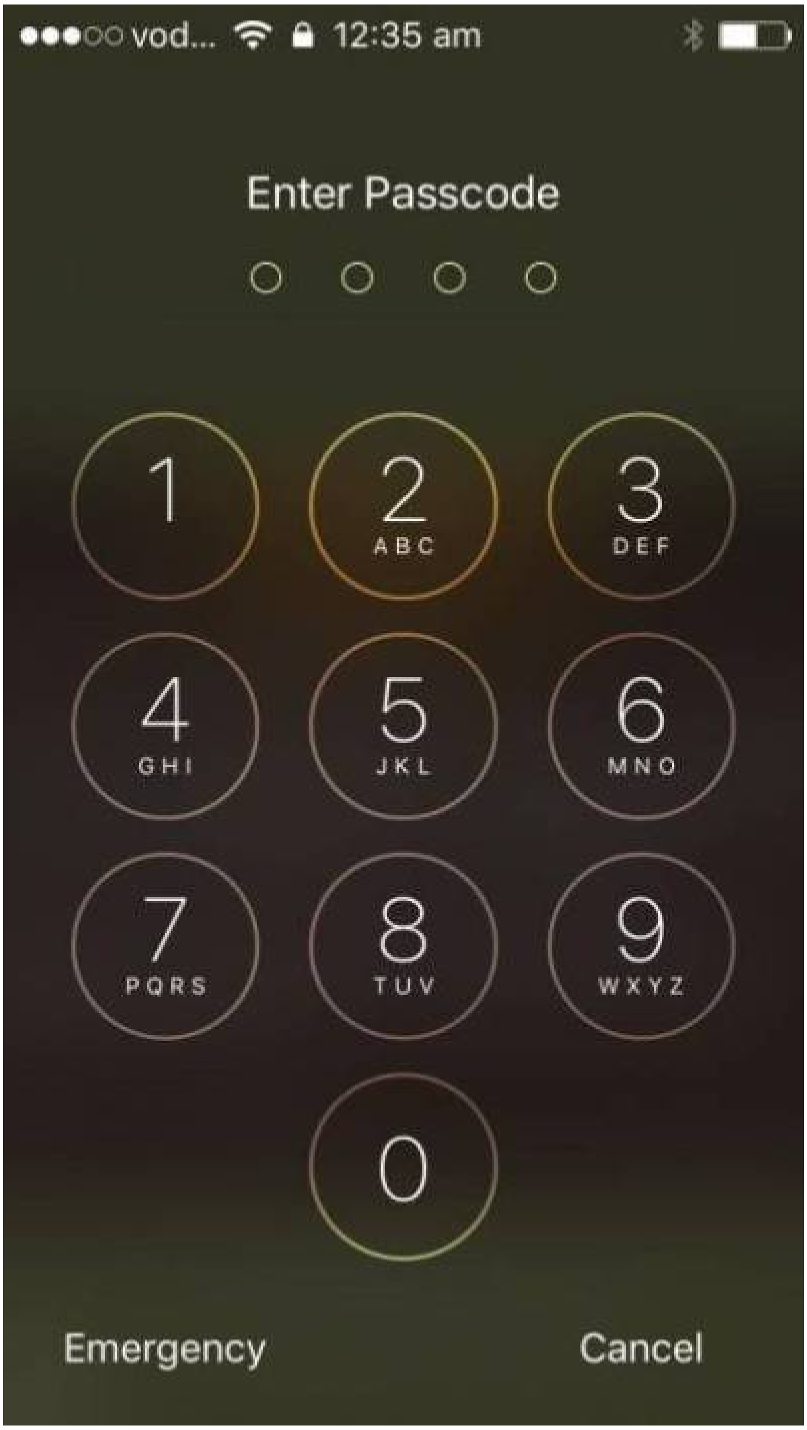
Your device is being protected.

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

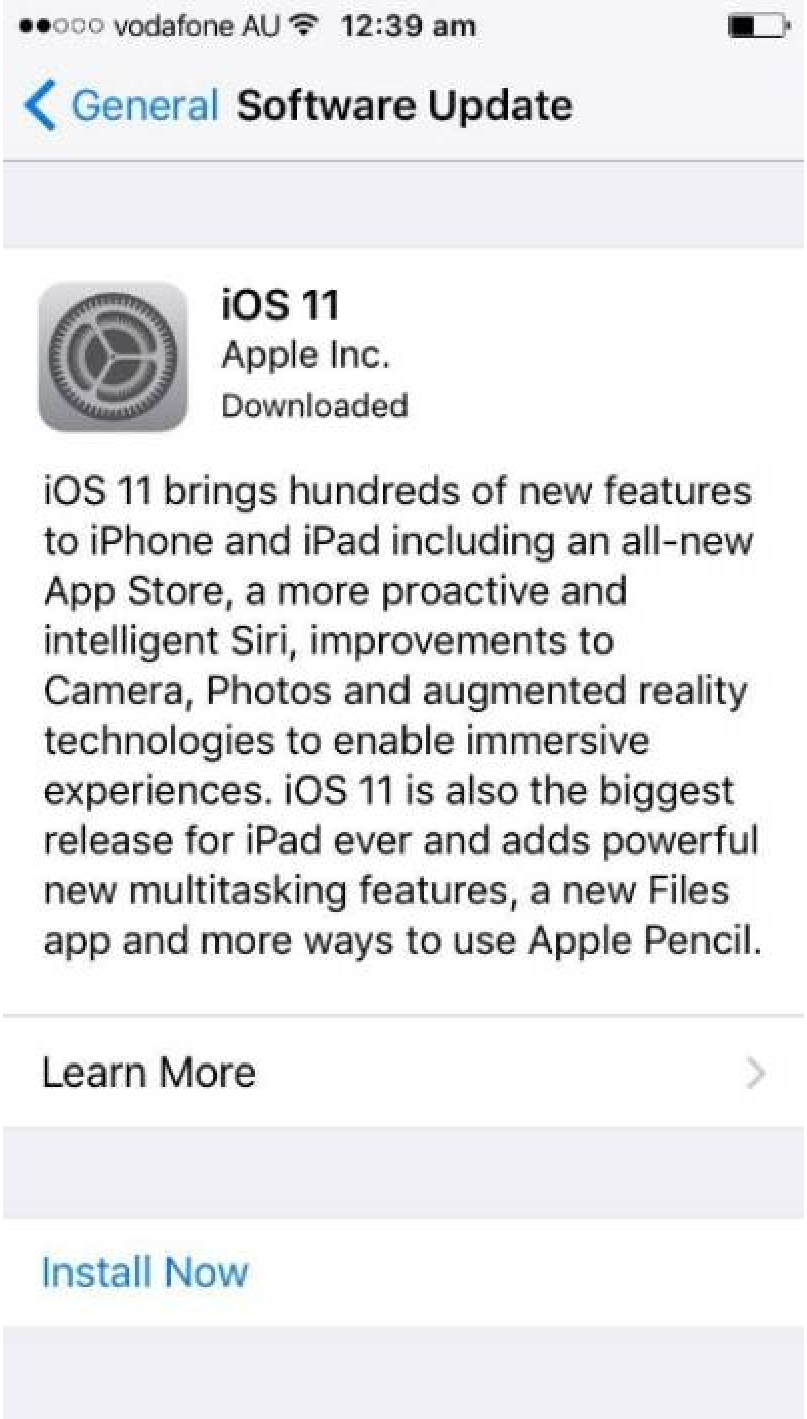
Virus & threat protection: No action needed.
Device performance & health: No action needed.
Firewall & network protection: No action needed.
App & browser control: No action needed.
Family options: Manage how your family uses their devices.

On your mobile

Use a secure password, pin, gesture or biometric data to lock your device when not in use. Consider using a setting that locks the device after a set amount of time if not in use.



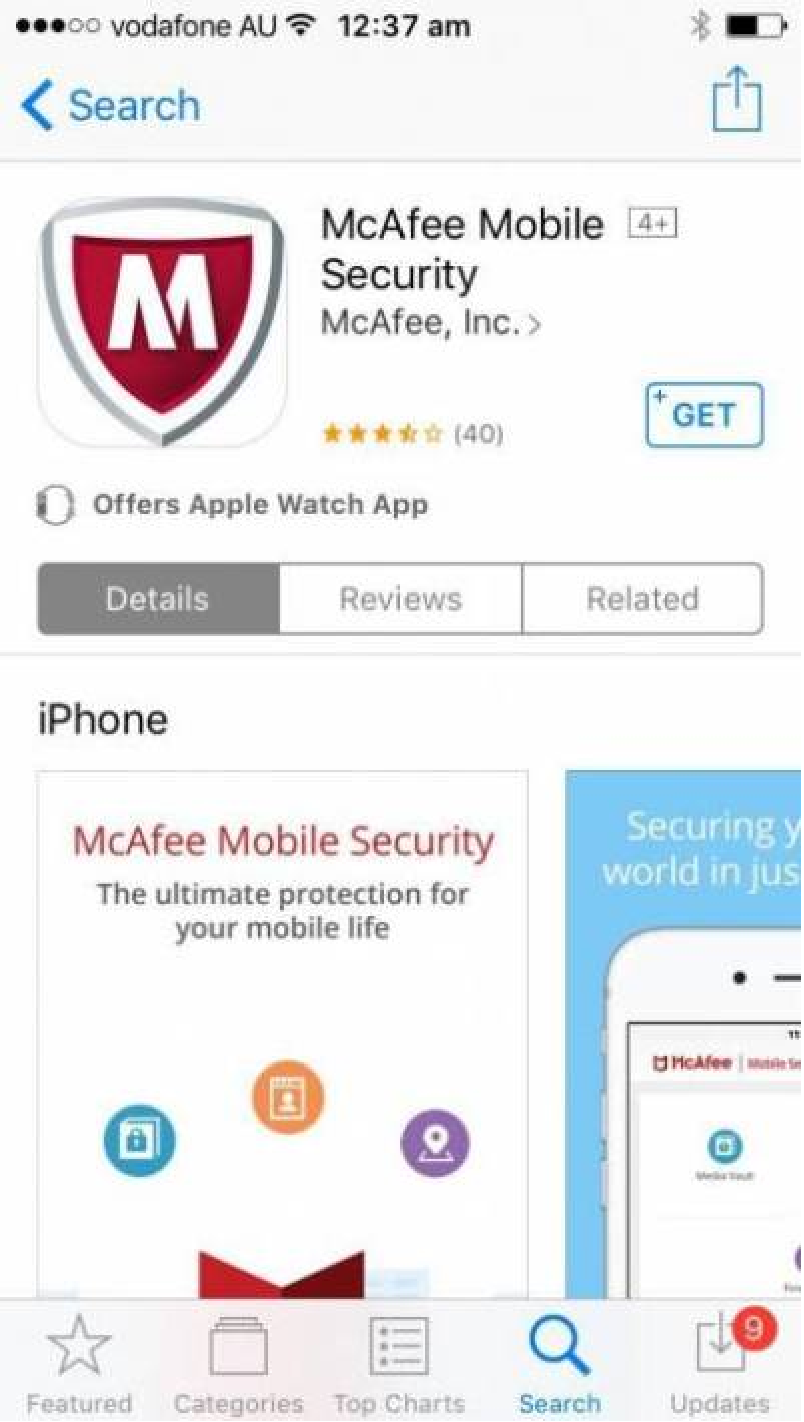
Keep your device’s software up to date, as security patches help prevent or repair vulnerabilities. This includes the IOS, apps, etc.



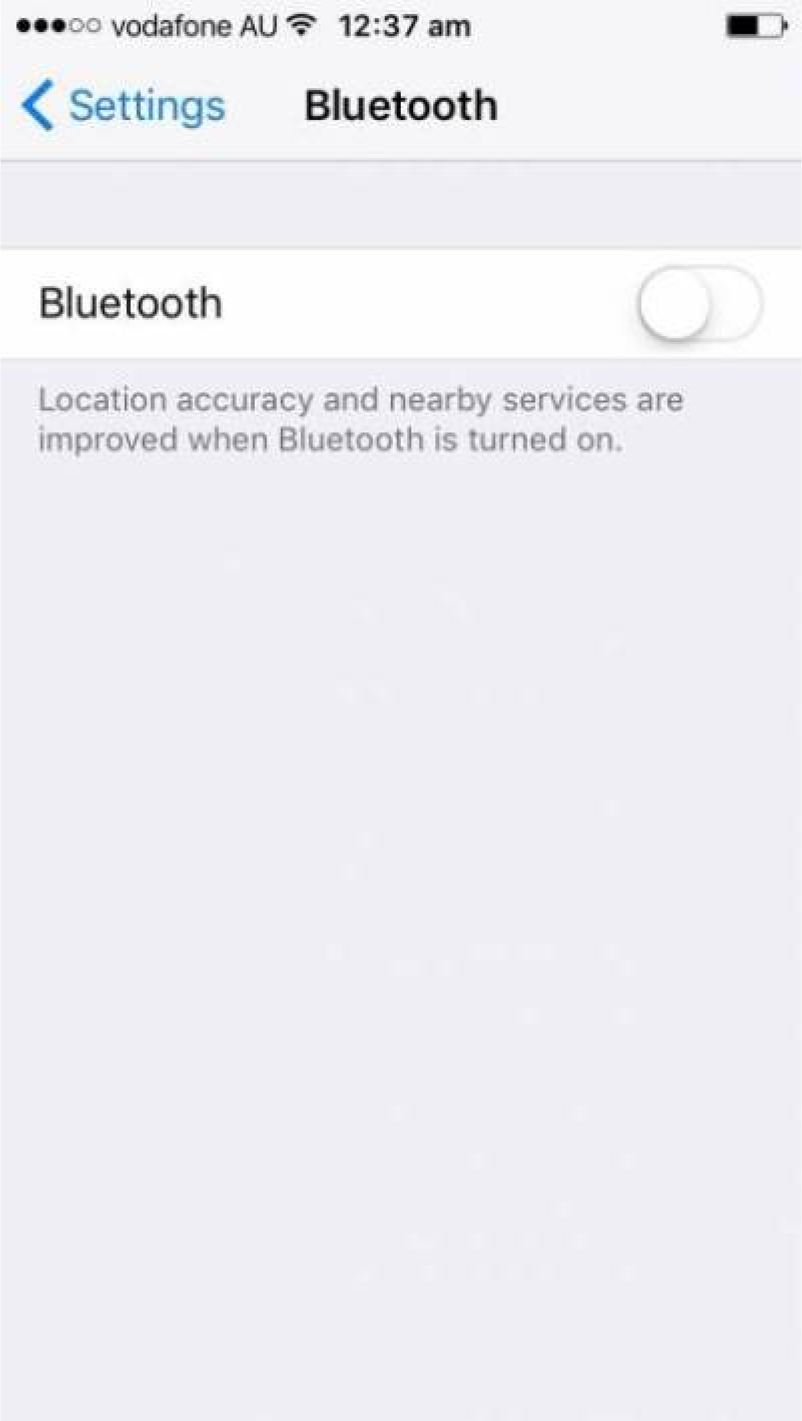
iOS 11 brings hundreds of new features to iPhone and iPad including an all-new App Store, a more proactive and intelligent Siri, improvements to Camera, Photos and augmented reality technologies to enable immersive experiences. iOS 11 is also the biggest release for iPad ever and adds powerful new multitasking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

Only download reputable apps from trusted sources, such as Google Play and the iPhone App Store.

Install reputable security software that includes anti-virus and potentially anti loss/theft capabilities.



