Workshop 04 - Social Media and Online Safety

SLQ Wiki Fabrication Lab 2024/04/27 02:50

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.

lange .		- 8 - 8
· Home	Windows Update	
Find a satting	Update status Tour device is up to date. Last checked: N/04/2008. SU4 PM	Update at your convenience To salact a convenient time to receive updates, select Ovange
Update & Security	Check for inpdates	action house and specify which bours you use your device. Windows worn't update sharing that time.
 Windows Defender Eackup 	View installed update history	Get help with your undates
 Finaldenhoot Recovery 	Update settings We'll automatically download and initial 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.	Looking for into on the latest updates?
Activation	Change active hours	Related Torks
🗄 Find my device	Keelart option	Check Shorage
For developers	Advanced options	CS hadd infa
Windows Insider Program		Mave a question? Get help
		Make Windows better Give un twedback

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)

Home	Windows Defender	Walter	Defensive Security Center			- 11 X
. Find a satting	P Windows Defender Antivirus protects viruses, spyware, and other maticious Defender Security Center to use it.		Your dev	vice is beir	ng protected	
Update & Security	Open Windows Defender Security (2			21	
C Windows Update	Version info	0	Lett threat years 16/04/201 Last threat definition updat Last health years 16/04/201	e 19/05/2018		
Windows Defender	Antimalware client version 4.14.57	9				
Ŧ Backup	Engine version: 1.1.147 Antivirus definition: 1.2053	3 M K K	~			
P Troubleshoot	Antispyware definition: 1,2053 Network inspection system 1,1147	1		~~	(I)	
Recovery	engine version. Network inspection system 1,2651	.8	Virus & threat	Device performance &	Filewall & network	
 Activation 	definition services	Ĩ.	protection to action rendmi	Health No action releted.	protection No action needled	
A Find my device						
# For developers				R		
 Windows Insider Program 			App & browser control for active rended.	Family options Manage how plue family uses their denses.		

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.

●●○○○ vodafone AU 🗢 12:39 am

.

Control Con



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.

Learn More

Install Now

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.

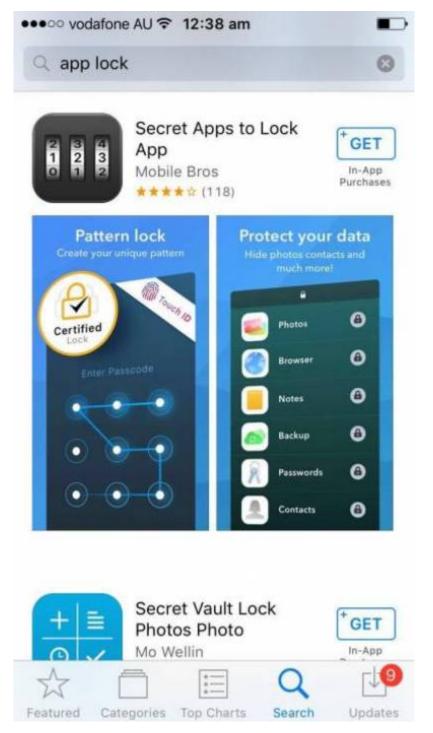


Consider app-lock applications to protect unlocked access to apps with sensitive information.

Line Edge 2024/04/27 02:50

Workshop 04 - Social Media and Online Safety

8/30



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

VOICE DIAI	\cup
Music Voice Control is always	enabled.
ALLOW ACCESS WHEN LOCK	(ED:
Today View	\bigcirc
Notifications View	\bigcirc
Reply with Message	\bigcirc
Home Control	\bigcirc
Wallet	\bigcirc
Erase Data	
Erase all data on this iPhone a passcode attempts.	after 10 failed
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

SLQ Wiki 10/30

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.

	Configuration		
Marken	* Aspens Corms		
Dute Siler	Patameters		
Certgulater	Land	[Agreensthator -]	
+ LAN	1 0 M 17		
* WITHINGS 2.4G (1000)	Userate	athri	
* Wirelese 80 (wrt)	ONI Password	aaaaa (maximum längth is 15)	
* HAN	New Pageword	(marmum length is 15)	
* Bystein	Contem Plansword	(maximum langes is 15)	
* Internet Time		Transfer and the set	
- Firmware Upgrade	Augus Cantet		
- Beckup / Update			
 Ausses Cardrol 			
 Blatt Alert 			
- INK Alert			
- 1962 (Aler)			
· Configure Log			
- Configure Log			
- Configure Log F USO			
- Configure Log F USO F IP Turonel F Security			
Configure Log UBO P Torool Encotty Constity of Service			
 Configure Log URD P Turoni Recoffp Quality of Service NA 1 			
Configure Log UND UND FIF Turbol Possify Gastly of Service HA1 Wake On LAN			
Configure Log UD0 UD0 FIF Tuppel Becartly Gastry of Service HA1 Vision On LAN Vision			
Configure Log UD0 Fill Subset Foronel Constity Constity of Service HAT Yeaks On LAN			