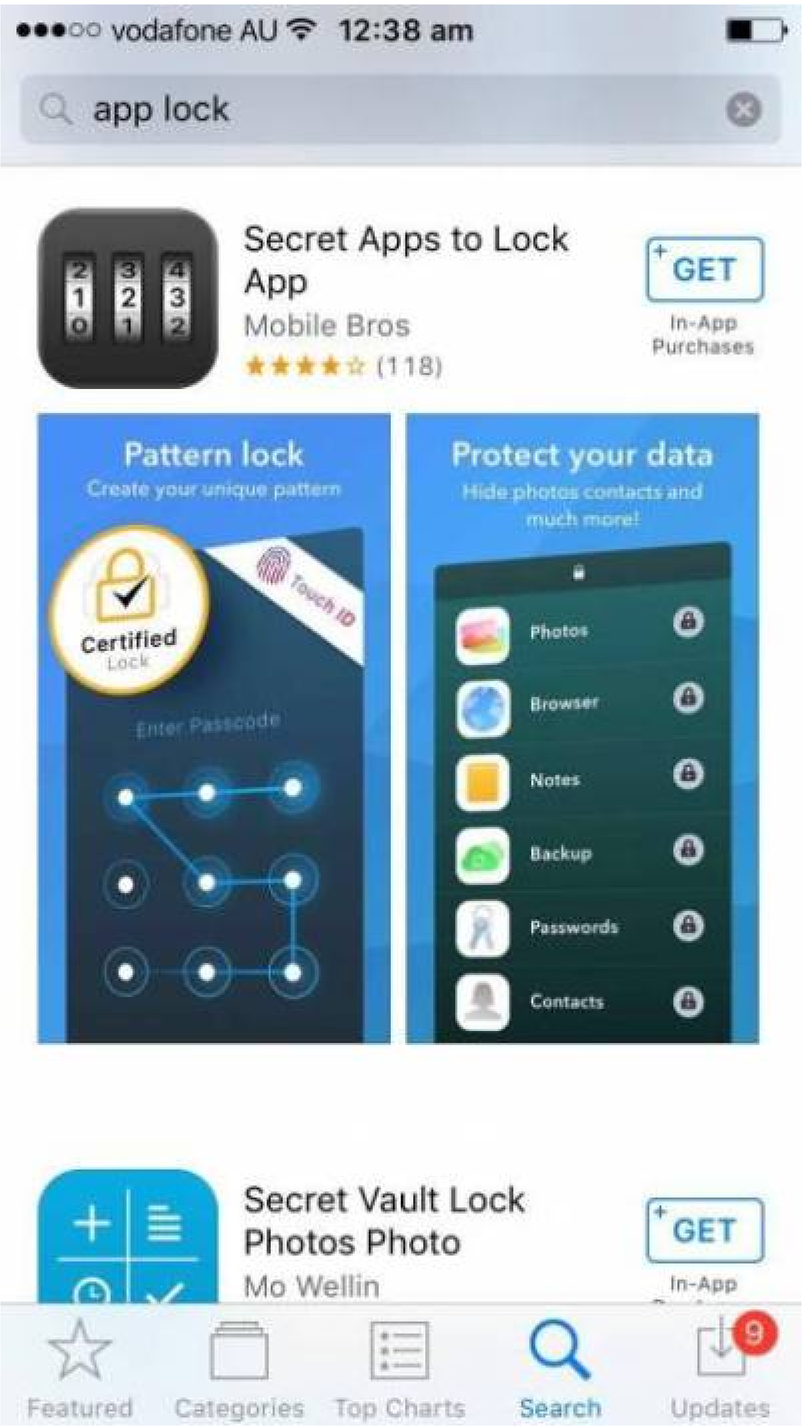
Keep Bluetooth turned off or set it to hidden if not in use.



Bluetooth ○

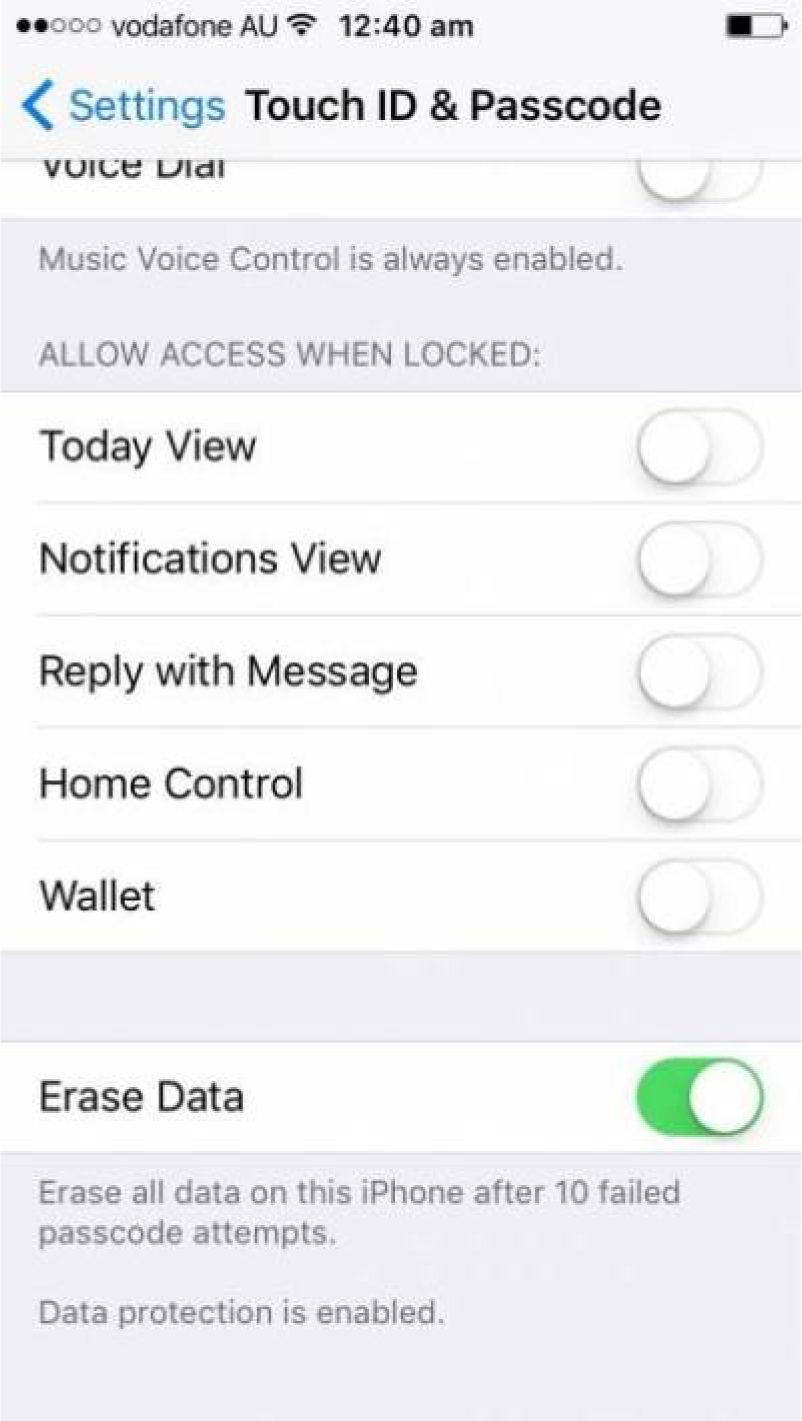
Location accuracy and nearby services are improved when Bluetooth is turned on.

Consider using an app-lock application to require a pin or other verification before opening particular apps, so that if people do get past the lock-screen, they'll still have an added layer of security to get through before accessing sensitive information.



Consider enabling remote locking and wiping functions on your device, if supported. If something happens to your device, this will allow you to lock your phone or wipe it, even if it's not in your possession.

Consider using auto-wiping functions. iPhones, for example, have a setting you can enable to automatically wipe the device if the pin is entered incorrectly a set number of times.



●●○○○ vodafone AU 12:40 am

< Settings Touch ID & Passcode

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.

Don’t leave your device unlocked and unattended in public areas, even for a short time. Treat it as you would your wallet – never let it out of your sight. Also be very cautious of lending it to people, even if they seem harmless, and never let them out of your sight if you do. Handing over your unlocked phone can leave you vulnerable.

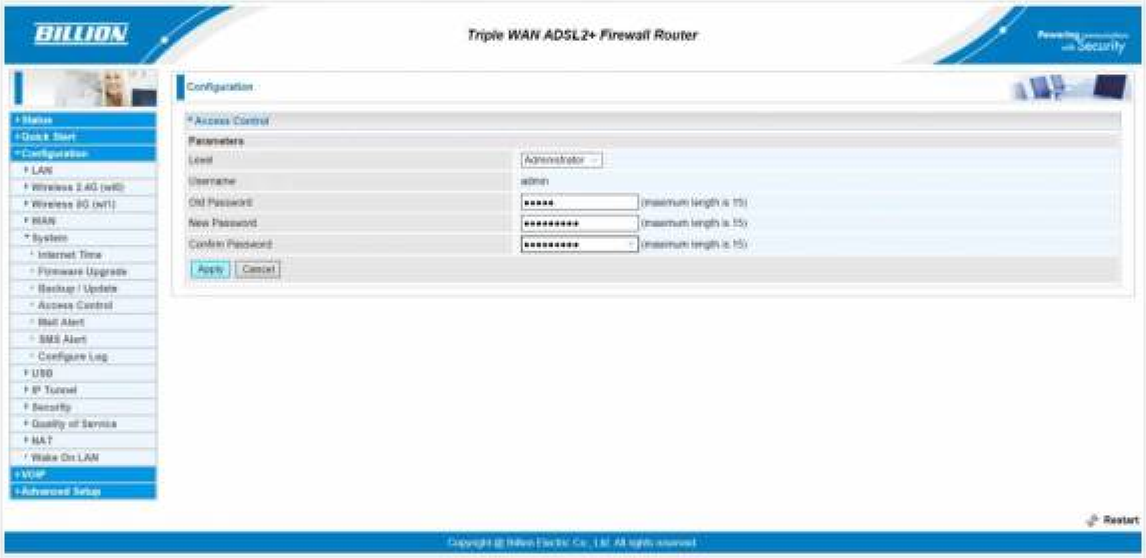
Consider including emergency information as a picture on your lock screen. If you do misplace your device, this may help get it returned. You can include contact details for a trusted friend, for example.

Step Two - Secure your Internet Connection

Setting up your home Wifi

Your internet connection allows your computer (and other connected devices) to communicate to the outside world. If your connection is not secure, it may allow others to access your computer and personal information, or to use your connection without your permission for whatever purpose.

Change the administrator password from the default on your router. Default passwords for many routers are available easily online. Choose a strong and secure password to replace it. (This screen will look different, depending on your router)



Configuration

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)

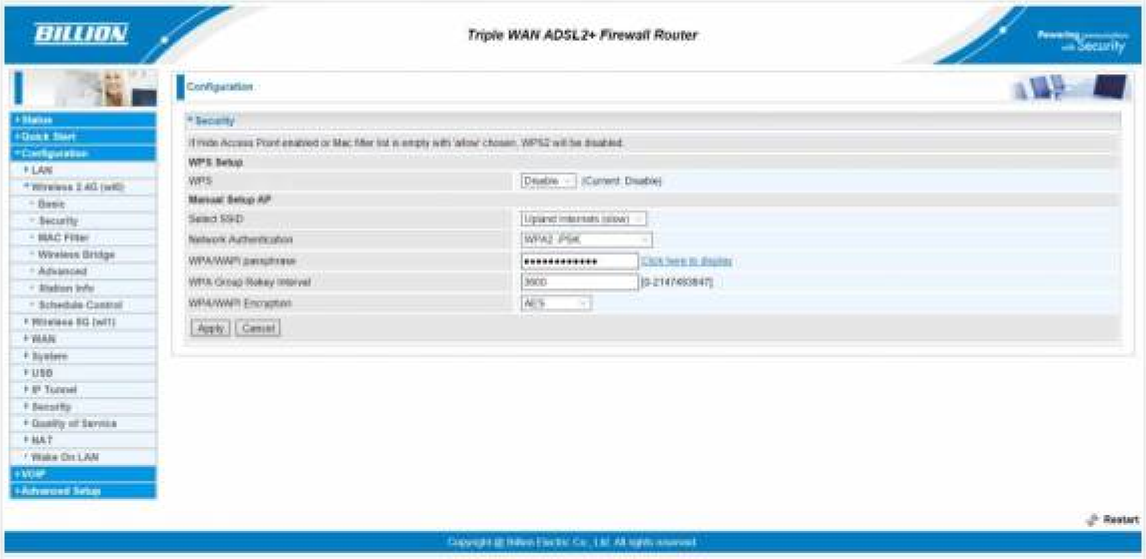
Apply Cancel

Disable remote router management. If people can access your router remotely, it makes it easier for others to make unauthorised changes – especially if you've kept the default administrator password!

Use strong encryption. WPA2 is the strongest encryption protocol currently provided. If your router was produced before 2006, it will not have this option, and it will be more vulnerable than newer models. (This screen will look different, depending on your router)

Give your SSID (Service Set Identifier) a unique but non-identifying name. E.g. 'Wifi art thou Romeo' rather than 'Billion7800N' (default router name makes it easier to find default login details, for example) or 'John Doe at 123 Fake Street' (personally identifying information)

Set a strong password as your Network Key. This is not the same as your administrator password (to edit the router settings) – this is the password people will use to gain access to your wifi network. If you want to revoke access once you've given that password to someone, you'll need to either 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: Upand internals (slow)

Network Authentication: WPA2 -PSK

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

WPA Group Rekey Interval: 3600 [0-2147483647]

WPA/WAPI Encryption: AES

Turn off Guest Networks that don't require a login. Only give access to people you can trust to use your network responsibly.

Activate your router's firewall if it isn't turned on by default.

Keep your router firmware up to date. Some routers will let you check this with a button directly on the router – others will require you to log into the device to check.

Consider using a VPN. VPN stands for Virtual Private Network, and acts as a tunnel between your computer and the internet through a third party server. It is an added layer of protection against potential prying eyes.

Consider physical access. Someone with quick physical access to your router may be able to pair a device with it quickly by pressing a button if Wifi Potected Setup (WPS) is enabled. Consider disabling WPS or only allowing access to the physical router to people you trust.

Using Public Wifi

Free wifi is useful, but it does come with security risks. It pays to be safe when using public wifi options.

1. **Only use public wifi offered by networks you know and trust.** Eg, the State Library wifi. Avoid obviously dodgy networks – eg, an open network with the name 'Free Wifi'. Verify the network with staff before connecting, if you have to
2. **Opt for password protected public wifi** if possible, over fully open networks. E.g. some places will only give passwords if you're buying a coffee, rather than giving access to everyone all the time
3. **If the network presents terms of service and privacy notices, read them.** There can be important information about how they use your data, what kind of content is restricted, etc.

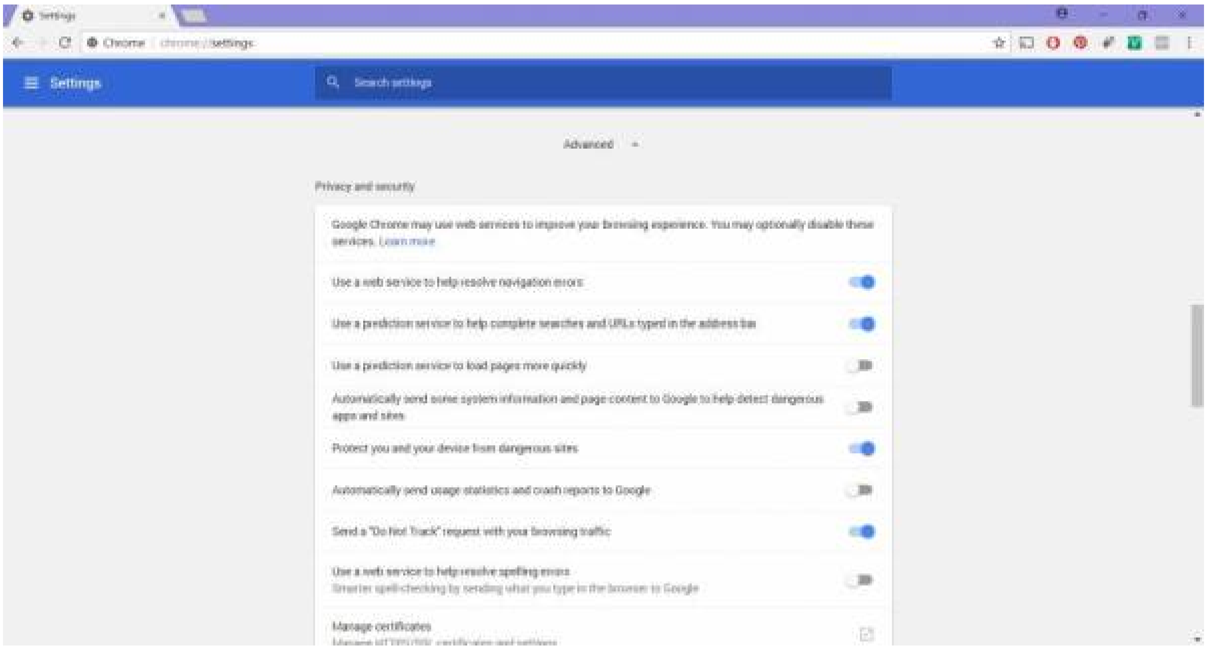
1. **Avoid working with sensitive data if using public wifi**, such as logging into secure sites, online shopping, sending personal emails with identifying data, doing internet banking, etc. If you must do something with sensitive data over a public network, make sure you're using a secure site to do so
2. **Make sure you have secured your device** as mentioned in the previous steps. E.g. make sure you have anti-virus and firewall software installed
3. **Identify the network as a public network when you connect**, if connecting via computer. Turn off file sharing, and consider turning off location services also

1. **Turn off wifi when not in use.**
2. **Consider avoiding public wifi altogether.** Tether your mobile phone to set up your own mobile hot-spot if you need to use the internet on other devices (like your laptop). Setting up a mobile hotspot with your device will differ depending on your model (and Android vs Apple), but guides are easy to find online if needed.

Interesting viewing: 7 year old hacks into public wifi network in just over 10 minutes. https://youtu.be/qQVCHt5S9B0

Step Three - Secure your Browsing

Different Browsers offer different levels of security. It is a good idea to check the security and privacy settings, so you know what information is being shared. Sometimes these settings are under the 'advanced' options.

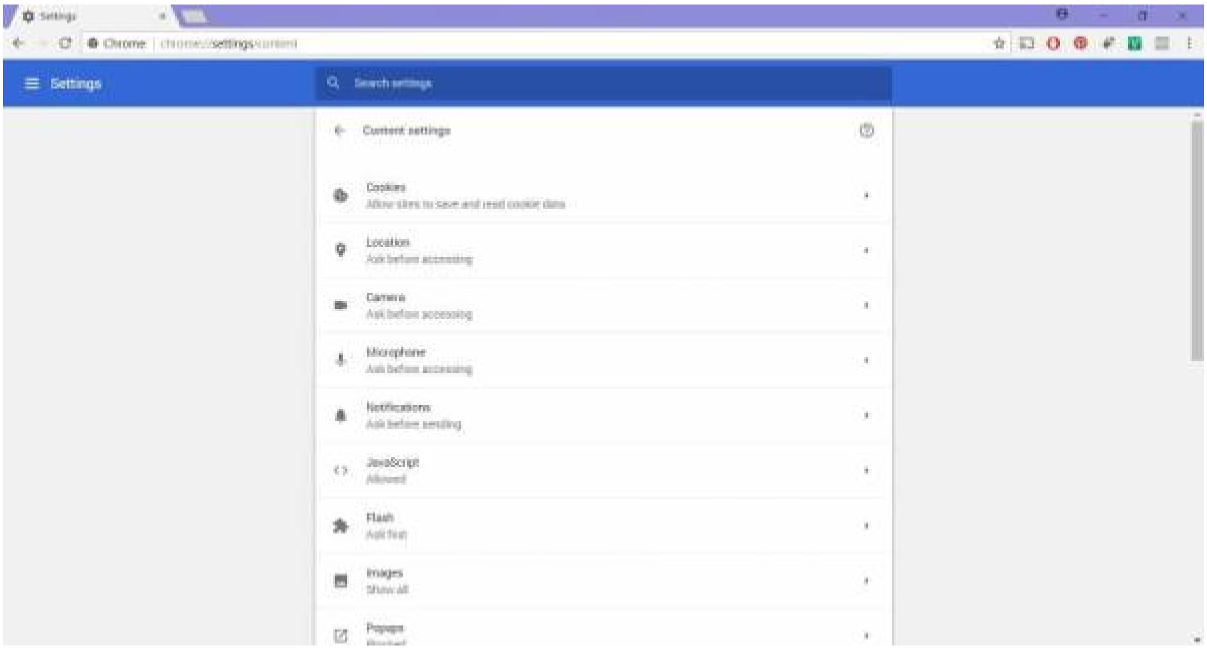


Privacy and security

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

Note some of the content options below.



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 software features that provide functionality to a web browser may also introduce vulnerabilities. You can turn these off completely, or in some browsers, turn them on only sometimes.

Cookies are files placed on your system to store data for websites. They can contain any information that a website wants to store. Eg, the sites you visit, or login to access the site. They can only be read by the website that made the cookie.

Cookies can be a privacy concern, as they can track visitor information. If intercepted, it can give attackers the information contained in the cookie – e.g. login credentials

Java is a programming language used to develop active content for websites. Java applets usually execute within a “sandbox” (interaction with the rest of your system is limited).

There are potential vulnerabilities that could allow it to ignore these restrictions. Signed Java applets can also ignore sandbox restrictions, but users often need to authorise them before they load

JavaScript is a scripting language used to make websites interactive. There are specifications in the JavaScript standard that restrict features such as accessing local files

ActiveX is used by Microsoft Internet Explorer to allow the browser to use other applications. It can be quite vulnerable to attack **VBScript** is a scripting language also unique to Internet Explorer. These are not used often. Use them only if you need to

It is up to you to decide what to allow, and what to restrict, along with other content settings, such as allowing access to camera, microphone, location, etc.

1. **Check for 'HTTPS:' in website addresses.** Don’t enter sensitive information into any site that doesn’t use it.
2. 'HTTPS:' indicates that the site has a SSL (Secure Socket Connection) Certificate installed.
3. SSL encrypts the traffic between you and the website, so that other people can't see your information.

Ensure you’re happy with your privacy and security settings.

Be careful when you install browser plugins and extensions. Some may introduce vulnerabilities, so do you research first.

Always keep your browser up to date. Updates often include security patches to reduce vulnerabilities.

Only enter information into sites with 'https:'

Step Four- Secure your Accounts

Passwords are the first line of defense to secure your accounts – they should be something only you know.

Cyber-criminals can crack your passwords, if given the chance:

1. Specialist software can use a brute-force attack to test hundreds of letter, number and symbol combinations very quickly, much faster than any human
2. A dictionary based attack will cycle through common words used as passwords
3. Guesses can be made based on personal information they know about you

Also give consideration to your username. E.g. ‘admin’ is a very easy username to guess if you’re the administrator of a website!

How to pick a password

Do:

1. Use numbers, upper case and lower case letters, and symbols
2. Create something you’ll be able to easily remember
3. Create a long password – at least 8 characters (except where the site won't let you)

Don’t:

1. Use common words/phrases
2. Use words or numbers that could be easy to guess (e.g. your dog's name, your birthday)
3. Repeated characters or predictable combinations (eg, 1234)

Easy method of password generation

1. Think of a sentence you can easily recall
2. Use a part of each word (e.g. 2 or 3 letters from each)
3. Use numbers and symbols instead of letters. Use some capitals too.

E.g.:

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

Other example passwords:

1. **I ate six sundaes** = 186SunD@e5
2. **M**ay **t**he **force b**e **with you** = Mt4bw1thU
3. **Her**bs **are t**he **best** = herRtb3sT

Try doing it in a different language – it can make it even more difficult to crack!

Password Security

Make your passwords different

Don’t use the same password and password/username combinations across all accounts. Use different passwords when possible.

This can be easy! You can put extra letters in your password to make them different. E.g.

1. Gmail Password: 18**GIL**6SunD@e5
2. Facebook Password: **FOK**186SunD@e5
3. Twitter Password: 186SunD@e5**TW**

Be careful

1. Try not to use your passwords on public networks, or on public computers
2. Don’t ‘save’ passwords on computers unless you are the only user.
3. Always log out after using accounts in public places (e.g. on work computers)
4. Don’t enter your passwords through links in unsolicited emails or phone-calls - they might be a scam. Always go directly to the site or call the company if you are not sure.

1. Don’t enter passwords on non-secure sites (ones that don't use 'https:')
2. Don't share your passwords with others
3. If you need to keep a record of your passwords, write them down and hide them. Don't keep passwords in emails or on a file called ‘passwords’ on your computer.
4. You can use a password manager. If someone else uses your password manager though, they will have all your passwords
5. Use Two Factor Authentication if you can

What if your account is used by someone else?

If you think your account has been used by someone else, change your password/s immediately and/or perform a password recovery. If you use the same passwords across other sites, change all.

Password recovery

When you set up a password, you may also be asked to provide a secret question and answer set to be used for password recovery. Common examples include:

1. What is your mother’s maiden name?
2. What was the first street you grew up on?
3. What was the name of your first pet?

Use information only you can know (You can even use fake information, if you can remember it!). If your password is strong, but your password recovery is weak, you ca still be hacked - especially if a cyber-criminal can access to your email account.

Using 2FA

2FA stands for Two Factor Authentication – a type of Multi Factor Authentication. Many sites and services only use one verification method to confirm your identity:

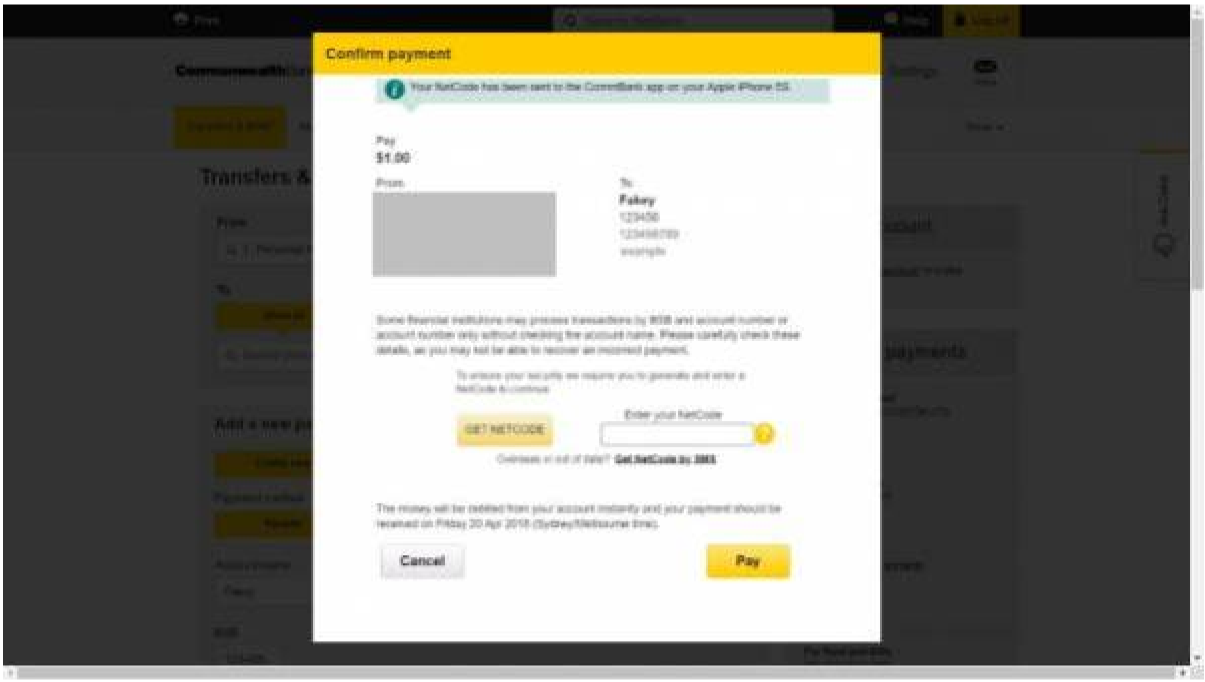
E.g. a Username/Password Combination

Two Factor Authentication adds another layer of security by using at least two pieces of evidence that you are who you say you are. For example:

1. something you **know** (e.g. a pin, a password, or answers to a secret question)
2. something you **have** (e.g. a bank card, security token, your mobile phone to receive a pin via text message or push notification)
3. something you **are** (e.g. biometric data - a fingerprint scan, retina scan or voice recognition)

This can make identity theft harder for a cyber-criminal. It can make your accounts and transactions more secure if you use more than one way to confirm your identity.

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]

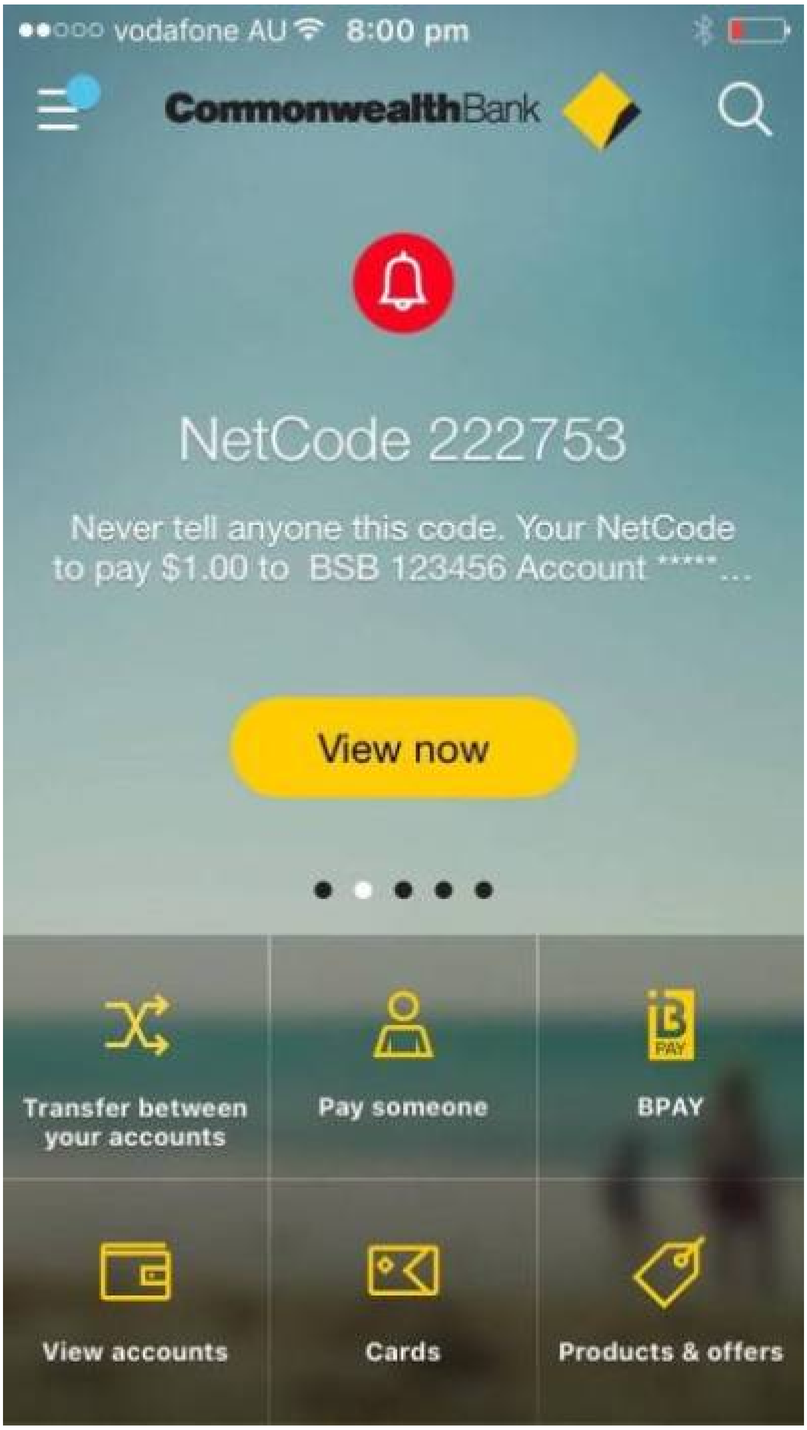
To
Fakey
123456
123456789
example

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.

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 that shows up on your phone to make the transaction



vodafone AU 8:00 pm

CommonwealthBank

NetCode 222753

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

It is a good idea to use Two Factor Authentication if you can.

2FA is not perfect – especially on mobile phones.

1. Security tokens sent by **push notifications** (from an app) are more secure than **SMS**. SMS can be intercepted
2. If you don't have your phone, if it is not charged, or you don't have access to the internet/network, you **can not access your accounts** that use phone 2FA
3. Your phone could be **lost or stolen**. You might keep your email and other accounts logged in on your phone. If someone steals your phone, they could gain access to your email, other accounts, and access to your 2FA method

Two Factor Authentication reduces your risk. It makes it harder for a cyber-criminal to attack your accounts. But it is not 100% perfect.

Spotting Scams and Staying Safe

Many people are tricked with internet scams every day. Scams trick people into giving personal details and secure information (such as login credentials) that can lead to identity fraud. Scams might trick people into giving credit card details and money.

Stay safe by being careful online.

If you think something might be a scam, be safe, and check https://www.scamwatch.gov.au. The site has a long list of common scams.

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

The most important things are:

1. Be aware that scams exist
2. Keep your personal data personal
3. Know who you're dealing with, and know who to trust
4. Keep an eye out for fakes (emails, phone calls, websites, etc)
5. Don't click on anything you don't trust (website links, email attachments, etc.)
6. Be careful if someone asks you for money, personal information, or account details
7. It is better to be safe than sorry

We're going to look at some of the most common scams and how to spot them. There are many more.

Phone Scams

1. Always be wary of text messages and calls from numbers you don't recognise
2. When possible, try to keep your mobile phone number a secret or only known by legitimate businesses who have secure privacy policies
3. Even if your number seems private, scammers can still use random number generators to contact your number

Missed Call Scams are when a scammer calls your phone, but only a short time, so it shows a missed call.

1. Calls are often from international numbers, and may appear as missed calls multiple times.
2. If you call back, you get charged a high rate – much more than a standard call.
3. They might try to keep you talking for a longer time to charge you more.

To avoid this type of scam:

1. Don’t return calls to numbers you don’t recognise – especially if the number is from overseas
2. Don’t return calls to numbers that start with 1900 or 19 (these indicate premium line numbers in Australia)
3. Block problematic numbers if they keep calling

If you do fall victim to this type of scam, contact your mobile provider. Sometimes, they will remove the charges for you

Premium Service Text Scams are when a scammer sending you an unsolicited text message that tricks you into replying. If you reply, you will be charged a premium text rate.

1. These are often disguised as customer surveys, or competitions, such as answering trivia. This is so you reply more (so they can charge you more.)
2. If you do reply, you may also be signed up to a premium services that you don’t know about until you see your next bill.

To avoid this type of scam:

1. Be careful of unsolicited text messages, especially ones that offer prizes. Do not respond to numbers you don’t recognise
2. Do not respond to any number starting with 1900 or 19 (these indicate premium line numbers in Australia)

If you do fall victim to this type of scam

1. Contact your mobile provider. In some cases, they will remove the charges for you or unsubscribe you from this service

Remote Access Scams (a common type of phishing) is when a scammer calls you and claims to be from a technical support service. They tell you that you have a phone or internet problem, and try to get you to hand over personal information, provide login credentials or credit card details to pay for a ‘fix’ the problem.