- 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.			
Halter	* Security			
Dank & Shiert	il mute Access Point enabled or Mac filler tol is an	pty with failow chosen. WP52 will be deabled		
Configuration	WPS Betup			
LAN	WPS	Develop - Current	Disabilit	
"Wirewas 2.45 (sell)	Manual Belop AP	Designed and the	e-stand	
- Beek	Send SSD	Upland internats into-		
- Security			0	
- BLAC FITHER	Network Authentication	WPA2 PSK		
Wireless Bridge Advanced	WPA/WAPI paraphrase	********	Class been to depine	
· Station infu	WHITE Group Rokey Interval	3900	[D-21474K3847]	
· Schedule Control	WP4/WWP Encretion	AES	52 CF	
Peteriese BG (witt)				
WAN	Apply Cantat			
* Bystern				
+ US0				
P IP Tunnel				
P Seconty				
Guality of Savvica				
HAT .				
Weike Dri LAN				
w#				
Advanced Setup				
				de Rea
				Q. 100

- 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.

E Settings	Q, Search petilings				0 1
	Advanced				
	Privacy and annually				
	Google Chonse may use web annexes to improve your breaking experience. You may optionally deal services, Lournmole	le these			
	Use a net service to help resolve novigation errors	-0			
	Use a prediction service to help complete searches and URLs typed in the address that	-0			
	Use a prediction service to load pages more quickly				
	Automatically send some system information and page content to Google to help detect dangenous approard sites				
	Protect you and your device from dangerous sites	-0			
	Automatically send usage statistics and crash reports to Google	08			
	Send a 'Do Not Youck' request with your browsing traffic	-0			
	One a web service to help reache apelling errors. Torrarter spelic-besiding by sending what you type in the bosone to Google				
	Manage certificates Internet ITTETTETTE certificates and settings	E			

Senings + C		\$	13 0 @ # 1 =
E Settings	Q. Smarth primup		
	e- Content satings	0	
	Cookies Allow sites to save and read cookie data		
	Location Solid before accenting		
	Carriero Asili befase accessing		
	Microphone Anis befram accounting		
	Recticutions Auto before sensiting		
	cs. JavaScript Advent		
	And Flash		
	E thiges the st		
	E Papages		

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.

Line Edge 2024/04/27 02:50

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.

Line Edge 2024/04/27 02:50

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: 18GIL6SunD@e5
- Facebook Password: FOK186SunD@e5
- Twitter Password: 186SunD@e5TW

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)

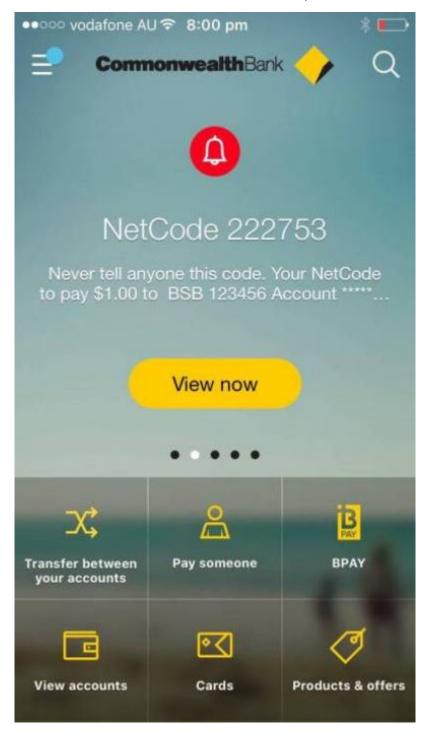
Your accounts and transactions are more secure with 2FA.