To avoid this type of scam:

1. Never give an unsolicited caller access to your computer
2. Never give your personal, credit card or online account details over the phone unless you made the call or it’s from a trusted number
3. If you receive an unsolicited call claiming that they need remote access to fix a problem, hang up. Real companies like Telstra or Microsoft will not do this.

If you do fall victim to this type of scam

1. If you have given access to your computer or think it may have been hacked, seek help from a qualified computer technician.
2. If you think you have provided your account details, contact your bank or financial institution

immediately and change credentials as soon as possible

Phishing

Phishing scams are when scammers try to trick you into giving personal information like bank account numbers, passwords and credit card numbers.

Personally identifying information can be used in identity fraud, so always be careful before giving your passport information, licence number, tax file number, medicare number, or other details.

You could get an email, text or phone call pretending to be from a bank, telephone company, tax office or other business, asking you to update or verify your details. They could ask you to give information quickly to secure your account.

They are often designed to scare you – e.g. they could pretend to be from Centrelink and tell you to confirm your details or risk stopping your payment.

To avoid this type of scam:

1. Never click on links or attachments in emails claiming to be from banks or organisations asking you to verify your details or log in using their link. (If you search for the exact words in the email online, you may find that it is a known scam).
2. Check emails against ones you know are real. Do they follow the same format? (Eg, The real ones may use your full name, to prove they are official.) Emails should not have formatting errors, or incorrect grammar and spelling. If in doubt, check it out!
3. Check the email address. Is it from the real organisation? Does it come from a different domain name, or follow a different structure than usual? E.g. NetBankNotification@commmbank.com instead of NetBankNotification@cba.com.au ?

Check website addresses carefully before entering login credentials or other personal information, especially if you didn't type in the website address yourself.

1. Is it secure (uses 'https:')?
2. Is it different from normal – e.g. commmbank.com instead of commbank.com.au?
3. Never provide your personal, credit card or online account details if you receive a call claiming to be from your bank, ATO, Centerlink or any other organisation. Instead, ask for their name and extension number. You can call the organisation directly (using their official listed number) to check

If you do fall victim to this type of scam, change your account details immediately, and contact your bank, financial institutions or other agencies immediately to secure your details.

Buying and Selling Online

Be careful when buying from classifieds without seeing the item in person first. Scammers might use information from real ads to trick you, then tell you that you can't see the item before paying. Eg, they might say they are traveling or have moved overseas, and will deliver once payment has cleared.

1. Check reviews for the seller before buying
2. Use a payment method with fraud protection (e.g. don't pay by money order, wire transfer or international money transfer – try paypal payment instead)
3. If something seems too good to be true, it might be a scam. Eg, rental properties and underpriced big ticket items that ask for payment upfront

1. Be careful when selling on classifieds – especially the buyer wants to pay with a cheque, or want an expensive item (like a car) without seeing it in person
2. The scammer might 'overpay' via cheque, then get you to refund the difference. When the fake cheque is refused by the bank, the scammer will have both the item and the 'overpayment' you refunded
3. Never send items until payments have cleared

Be careful when buying from unknown online stores, especially if they are new social media stores. It is quick and easy for scammers to create a fake store online. ACCC Example Video: https://www.youtube.com/watch?v=3IluT4Jo4f8

1. If prices are too good to be true, it might be a scam. Sometimes you won't receive goods at all – sometimes you will receive goods, but they are not genuine
2. Check for online reviews of the store from trusted sources and real shoppers
3. Check for privacy policies, terms and conditions, and policies about refunds and return. Do they comply with local laws?
4. If they don't accept payment methods that include fraud protection, don't buy. If they're asking for credit card details, is the payment gateway they're using trusted and secure?
5. Does the online store have a way to contact them via methods other than email? Eg, do they have a physical address and telephone listed? If they do list those details, are they legitimate?

If you do fall victim to this type of scam and you have used a legitimate payment method with fraud protection (such as credit card or paypal), you may be able to arrange a charge-back.

You may also want to contact your local Consumer Protection Agency. In Queensland, that is the Office of Fair Trading: https://www.qld.gov.au/law/fair-trading

Online Social Interactions

Socialising online comes with its own set of dangers – especially when it comes to people you've never met in real life. It can be tempting to think that you 'know' someone after chatting to them for a while, or reading what they've sent you. It always pays to be safe.

ACCC example video: https://youtu.be/YDt0F7ETmRU

‘Catfishing’ is the practice of setting up a fake profile to take advantage of people often looking for romantic partners. Catfish profiles are usually set up on dating sites, but can also use social media

1. The scammer may show signs of developing strong feelings for you in a very short space of time. They will try to make you trust them quickly. Always be careful if this happens
2. Consider doing a 'reverse image search' – catfish scammers often use pictures that belong to other people to build up a ‘real’ looking profile.
3. Never send gifts, money or personal details to someone you don’t know in person. Usually the scammer will try to make you feel for them to send these things. Eg, they have a sick relative, or they want to fly to meet you.

If a friend or family member has an account (email, social media, etc) hacked, similar methods can also be used.

1. Sometimes the hacker might message people on social media (eg, by using Facebook Messenger) to tell them that they’re traveling in another country and have no money to get home
2. Because it seems to come from someone we trust, it seems real
3. Confirm the facts with them using a different method – e.g. by telephoning. Be careful if they ask to have money transferred to them by untraceable means – e.g. money order, international transfer, etc.
4. If in doubt, say no

Where to go for more help

There are many more scams than the ones we’ve listed here. It pays to be vigilant against cyber criminals. https://www.scamwatch.gov.au/ provides a comprehensive list of many scams.

If you suspect you’ve been scammed, the Australian Competition and Consumer Commission has resources on how to get additional help here: https://www.scamwatch.gov.au/get-help/where-to-get-help

1. Banking - Your bank or financial institution
2. Cybercrime - Australian Cybercrime Online Reporting Network
3. Financial and investment scams - Australian Securities and Investments Commission
4. Fraud and theft - Your local police - call 131 444
5. Spam - Australian Communications and Media Authority
6. Tax related scams - Australian Taxation Office
7. Identity Fraud - iDcare. iDcare is a free government-funded service which will work with you to develop a specific response plan to your situation and support you through the process. Visit the iDcare website (https://www.idcare.org/) or call 1300 IDCARE (432273)

What is Online Privacy?

Online privacy involves the ability to control what information you show about yourself over the internet, and to control who can see that information.

Some information you give on purpose. Eg, If you set up an account that requires a name, address, phone-number, etc. This is **Personally Identifying Information**.

Other information you might not know you’re sharing – Eg, shopping habits, online search history, or sites you have visited. Most of this information is **Non-Personally Identifying Information** – it is connected to 'someone’, but it could not be used to identify 'you' personally.

Who Owns your Data?

Video explaining who owns your data: https://www.youtube.com/watch?v=y1txYjoSQQc (up to 1.46 minutes is most relevant)

Information may be *about* you, but it is not owned *by* you. It belongs to whoever collects the data.

1. It is important be aware of **terms and conditions** and **privacy policies** before deciding to use a service. For a quick check of some common website conditions - check https://tosdr.org/
2. Your data can be used for advertising, or for making ‘targeted content’. On Facebook, it even changes when posts are shown to you
3. Often we **give our data to get a service**. E.g. if you use Facebook, you give them permission to use your data, so you can connect with friends and family. Facebook profits by ‘selling’ data to advertisers, to make Facebook ads

How to secure your data

1. **Be careful about how much information you share online.**
2. Information such as telephone numbers, your name, address, photos and location tagging can be used to identify you. **Your date of birth is often used in Two Factor Authentication** to access accounts - eg, banking institutions – so **don’t tell everyone**
3. **Secure your browsing** – firewall, anti-virus, vpn, only logging into sites with https:, etc.
4. **Check your privacy settings** and make them as secure as you can

1. **Consider if you want to allow cookies.** Cookies can track information like the sites you've visited. You can turn off cookies in your browser settings, but you may lose other website functionality
2. Consider **archiving or deleting data** and accounts you no longer need. The less information you make available, the less there is to compromise

The only way to be sure your data is truly secure is not to give it in the first place. This is becoming increasingly difficult though as services become more connected.

Is information you put online (especially on social media) ever really private?

Once you put something on the internet, there is no guarantee that it will stay private. Even with the most secure privacy settings, there are still ways people can obtain what you've put up.

1. People who do have access can take **screen-shots** and show people who don't
2. People who do have access may **copy or download your pictures/information** and show people who don't
3. You may inadvertently **give access** to someone with malicious intent (eg, by allowing another app to use your information)
4. There may be a **security flaw** that makes private information public (even login credentials)

The easiest way to keep private information private is not to share it on the internet.

Never have an expectation of complete privacy when you put something online.

Do not put anything on the internet that you would be ashamed for someone you care for to see.

How To Set Your Social Media Privacy Settings

There are many social media channels you may want to use. Each one will have its own terms of service, which identifies how your data is used, stored and transmitted. Most will have a specific page set up to explain how privacy works on that platform.

Today, we're going to focus on the three most commonly used social media platforms:

1. Facebook
2. Instagram
3. Twitter

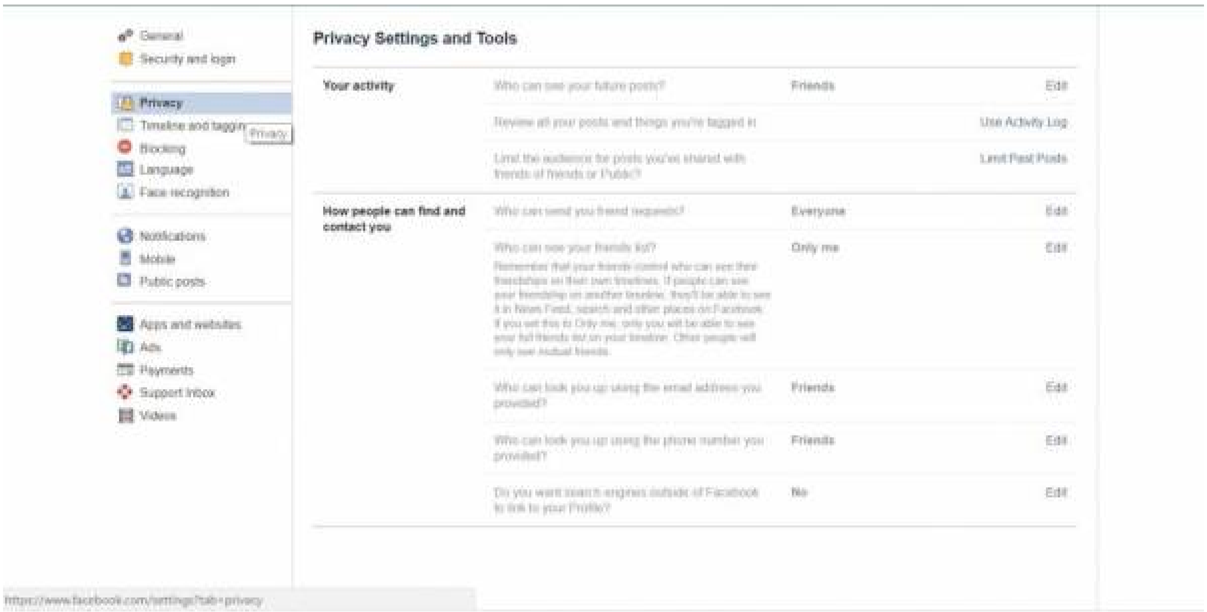
As with email and telephone, you can be scammed on social media. Always be careful.

1. Don't click links you are unsure of - especially shortened URLs that hide the real site address.
2. Be very sure that people sending friend requests are who they say they are. It is easy to set up fake profiles.
3. Be careful of memes that ask you to reveal your birthdate or other identifying details. Some are disguised as quizzes or 'name generators' that trick you into revealing personally identifying information to the public.

Facebook

Facebook offers a number of settings to control your privacy on an account level. These help you decide who sees what you post and how people can connect with you.

You can adjust these on the ‘Settings’ page:

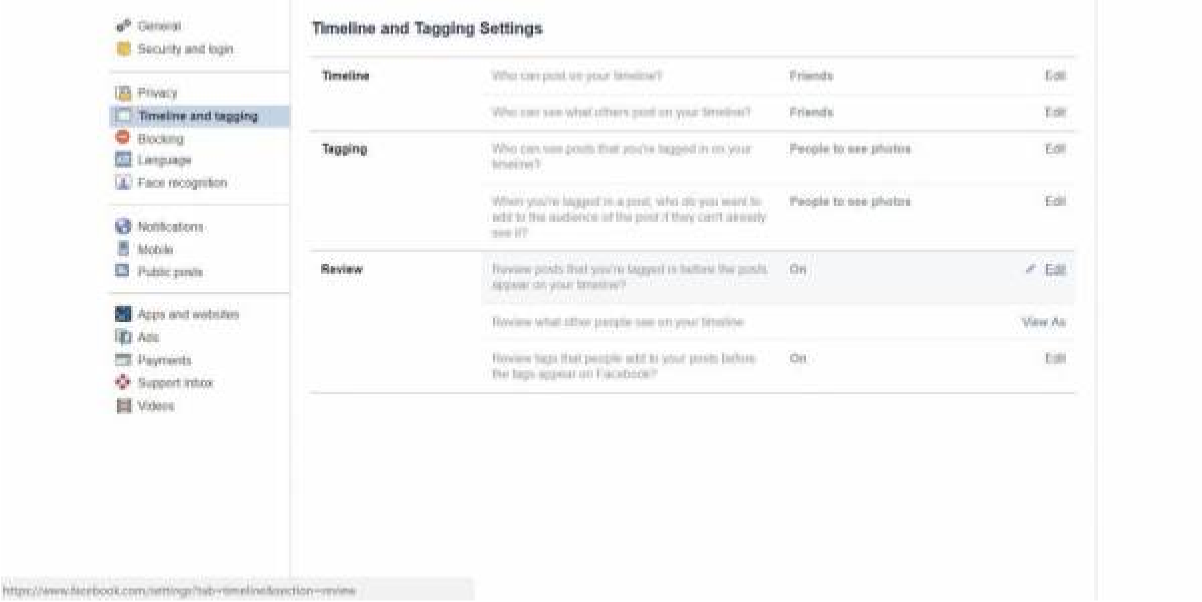


Privacy Settings and Tools

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 settings allow you to restrict who can see what you share, and who can ‘tag’ you in a post. You can make lists to show content to specific groups of people (eg, below, I have created specific lists for ‘people to see photos’)

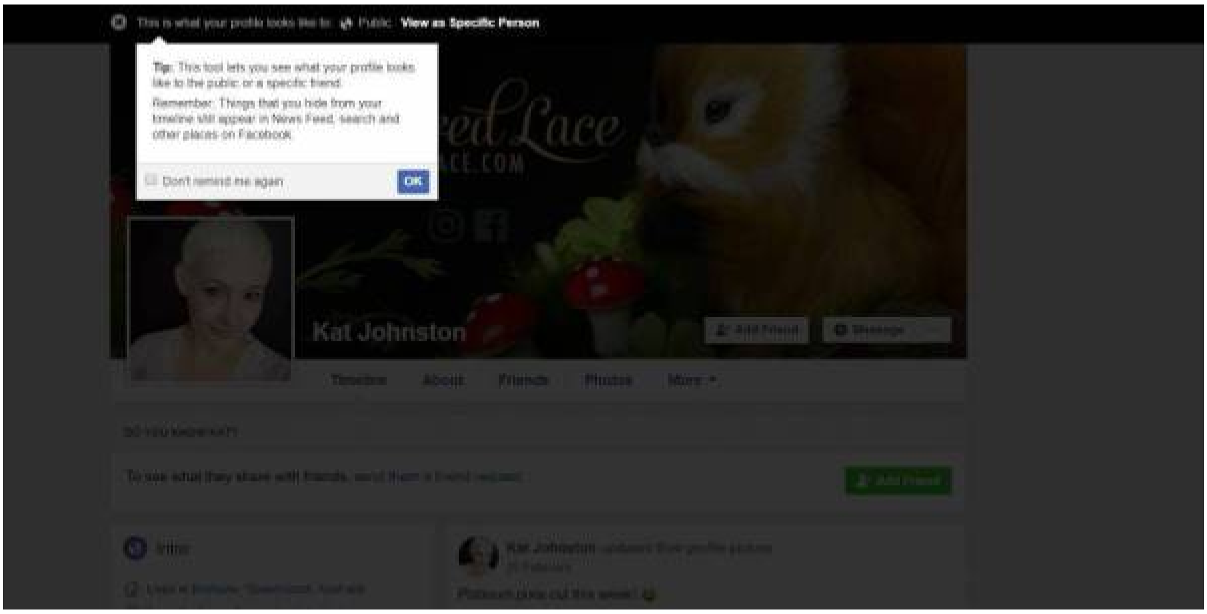


Timeline and Tagging Settings

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

The ‘Review what other people see on your timeline’ option can be very helpful, as it allows you to view your timeline as a general internet user, or even a 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.

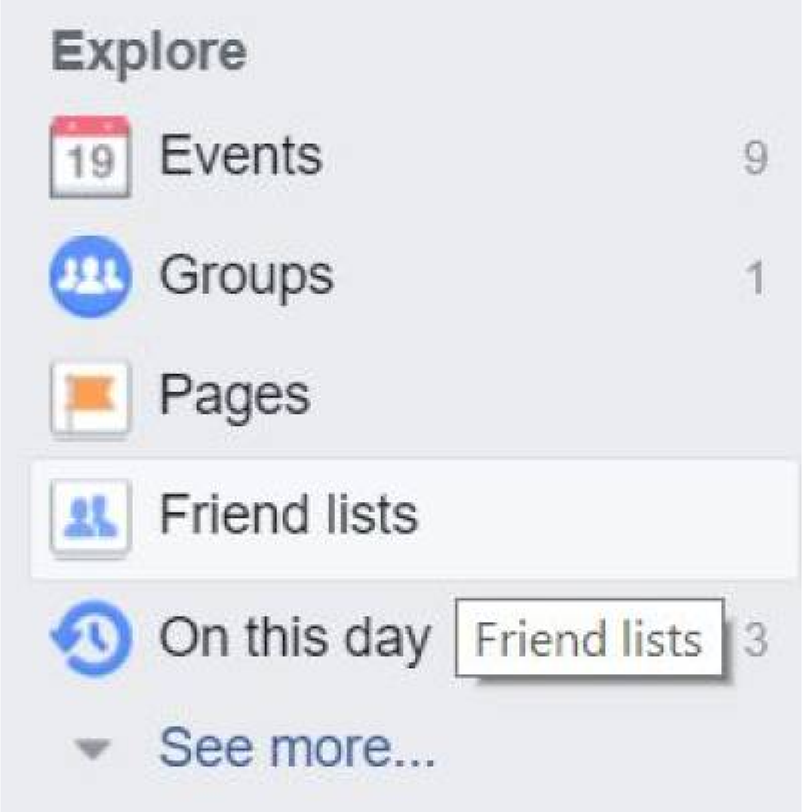
Remember: Things that you hide from your timeline still appear in News Feed, search and other places on Facebook.

□ Don't remind me again OK

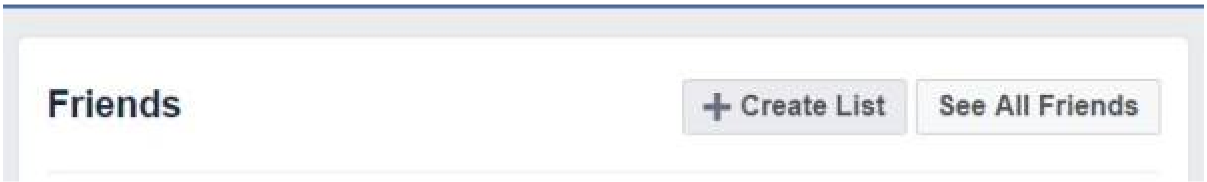
Kat Johnston
Add Friend
Message
Timeline
About
Friends
Photos
More ▾
DO YOU KNOW KAT?
To see what they share with friends, send them a friend request.
Add Friend
Intro
Kat Johnston updated their profile picture.

How to create friend lists

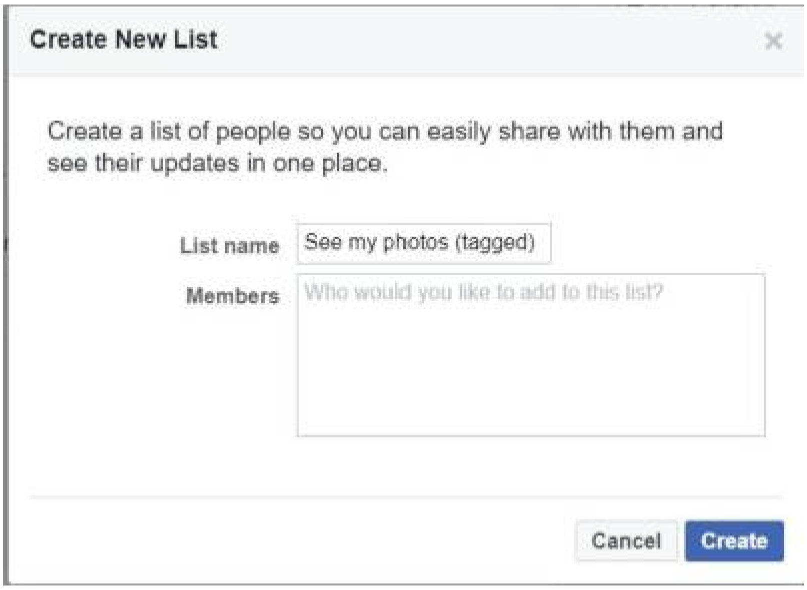
You can create friend lists to share content only with specific people. To do this, go to the Facebook home page, and on the left-hand side, you'll see the Friends lists option.



Select 'create new list' from the options at the top of the screen.



Give your list a name, and add people. You can now use that list when changing your privacy settings.


Create New List

Create a list of people so you can easily share with them and see their updates in one place.

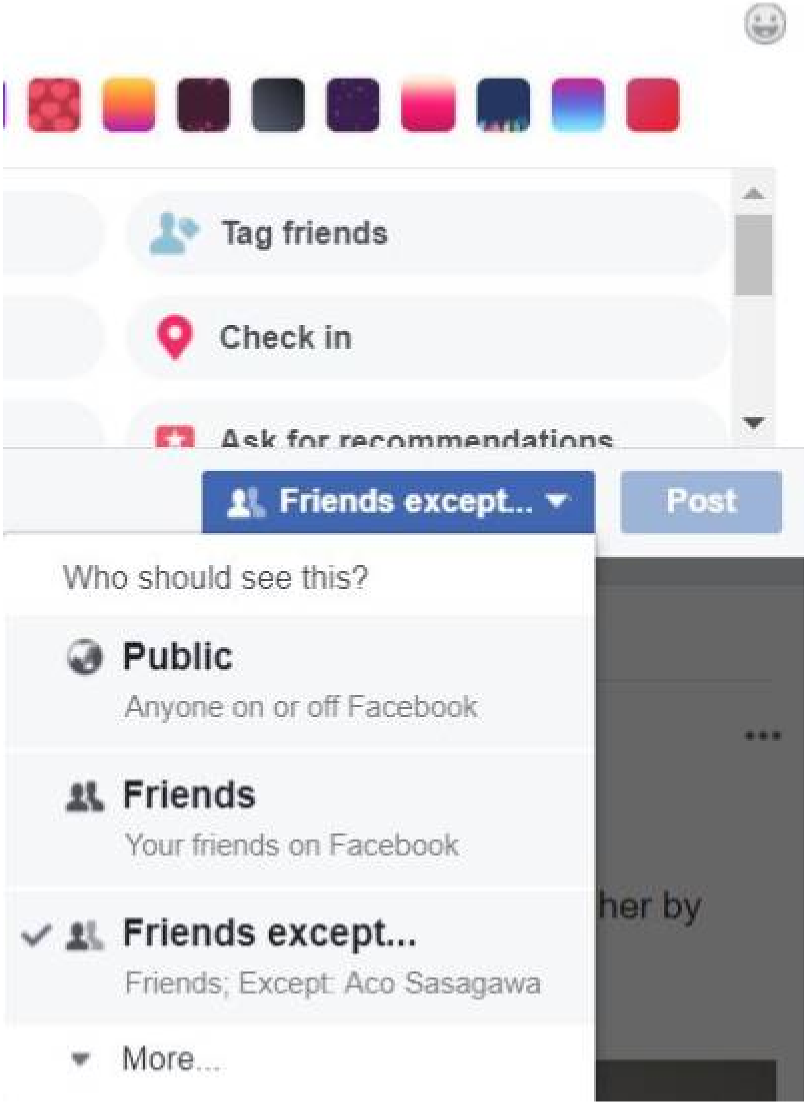
List name: See my photos (tagged)

Members: Who would you like to add to this list?

Setting privacy on individual posts

You can set privacy levels on individual posts. You can use a list, default settings, or exclude just certain people.

Select the privacy setting you want from the drop-down menu. It will stay on this setting by default the next time you post, but you can always change it back.



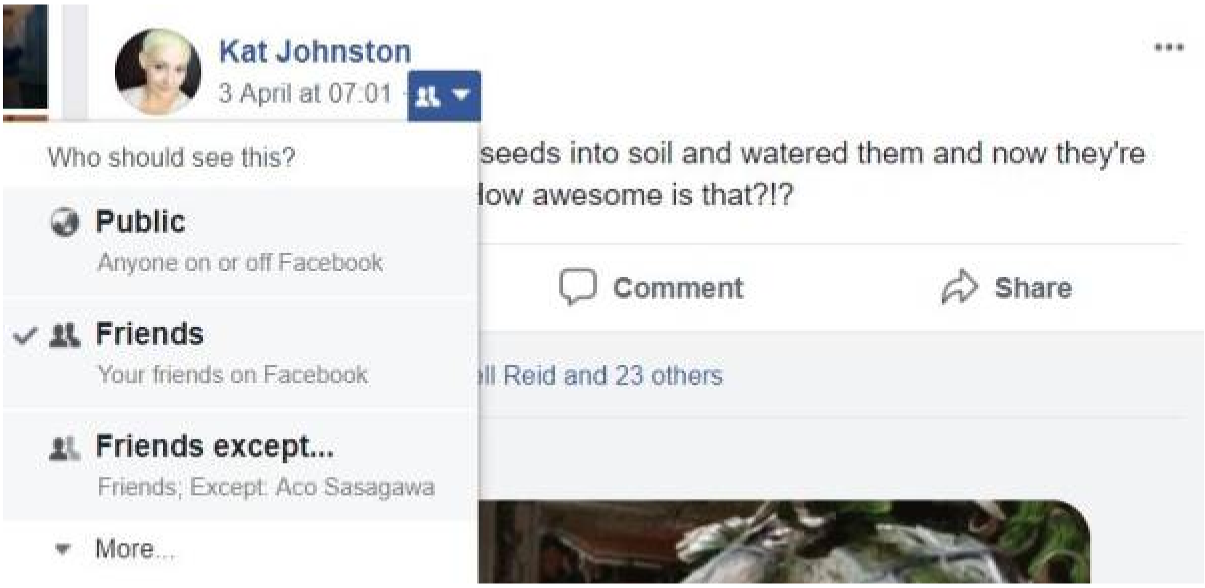
Who should see this?

Public
Anyone on or off Facebook

Friends
Your friends on Facebook

✓ Friends except...
Friends; Except: Aco Sasagawa

If you made a mistake, or you’ve changed your mind, you can change the privacy of a post later, too.



Kat Johnston
3 April at 07:01

Who should see this?

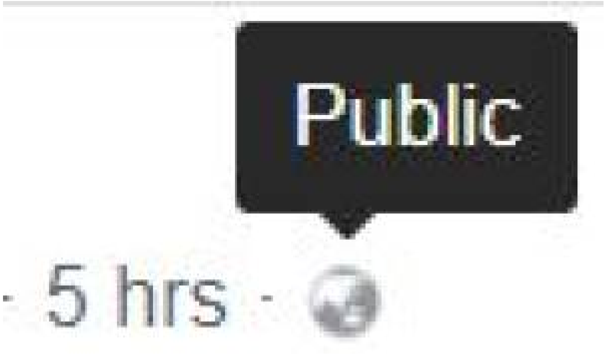
- Public – Anyone on or off Facebook
- ✓ Friends – Your friends on Facebook
- Friends except... – Friends; Except: Aco Sasagawa
- More...

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

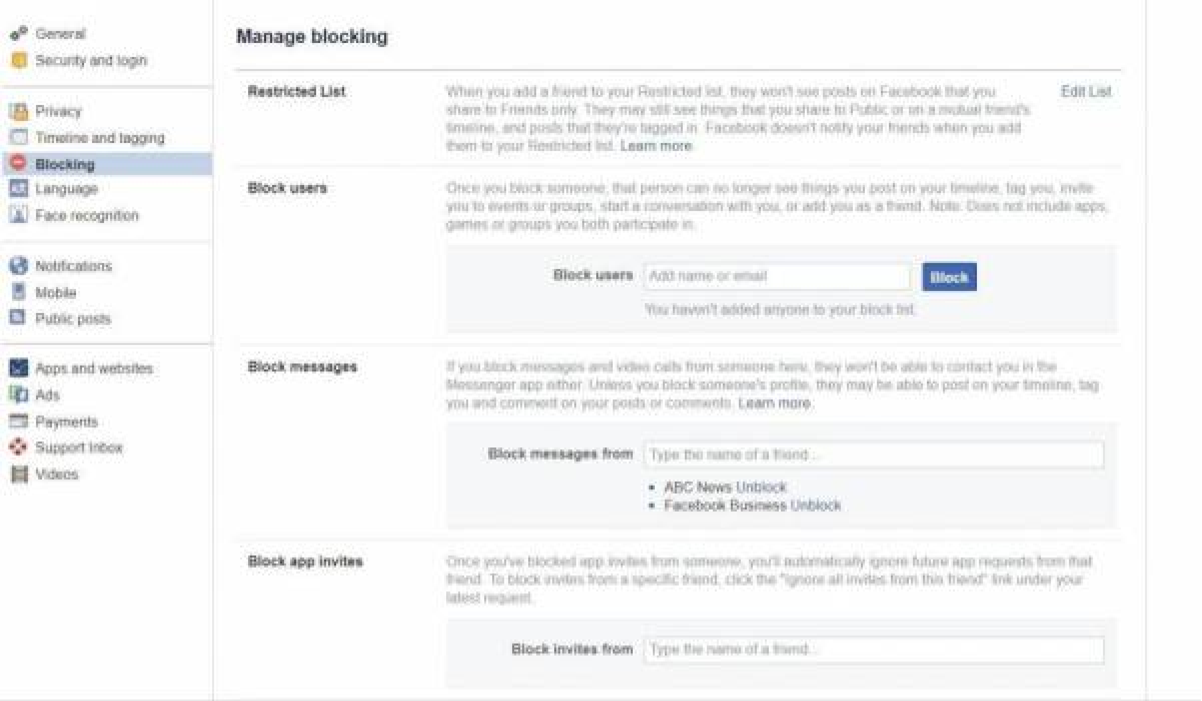
Anyone can do this with their posts. Your comment on someone’s post takes the privacy settings of the original post.

Eg, if it was ‘Friends’ (visible to only their friends) and then changed to ‘public’, your comment will also be visible to the public too.

Facebook Pages and most **Facebook groups** set all post to ‘Public’. If you comment, be prepared to have it seen by everyone. Your account level privacy does not protect your content from being seen if you post in on something marked as public.



Blocking allows you to block activity – you can access this under ‘settings’. If someone is harassing you or bullying you online, it may be a good idea to block them completely. You can also report bad behaviour 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

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.

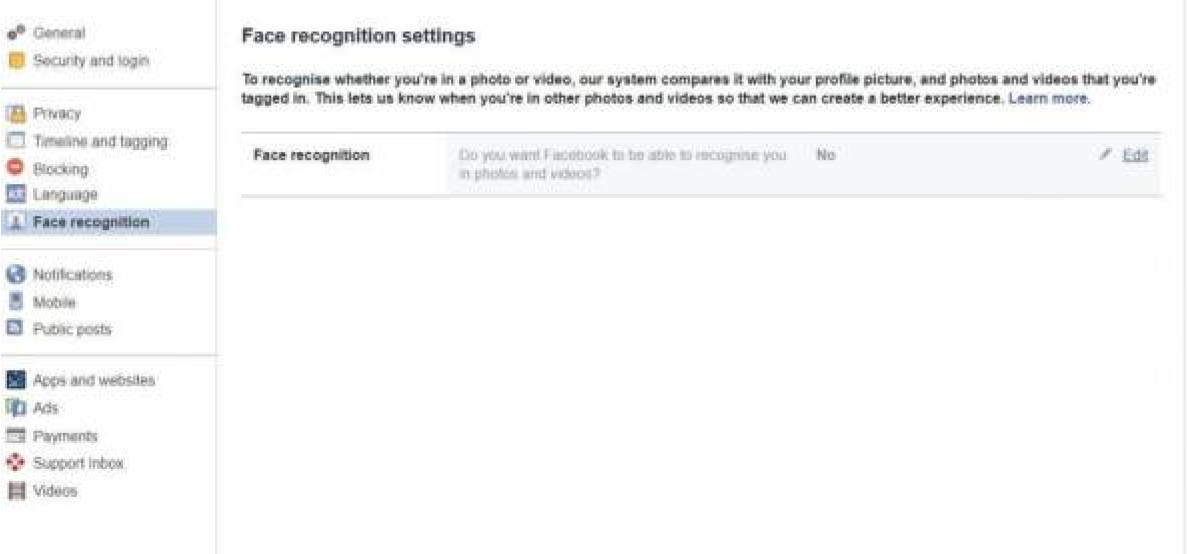
Block messages from: Type the name of a friend...

- 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...

Facial recognition may be something you want to turn off to maintain your privacy to some degree.