Eg. This website sends a token via Push Notification:

			Q Search Million 8	A COLOR	
	Commence allitic	Confirm payment		-	
		Tour NurCaste has been sant to	the Convertilierit sup or your Appie Phone 55.		
		74		the state	
	Transfers 8	\$1.00			
		Pan	74 Fahry		
			123458	and shall be	
		and the second second	westights	adapt to the	
			transactions by RDB and account number or		
		statute, se you may not be attacto record	for account name. Please carefully check these or an incomed payment.	pagamanta .	
		To unitaries prior test prior Natificade de continues	ne migree pluchs generalis and other a		
			Enter your NerColler	and the second s	
		GET NETCODE			
		CHEMIN IS IN	or over Get NetConcey JMX		
		The money will be redeled from pilor as received on Pilotay 20 Apr 2018 (three	spart industry and your payment about the syffeetuurne time;		
		Cancel	Pay	and the second se	
		- NEW DESIGNATION		CORE D	
			Par 10	Card State	
_					

You must enter the code to continue the transaction:

17/30



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. commbank.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?

Line Edge 2024/04/27 02:50

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':

Security and login	Privacy Settings and			
A Privacy	Your activity	Who can see your future postic?	Friends	Edit
Timekse and taggin (many)		Newine all your posts and things you're tagged in		Une Activity Log.
Bicking Language Language Language Language		Limit the eachimer for profession analysis and with the thereign of mends or Public?		Lout Past Pasts
	How people can find and contact you	Whit can send you heard requests?	Everyone	6 da
Konstations Montations Montations Montations Pathic posts Apps and websites IP Ans		Why case your framits kg/? Furthermeter that your framits kg/? Instruction of the two in the second where can you free marking an instrument the second second second second part frameworks, search way frame phone on the two for heavy framework, search way frame phone of the second second framework in the phone of the second second part framework in the phone of the second second part framework in the phone. Other particular second second second	Only me	Eas
Payments Support Inbox Union		Who can look you up using the erral address you provided?	Prienda	Edit
		When each lock year op strong the please member year provided?	Friendla	Edil
		To you want source organis outside of Facilities to test to your Profile?	No	Edit

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

THE HOUSE	Timeline	What care paid, use your tabulitur?	Friends	6
Timeline and tagging		Who can see what others past on your Smellon?	Friends	T
 Biocking Language Face recognition 	Tagging	While care take positis that positive happed in microare benefities?	People to see photos	Ð
Notifications		When you're lagged in a post, who do you want to add to the audionce of the piet of they can't already use IP	People to see photos	E
 Mobile Public pants 	Review	Noview posts that you're lagged is halfest the posts appare on your termine?	04	× 6
Apps and websites		Roview what allow paratie saw on your brankse		View.
Ans Ans Payments Support intex		Noview high that people with is your productions. The laps appear on Facilitation?	On	0
E Voles				

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

This is what your profile tooks like for an Public W	lew ka Specific Person
Tigs: This tool lets you see what your profile looks like to the public or is specific there. Remember: Things that you hole from your transine will appear in Novis Feed, seenth and other places on Facobook.	ed Lace
💷 Don't remend me again	ж
Kat John	
	Acon France Protos Norg-
• ····	C The Adverse of the State State State

Friend lists

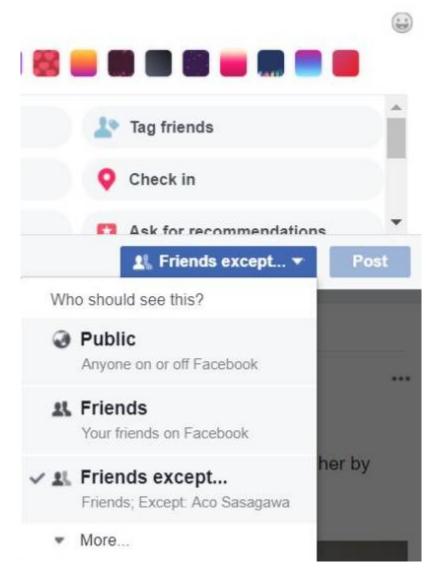
Create lists to easily share with only specific people.

- 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.**



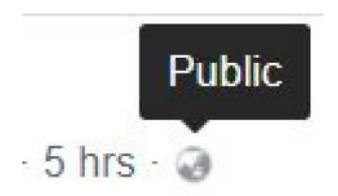


You (and others) can **change the privacy** of a post later.

SLQ Wiki	25/30	Workshop 04	- Social Media and Online Safety		
1	Kat Johnston 3 April at 07:01	•			
Who should see this?		seeds into soil and watered them and now they're			
Pub	Public	low awesome is that?!?			
	Anyone on or off Facebook	Comment	A Share		
~ 1	Your friends on Facebook	III Reid and 23 others			
1	Friends except Friends, Except. Aco Sasagawa				
-	More	Ph_	- A		

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.