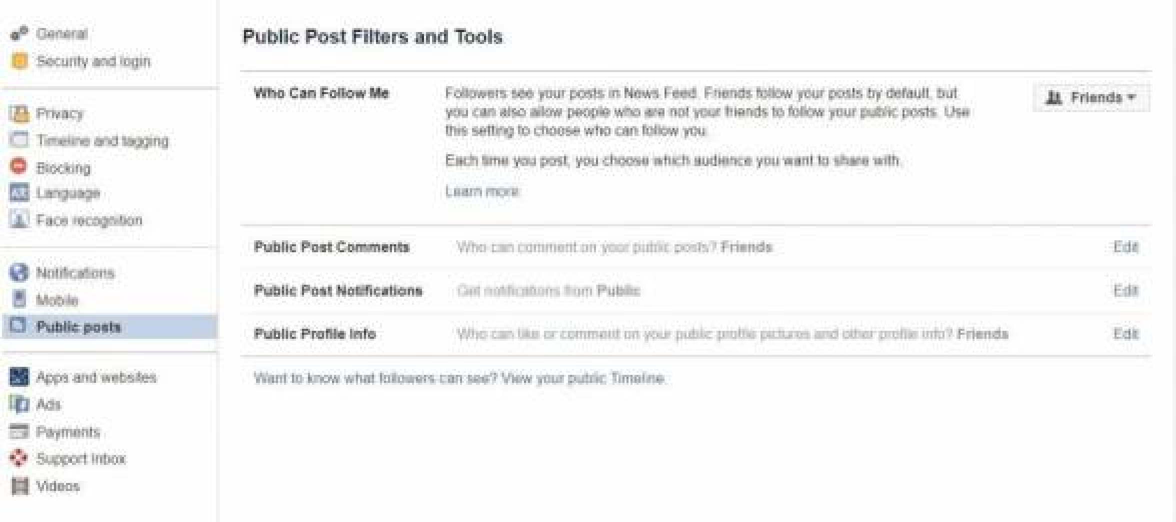
Face recognition settings

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

}}

Some posts are set to public by default – eg, your profile picture, and cover pictures. These settings allow you to adjust who can comment on and follow your public information.



Public Post Filters and Tools

Who Can Follow Me — Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you.

Each time you post, you choose which audience you want to share with.

Learn more

Public Post Comments — Who can comment on your public posts? Friends

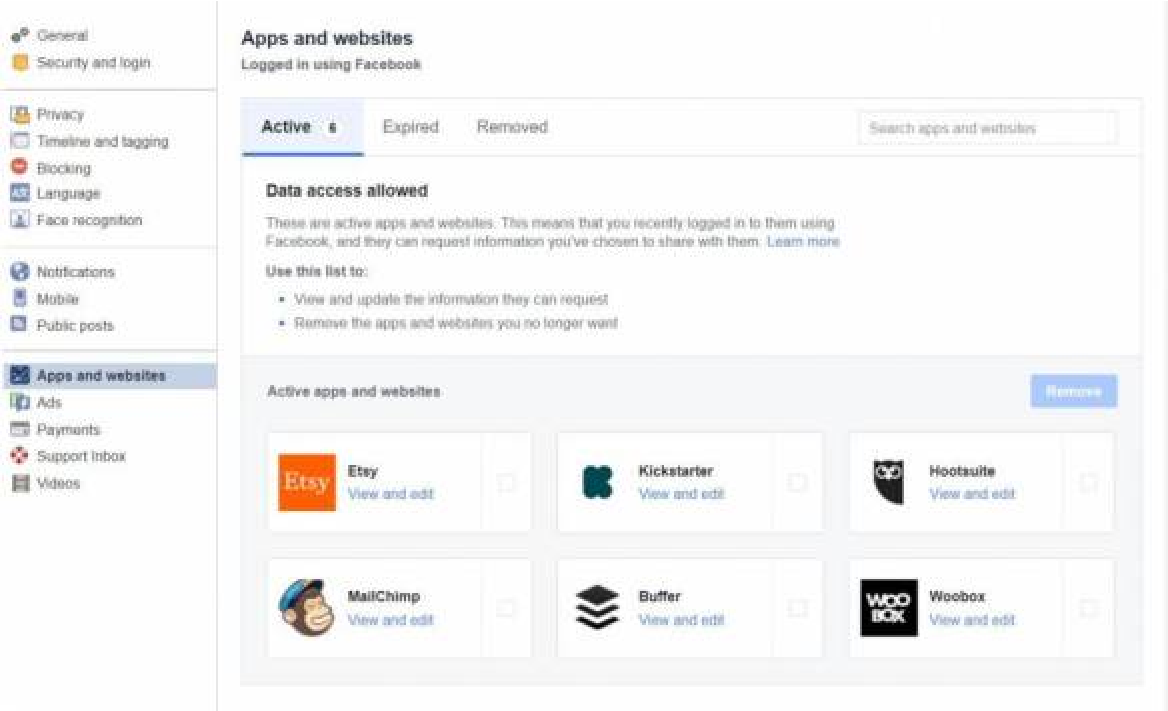
Public Post Notifications — Get notifications from Public

Public Profile Info — Who can like or comment on your public profile pictures and other profile info? Friends

Want to know what followers can see? View your public Timeline.

}}

View and edit the accounts you’ve logged into using Facebook. By logging in using your Facebook profile, you are allowing those sites to access certain information. It is a good idea to regularly check if you are still happy with that 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

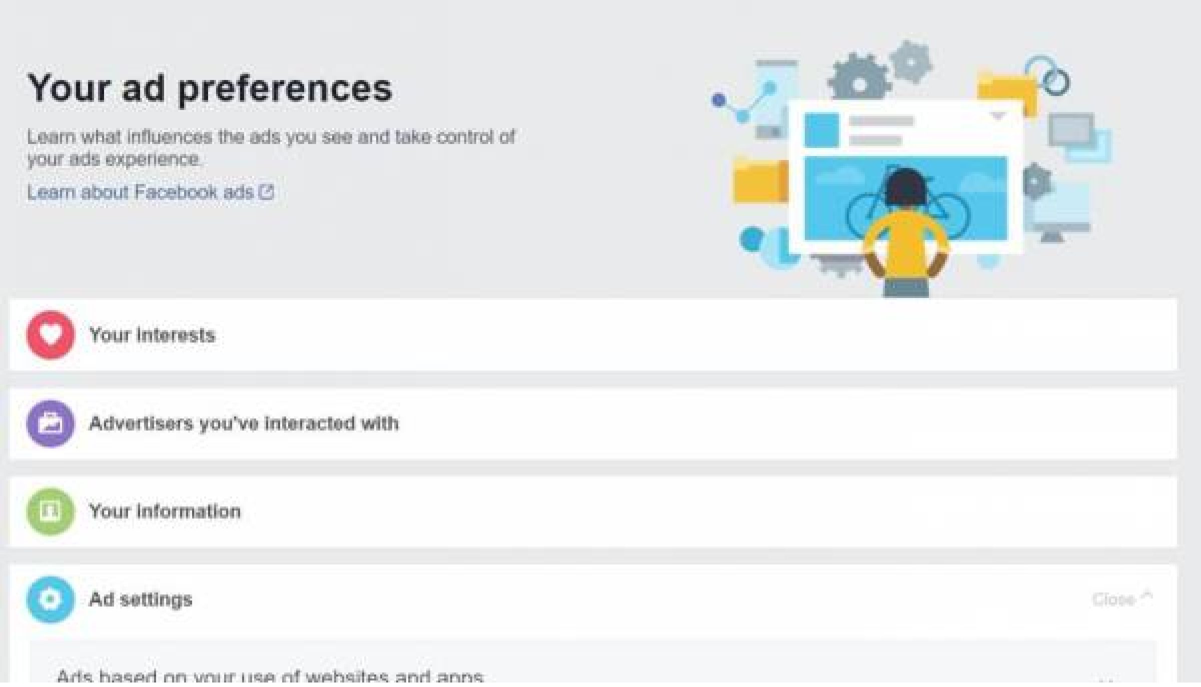
Use this list to:

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

Active apps and websites

}}

The next item on the privacy list is ‘Ads’. Advertisers use the data Facebook collects to show you advertising it thinks you will like.



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

Ads based on your use of websites and apps

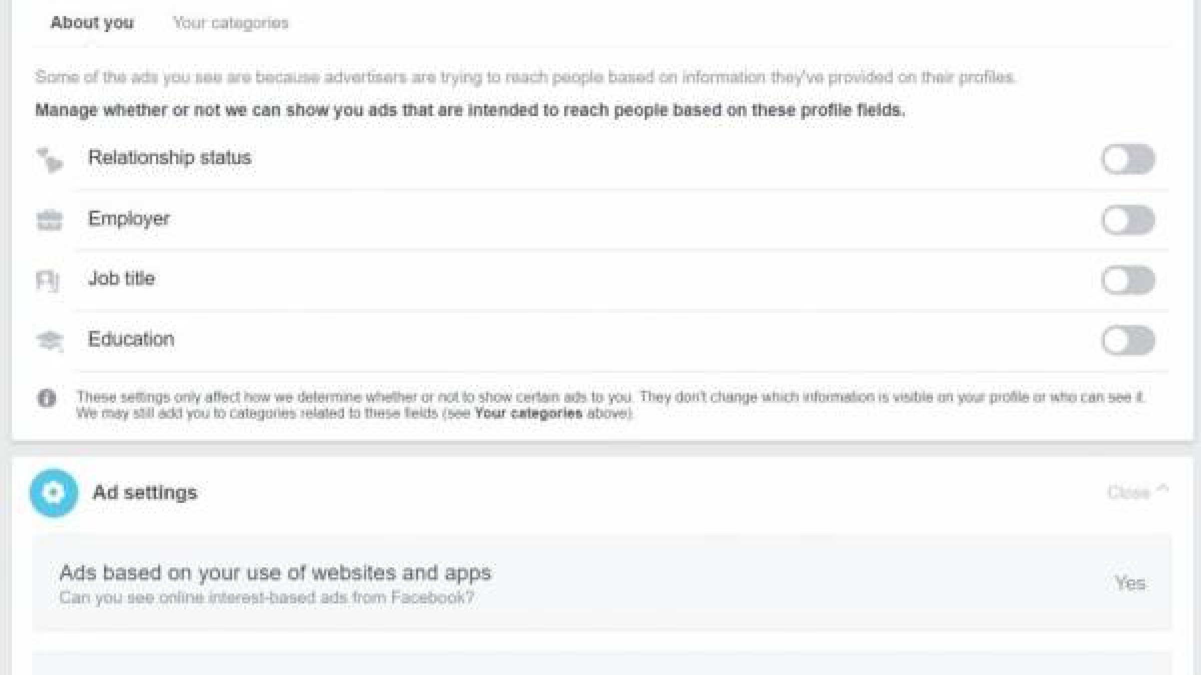
}}

A lot of your data is here. Eg:

1. Companies who have uploaded your contact information to advertise to you
2. What types of ads it shows you based on your interests.

You can remove information from these sections (e.g. your interests), but even if you do, Facebook will continue collecting data and rebuilding those lists.

You can change permissions in this section to allow or 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

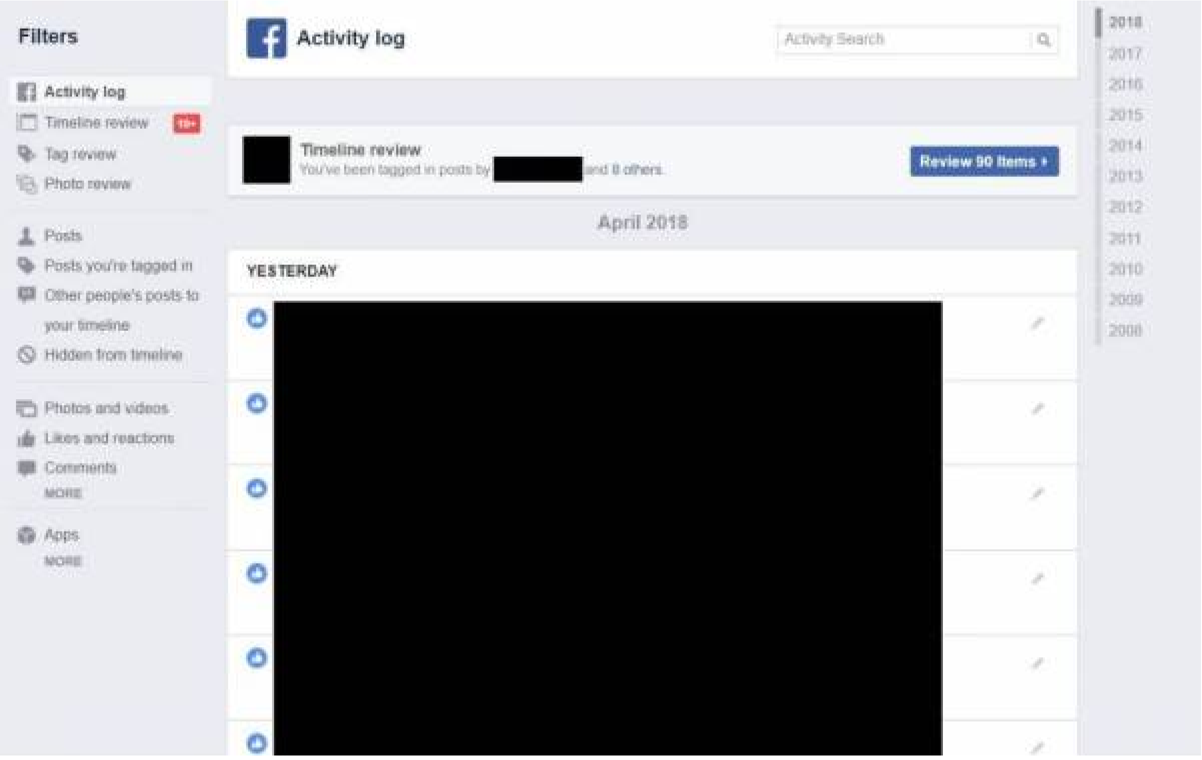
Ads based on your use of websites and apps

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 all that information?** You can remove what you don't need.



[redacted] Timeline review

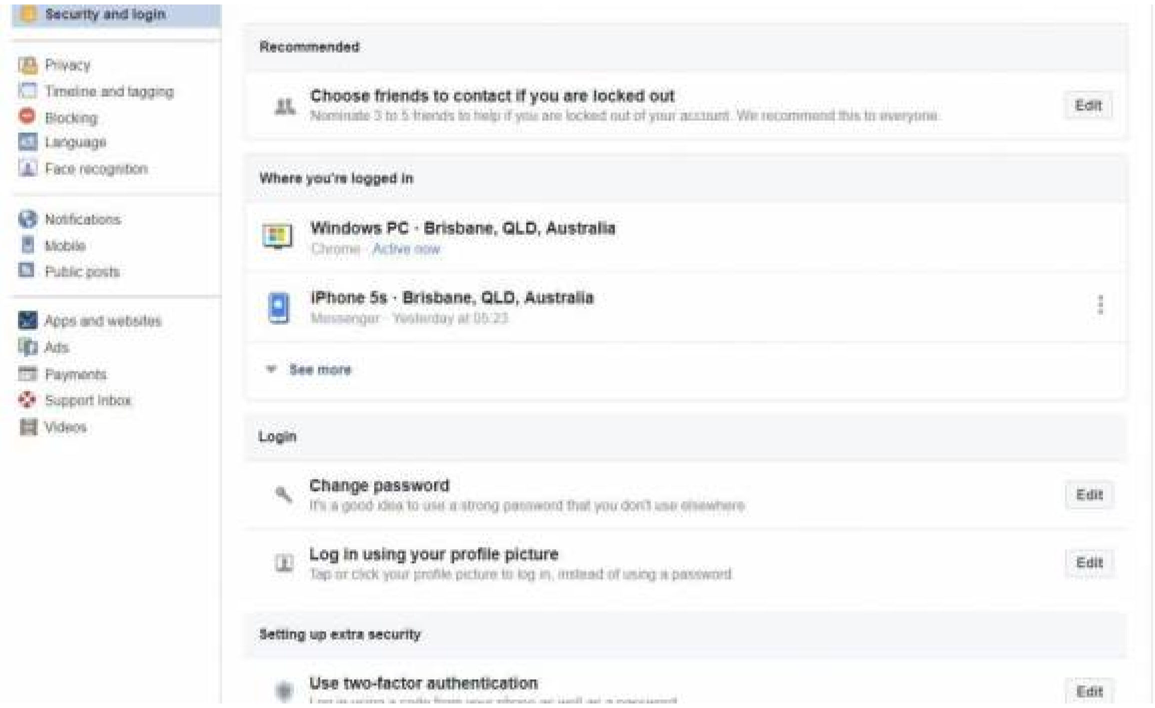
You've been tagged in posts by [redacted] and 8 others.

[redacted]

}}

You can turn on **Two Factor Authentication** or other security log-in settings. You can nominate people to vouch for you if you get locked out of your account.

The security and log-in screen is also where you can review if you’re logged in on other devices, and log out remotely. **If you left it logged in somewhere accidentally, you should log out here.**



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

There is a lot to consider when it comes to privacy on Facebook. Just remember:

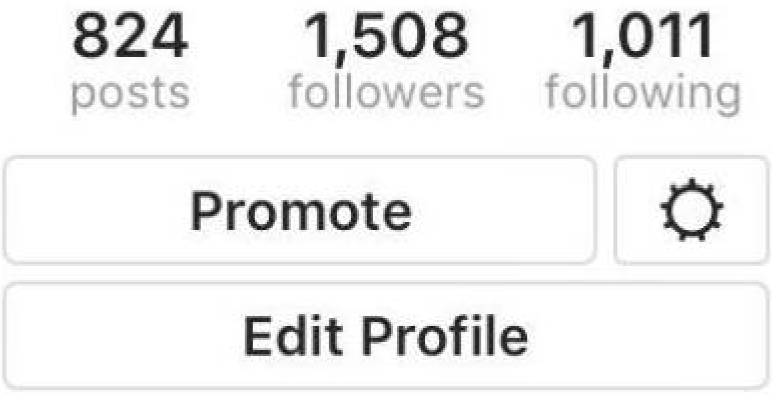
1. **Check your settings** (and retained data) regularly
2. **Assume that nothing is private.** You never know who can see what you post
3. **Be very careful with post permissions.** Remember that people can change them after the fact
4. **Report and block** people who are harassing or bullying you online

If you’re not happy giving so much of your data, consider not using Facebook

Instagram

Instagram is owned by Facebook, so it has similar levels of targeting and data-retention. It is a good idea to review their privacy policy in a web browser rather than on your phone, as it may be easier to read and review. https://help.instagram.com/155833707900388

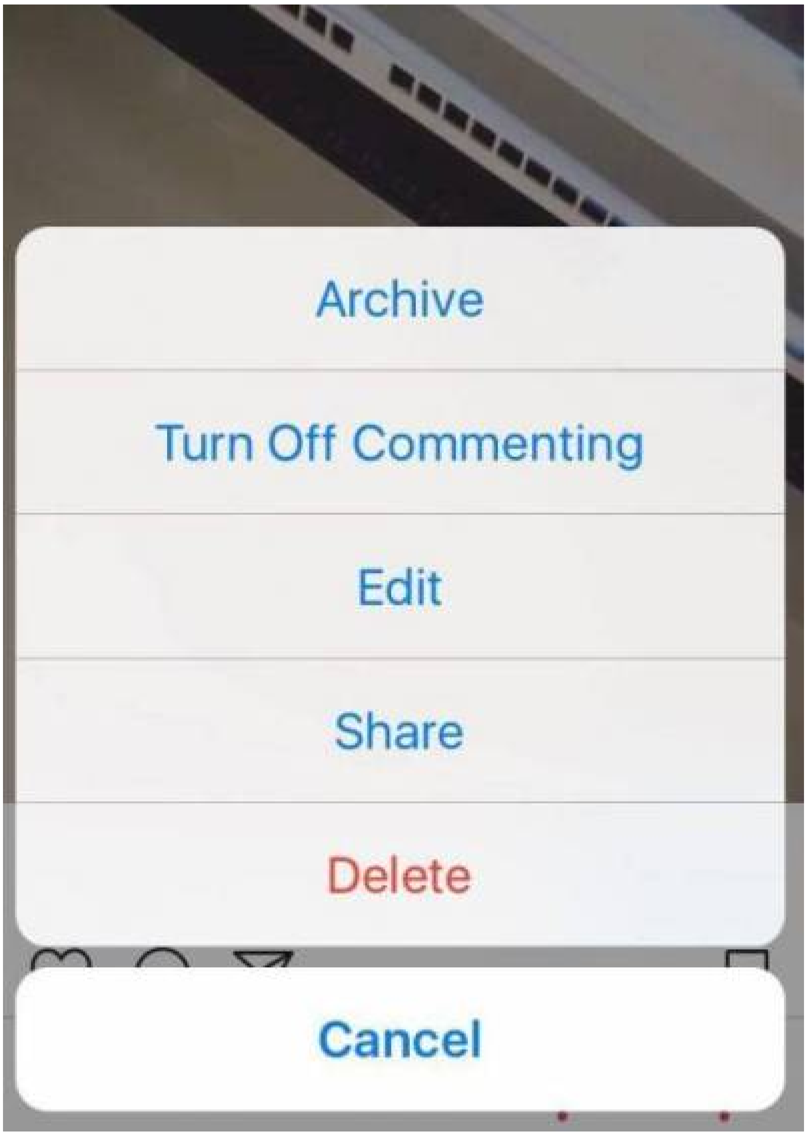
Review your privacy settings by accessing your settings from your profile screen. The ‘gear’ symbol is what you need to click.



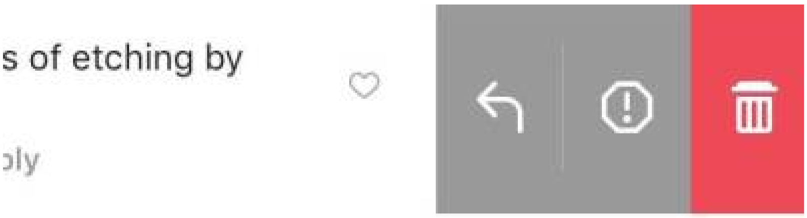
Your options may look different depending on your account type. If you have a personal account, you will have the option to set your profile to private:

1. If your posts are set to public, anyone will be able to see your profile and pictures. If you want to prevent individual people from commenting or liking posts, you can block them
2. If your posts are set to private, your photos will be visible to people logged into Instagram who you've approved to follow you
3. If you share a private post on other social media, people outside of Instagram will be able to see your post (just not on Instagram)

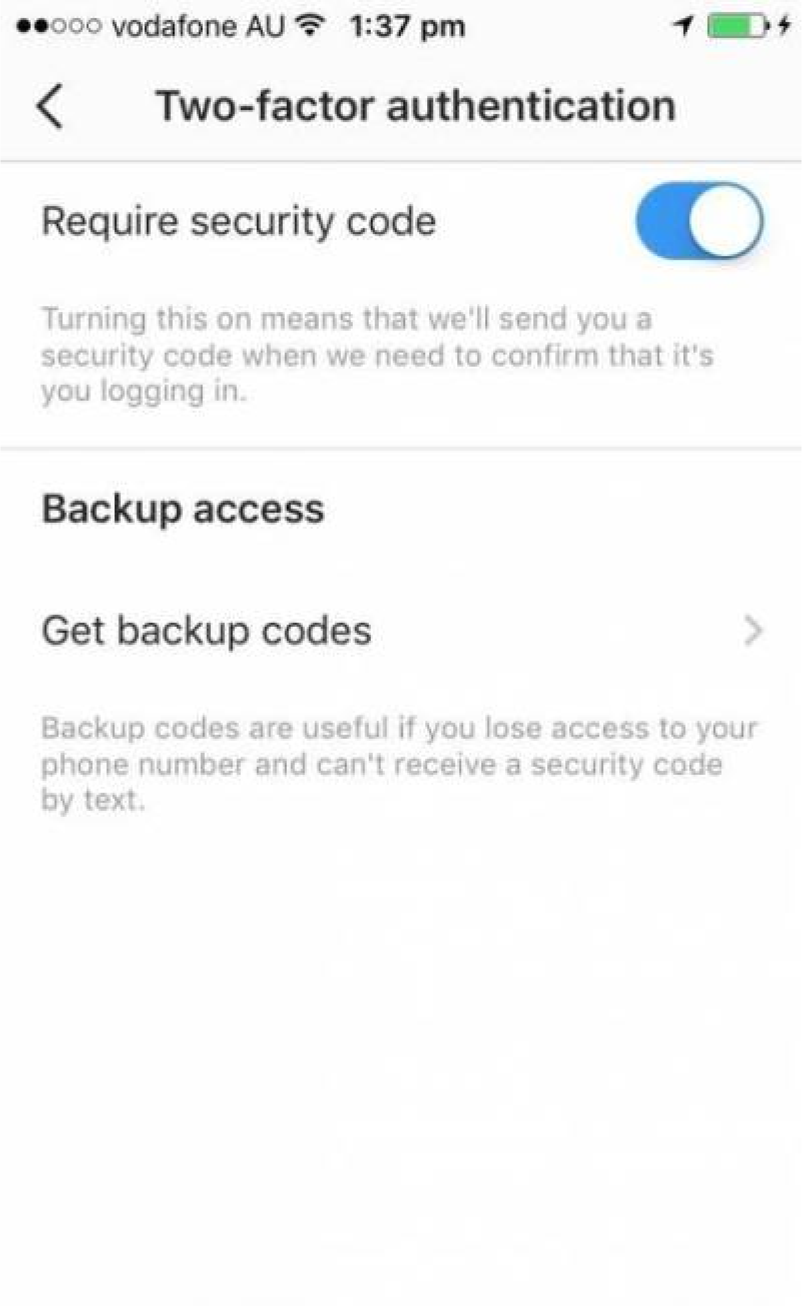
You can turn off commenting on individual posts by click the three little dots beside the post information (…) and selecting, ‘Turn Off Comments’.



Remove or report individual offensive or insulting comments by swiping right on a comment and selecting the appropriate action.



You can set up two factor authentication for your account under the ‘two factor authentication’ tab.



Two-factor authentication

Require security code

Turning this on means that we'll send you a security code when we need to confirm that it's you logging in.

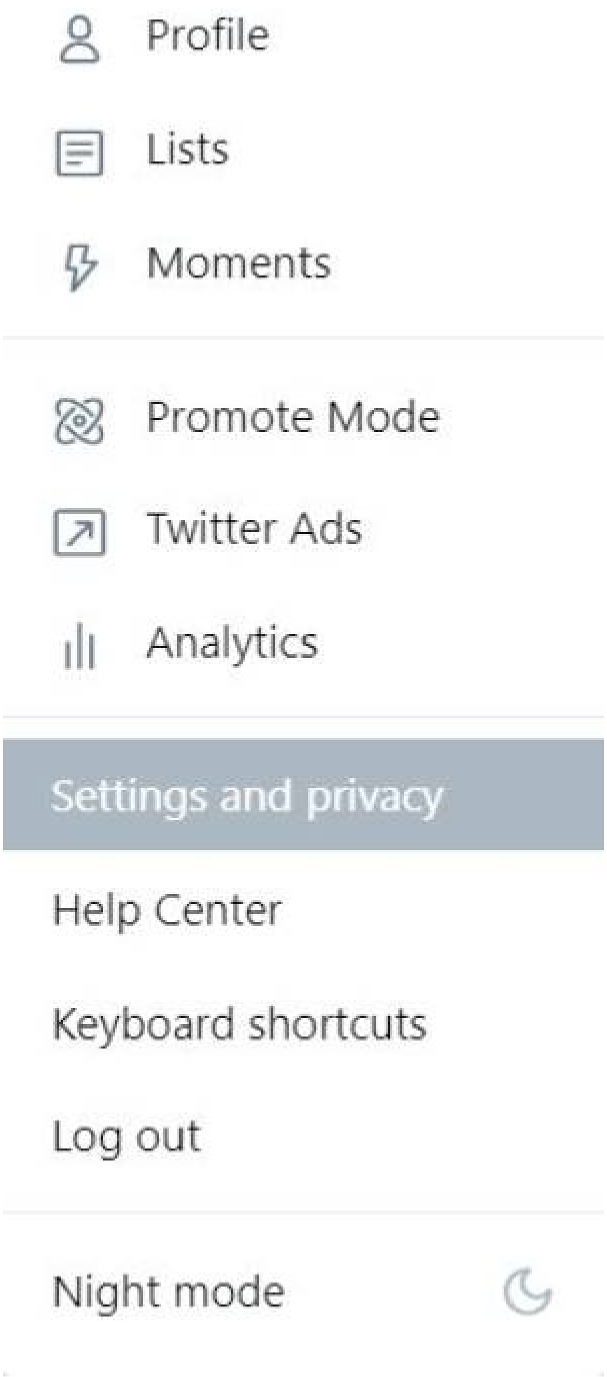
Backup access

Get backup codes

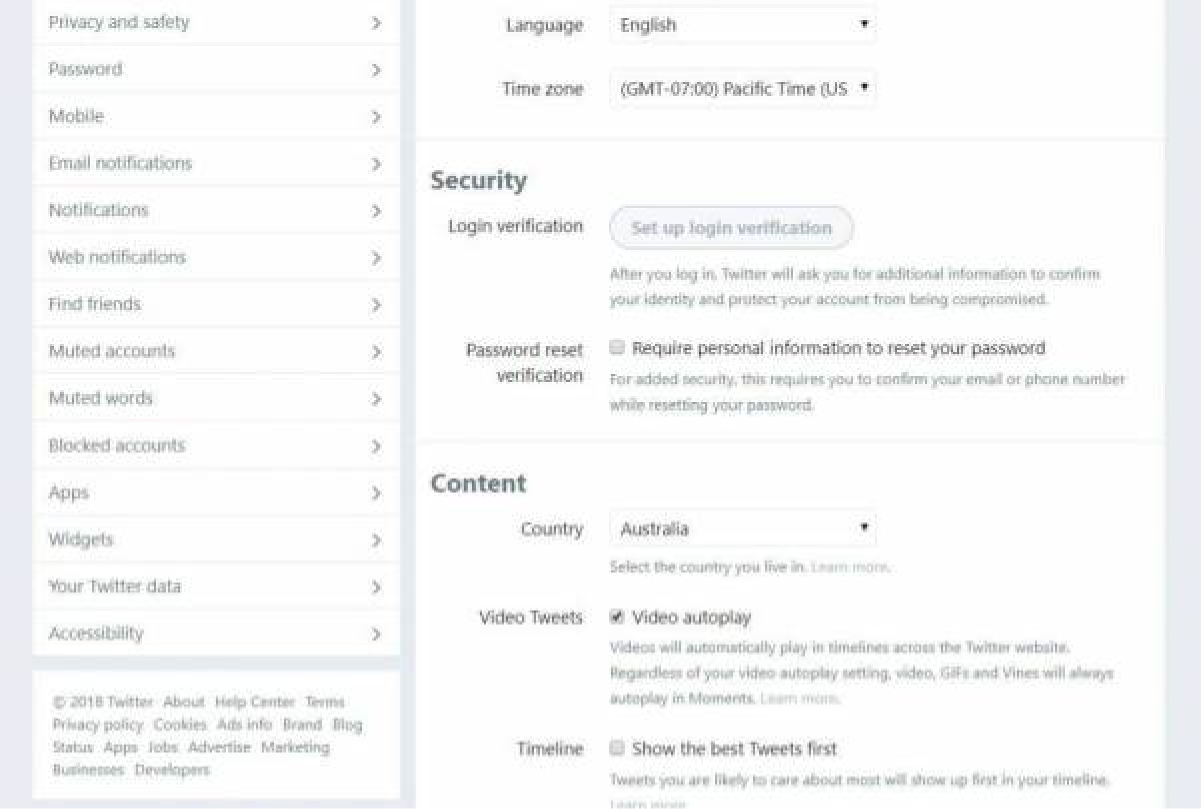
Backup codes are useful if you lose access to your phone number and can't receive a security code by text.

Twitter

Access your Twitter privacy settings from your profile menu.



Once on the Settings and privacy page, you can see your privacy and security options. You can set up two factor authentication and set basic settings. On the left, you'll be able to review more extensive privacy, security and account settings.



Language: English

Time zone: (GMT-07:00) Pacific Time (US

Security

Login verification: After you log in, Twitter will ask you for additional information to confirm your identity and protect your account from being compromised.

Password reset verification: □ Require personal information to reset your password

For added security, this requires you to confirm your email or phone number while resetting your password.

Content

Country: Australia

Select the country you live in. Learn more.

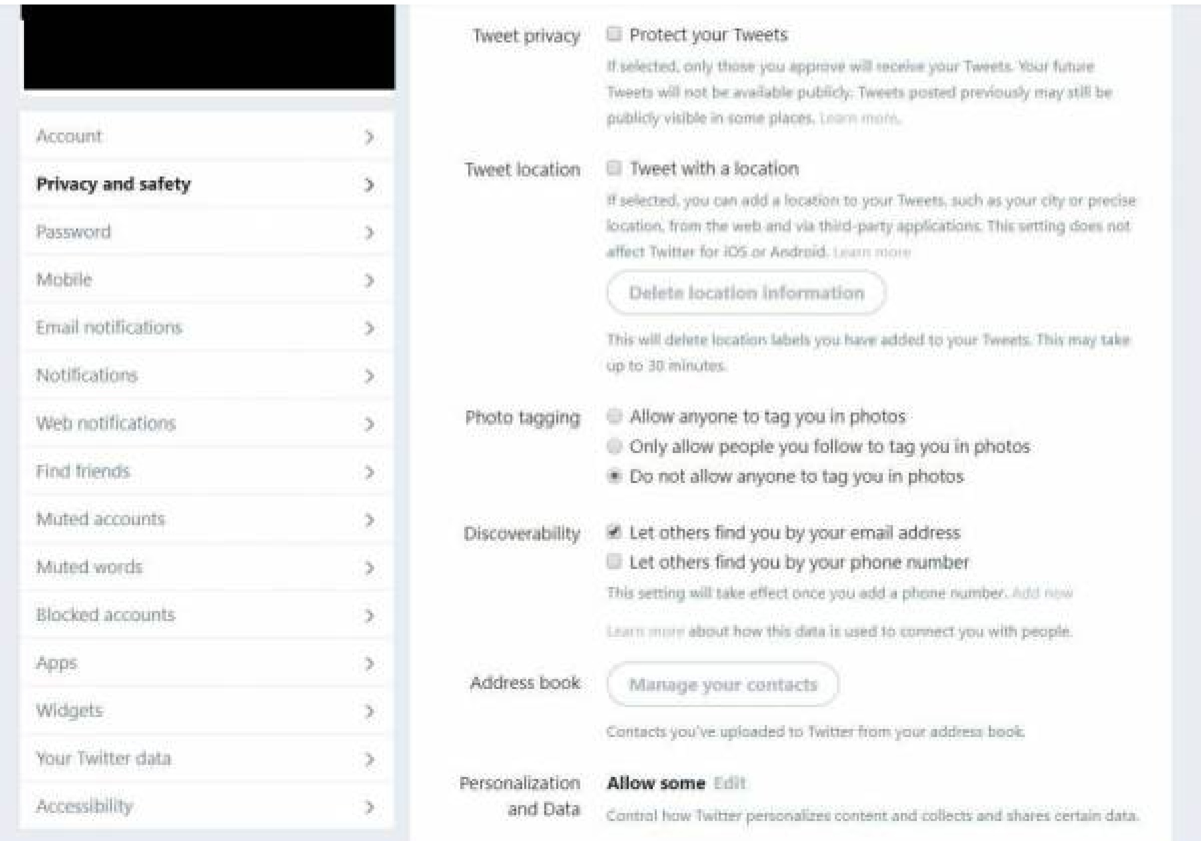
Video Tweets: ☑ Video autoplay

Videos will automatically play in timelines across the Twitter website. Regardless of your video autoplay setting, video, GIFs and Vines will always autoplay in Moments. Learn more.