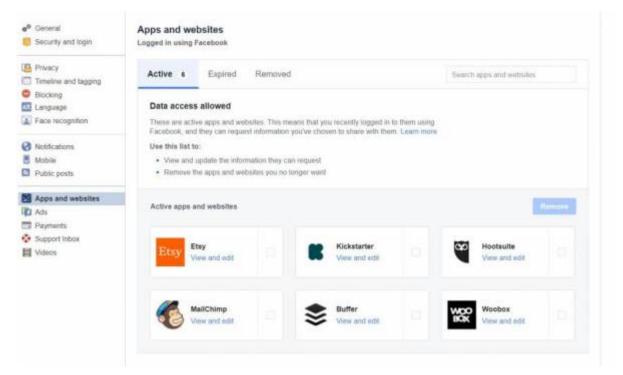
General Security and login	Manage blocking				
Privacy Timetine and tagging	Restricted List	When you add a Nevel to your Restlicted list, they word see posts on Facebook that you Edit List share to Friends only. They may still see things that you share to Public or on a mutual trianula termine, and posts that they're tagged in Facebook doesn't notify your hierds when you add them to your Restlicted list. Learn more			
Blocking Language Face recognition	Block users	Once you black xomeone, that person can no longer see things you post on your limitine, tag you, invite you to events or proups, start a conversation with you, or add you as a trivint. Note: Dees not include apps, gentes or proups you both perticipate in.			
Notifications		Block users	Add name or email	Illock	
Mobile Public posts			You haven't added anyonn to your block test.		
Apps and websites Ads	Block messages If you block messages and video calls from semicone here, they wor't be able to contract Messanger app either. Unless you block someone's profile, they may be able to post on y you and comment on your posts or comments. Learn more				
Payments Support inbox Videos		Block messages from	Type the name of a fillend :		
			ABC News Unblock Facebook Business Unblock		
	Block app invites	Once you've blocked app invites from someone, you'll automatically goons future app requer thend. To block owners from a specific friend, click the "ignore all invites from the triend" link i latest regiment.			
		Block invites from	Type the name of a third.		

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

General Security and login Privacy		ettings u're in a photo or video, our system compares it with yo low when you're in other photos and videos so that we c		
 Timeline and tagging Blocking Language 	Face recognition	Do you want Facebook to be able to recognise you in photos and videos?	No	/ Edit
1 Face recognition				
Notifications Mobile				
Public posts Apps and websites Ads Payments Support Inbox Videos				

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.

27/30



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 I	
O Your Interests	
Advertisers you've interacted with	
Your information	
O Ad settings	Close A
Arts based on your use of websites and anns	A22-

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.

6	age whether or not we can show you ads that are intended to reach people based on these Relationship status	
۳.	The new second	
5	Employer	
1	Job title	
8	Education	
9	These settings only affect how we determine whether or not to show certain ads to you. They don't change which We may still add you to categories related to these fields (see Your categories above).	information is visible on your profile or who can see it.
0	Ad settings	Clean
	ds based on your use of websites and apps	

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

Filters	f Activity log	Activity Search	Q,
Activity log Timeline review Tag review	Timeline review	8 offers. Review 90 I	tems +
12 Photo review		upril 2018	
Posts Posts you're tagged in	YESTERDAY		
 Other people's posts to your timeline Hidden from timeline 	0		1
 Photos and videos Likes and reactions 	0		2
Comments MORE	0		×
Apps			
NORE	0		1
	0		1
	0		2

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.

Privacy	Recommended	
Timeline and tagging Blocking Language	Choose friends to contact if you are locked out Nominitie 3 to 5 triends to help if you are locked out of your account. We recommend this to everyone	Edit
Face recognition	Where you're logged in	
Notifications Mobile Public posts	Windows PC - Brisbane, QLD, Australia Chrome: Active new	
Apps and websites	IPhone 5s - Brisbane, QLD, Australia Mussengar Yesherday at 05.23	1
 Payments Support Inbox 	* See more	
Videos	Login	
	 Change password If is a good data to use a strong paraword that you don't use elsewhere 	Edit
	Log in using your profile picture Tap or cick your profile picture to log in, instead of using it password.	Edit
	Setting up extra security	
	Use two-factor authentication	Edit

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

Workshop 04 - Social Media and Online Safety

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

Workshop 04 - Social Media and Online Safety