Timeline: □ Show the best Tweets first

Tweets you are likely to care about most will show up first in your timeline. Learn more

Privacy and Safety gives you a broad overview – you can turn on and off options as you wish. If you want only those who follow you to see your tweets, for example, pick ‘Protect your tweets’. If you don’t want to show your location when you tweet, leave ‘tweet with your location’ unchecked.


[redacted]

Tweet privacy: □ Protect your Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location: □ Tweet with a location

If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. Learn more

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging:
○ Allow anyone to tag you in photos
○ Only allow people you follow to tag you in photos
● Do not allow anyone to tag you in photos

Discoverability:
☑ Let others find you by your email address
□ Let others find you by your phone number

This setting will take effect once you add a phone number. Add now

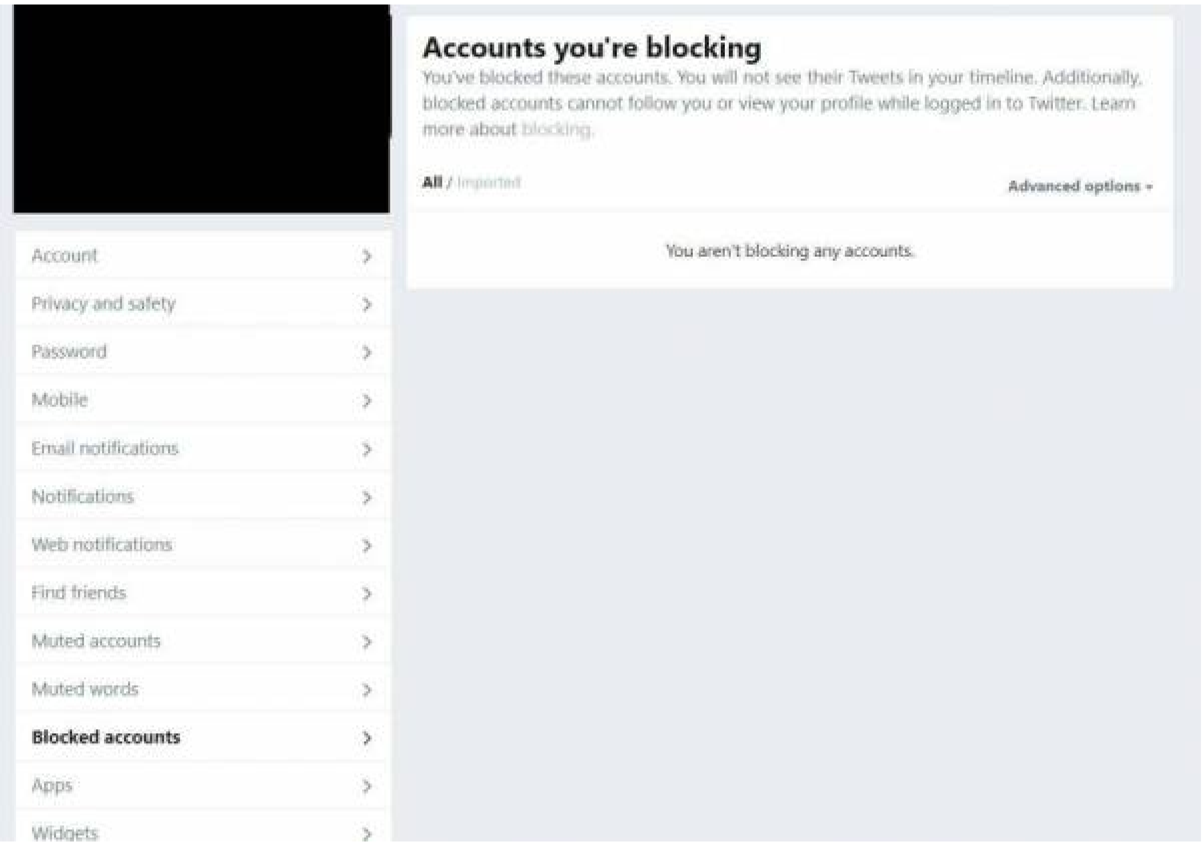
Learn more about how this data is used to connect you with people.

Address book: Contacts you've uploaded to Twitter from your address book.

Personalization and Data: **Allow some** Edit

Control how Twitter personalizes content and collects and shares certain data.

If someone is harassing you or bullying you on Twitter, you may want to block them completely. Add them to your block list if you do.



[redacted]

Accounts you're blocking

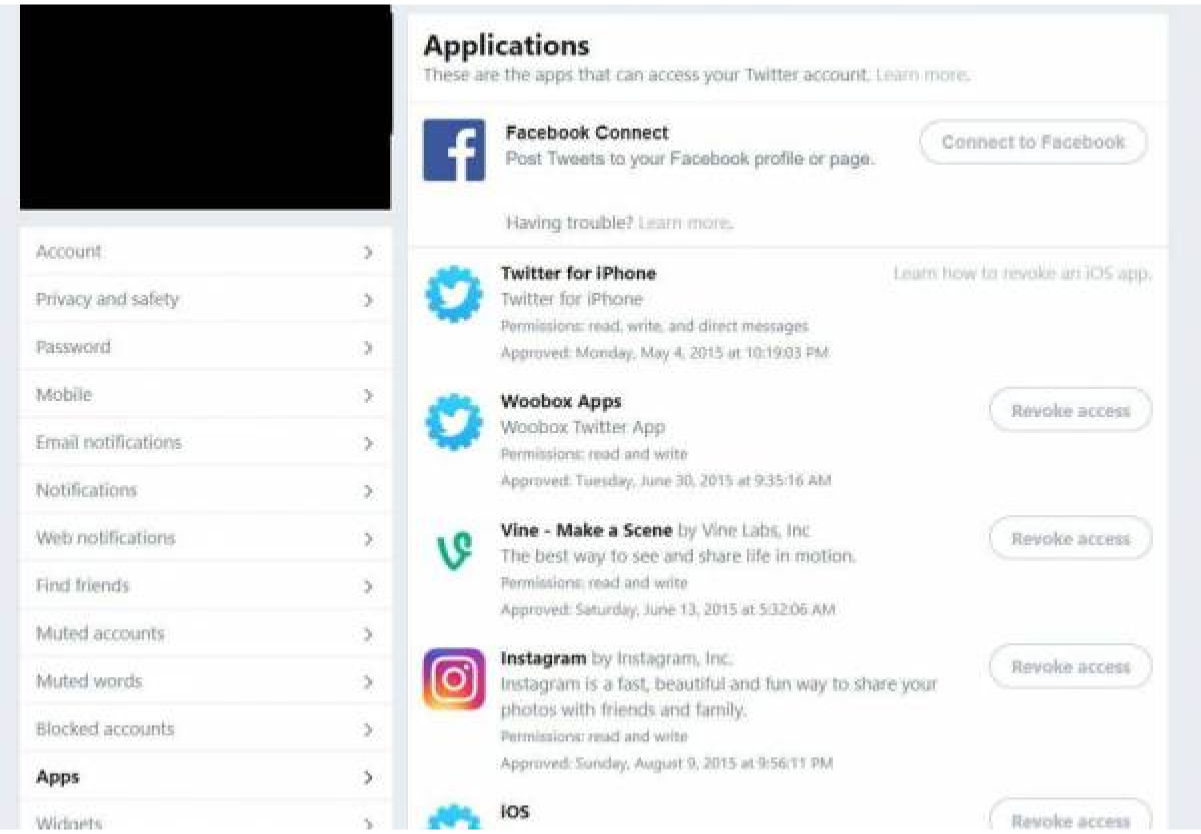
You've blocked these accounts. You will not see their Tweets in your timeline. Additionally, blocked accounts cannot follow you or view your profile while logged in to Twitter. Learn more about blocking.

All / Imported

Advanced options ▾

You aren't blocking any accounts.

You may give access to apps to connect to your Twitter account.Eg, so you can post to Twitter from Instagram. Check these regularly, and take away access if you no longer use the apps.


[redacted]

Applications

These are the apps that can access your Twitter account. Learn more.

Facebook Connect
Post Tweets to your Facebook profile or page.

Having trouble? Learn more.

Twitter for iPhone
Twitter for iPhone
Permissions: read, write, and direct messages
Approved: Monday, May 4, 2015 at 10:19:03 PM

Woobox Apps
Woobox Twitter App
Permissions: read and write
Approved: Tuesday, June 30, 2015 at 9:35:16 AM

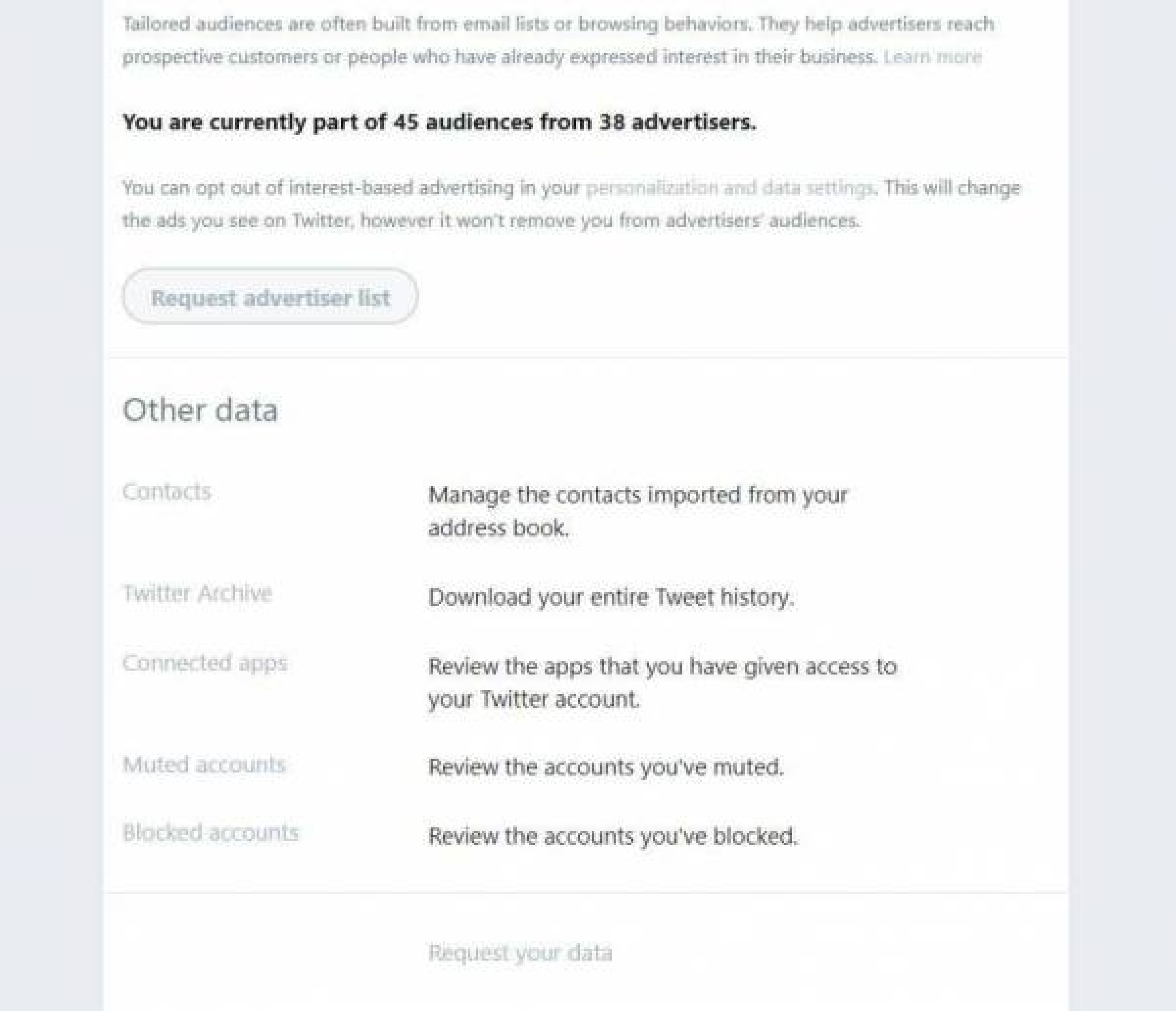
Vine - Make a Scene by Vine Labs, Inc
The best way to see and share life in motion.
Permissions: read and write
Approved: Saturday, June 13, 2015 at 5:32:06 AM

Instagram by Instagram, Inc.
Instagram is a fast, beautiful and fun way to share your photos with friends and family.
Permissions: read and write
Approved: Sunday, August 9, 2015 at 9:56:11 PM

iOS

We'll also look at the ‘Your Twitter Data’ tab. You will have to provide your password again if you want to access this section, as it holds sensitive information pertaining to your accounts.

From here, you can review the information Twitter retains about you. You can also request the list of advertisers who are targeting you and request that all of your Twitter data gets emailed to you in a file.



Tailored audiences are often built from email lists or browsing behaviors. They help advertisers reach prospective customers or people who have already expressed interest in their business. Learn more

You are currently part of 45 audiences from 38 advertisers.

You can opt out of interest-based advertising in your personalization and data settings. This will change the ads you see on Twitter, however it won't remove you from advertisers' audiences.

Other data

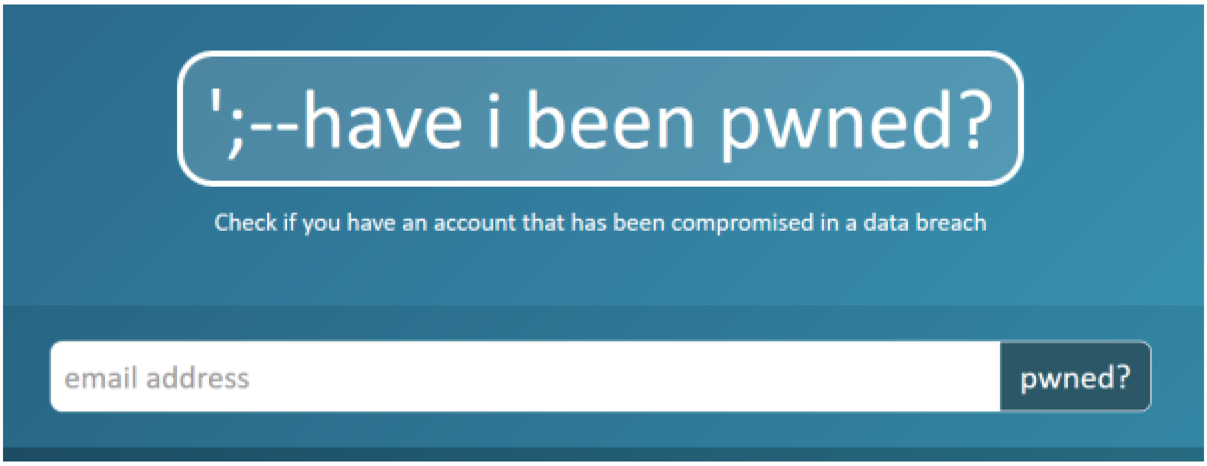
Contacts	Manage the contacts imported from your address book.
Twitter Archive	Download your entire Tweet history.
Connected apps	Review the apps that you have given access to your Twitter account.
Muted accounts	Review the accounts you've muted.
Blocked accounts	Review the accounts you've blocked.

Remember, even with tight privacy settings, you still can’t stop someone seeing a screen over someone’s shoulder, or taking a screenshot to show other people.

Always play it safe, and never post anything you’re not happy with the whole world seeing.

Play The Game

Let's check our email address to see if it has ever been compromised, we'll use the website https://haveibeenpwned.com/



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

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