



Privacy & Security Settings

A practical guide for u3a members

Facebook - Instagram - Amazon - Google

May 2026

Why These Settings Matter

Privacy

- 1 Who can see your personal information and posts
- 2 How your data is used to target advertising
- 3 What third parties can access about you
- 4 How browsing and purchase habits are tracked

Security

- 1 Preventing unauthorised access to your accounts
- 2 Protecting stored payment card details
- 3 Avoiding account takeover by scammers
- 4 Keeping your identity and personal data safe

General Principles



Defaults favour the platform

When you join a service, most data-sharing is switched on. You must actively switch it off.



Two-step verification is transformative

Even if a criminal obtains your password, they cannot log in without a second code.



Passkeys go further still

Where available, passkeys replace the password entirely and are resistant to phishing.



Review settings periodically

Platforms update policies and can reset options. A check every six months is prudent.

Facebook

Profile visibility, advertising, and account security





Facebook - Finding the Settings

1

Log in to Facebook in a desktop or laptop browser - the full range of settings is only available through a browser, not the mobile app.

2

Click your profile picture or the small downward arrow in the top-right corner of the screen.

3

Select Settings and Privacy, then Settings from the menu that appears.

4

Key sections in the left panel:

- Your Account → Accounts Centre → Password and security, Ad preferences
- Audience and visibility → Profile and tagging [Control who sees posts and tags]
- Your activity → Apps and websites → Third-party app permissions



Facebook - Profile & Privacy Settings

Setting	Recommended Action
Who can see your future posts?	Set to Friends rather than Public
Who can see your friends list?	Set to Friends or Only me - reduces targeting by scammers
Who can look you up by email or phone?	Set both to Friends or Only me
Can search engines link to your profile?	Select No - stops your profile appearing in Google searches
Who can send you friend requests?	Set to Friends of friends rather than Everyone
Tag review	Enable - tags must be approved before appearing on your timeline

Note: Facebook now uses 'Accounts Centre' for security and ad settings. Navigate to Accounts Centre from Settings menu.



Facebook - Advertising & Security

Advertising (Accounts Centre > Ad preferences)

Ads based on data from partners

Set to Not allowed

Ads based on your activity

Set to Not allowed

Social interactions in ads

Set to No one - your name will not appear in friends' ads

Ad topics

Select See fewer for categories you find intrusive

Security (Accounts Centre > Password and security)

Two-factor authentication

Enable - authenticator app preferred over SMS

Passkeys

Set up via Accounts Centre - available on iOS and Android (June 2025)

Login alerts

Enable - notification if someone logs in from an unfamiliar device

Third-party apps

Review and remove apps connected to your account

Instagram

Account privacy, location controls, and advertising





Instagram - Key Privacy Settings



Set Account to Private

Profile > Menu > Settings and Privacy > Account Privacy

Switch Private account ON

Only approved followers can see your posts and stories



Disable Activity Status

Messages and story replies > Show activity status

Switch OFF

Others cannot see when you were last active



Restrict Location Access

Phone Settings > Apps > Instagram > Permissions > Location

Set to Never or Only while using app

Instagram has no need to know your location



Instagram - Advertising & Security

Advertising (Settings > Ads)

Ads based on data from partners

Set to Not allowed

Ads based on your activity

Set to Not allowed

Ad topics

Select See fewer for categories you find intrusive

Security (Accounts Centre)

Two-factor authentication

Now mandatory for all accounts (2025) - via Accounts Centre > Password and Security

Passkeys

Arriving via Meta Account system (2026) - set up via Accounts Centre

Login activity

Review active sessions and log out of unrecognised devices

Hidden Words filter

Enable to reduce unwanted comments and messages

Amazon

Purchase data, Alexa recordings, and account security





Amazon - Privacy & Security Settings



Amazon stores your payment card details - making it one of the higher-risk accounts. Two-step verification should be enabled before anything else.

Setting	Recommended Action
Two-step verification	Account > Login & Security > Enable 2SV - the most important step
Passkeys	Account > Login & Security > Passkeys > Set up. Works on the website and major browsers. Note: a separate passkey is needed for each Amazon marketplace (e.g. .co.uk and .com)
Interest-based advertising	Account > Advertising preferences > Do not personalise ads
Browsing history	Account > Browsing History > turn off recording, or delete items
Saved payment cards	Account > Payment options > remove any cards no longer in use
Third-party app access	Account > Login & Security > revoke access for services no longer used



Amazon - Alexa & Echo Devices

The following applies only to members who own an Amazon Echo, Echo Dot, or other Alexa-enabled device.

Enable automatic deletion of voice recordings

Alexa app > Alexa Privacy > Manage Your Alexa Data > Automatically delete recordings. Set to 3 months or less.

Disable use of recordings to improve services

Alexa app > Alexa Privacy > Manage Your Alexa Data > disable both 'Help improve Amazon services' options.

Review your voice history

Alexa app > Alexa Privacy > Review Voice History. You can listen to and delete individual recordings at any time.

Mute the microphone when not in use

Press the mute button on the device. The ring turns red. The microphone is then physically off and cannot respond to its wake word.

Google

Activity controls, advertising, and account security





Google - Activity Controls

Access at: myaccount.google.com > [Data and Privacy](#) > [Web and App Activity](#)

Setting	Recommended Action
Web and App Activity	Consider pausing - stops Google saving your searches and browsing to your account
Location History	Pause unless you actively use Maps route history - Google otherwise records every location visited
YouTube Watch History	Pause if you prefer YouTube not to track your viewing habits for advertising
YouTube Search History	Pause for the same reason as Watch History
Auto-delete for all history	Set to 3 months so that older data is removed automatically

Advertising (myadcenter.google.com)

My Ad Centre

Visit myadcenter.google.com - review and remove interest categories Google has assigned to you

Personalised ads

May be turned off entirely - you will still see adverts, but not targeted using your personal data

Ads on non-Google sites

Turning off personalised ads applies across Google's advertising network on third-party websites too

Security (myaccount.google.com > Security)

2-Step Verification

Enable under the Security tab - use authenticator app or passkey

Passkeys

myaccount.google.com > Security > Passkeys. When set up, bypasses the second login step entirely

Security Checkup

Complete Google's guided Checkup - it reviews devices, passwords, and app access

Third-party app access

Security > Third-party apps - revoke access for any service no longer used

Passkeys & Authentication

The most secure way to protect your accounts





What is a Passkey?

You set up a passkey on your device

1

The platform stores a public key on its server. A private key is created and stored securely on your device. It never leaves your device.

2

You unlock your device as normal

Use your fingerprint, face recognition, or PIN - whatever you normally use to unlock your phone or computer.

3

That is all that is required

No password to type. No code sent by text message. Your identity is confirmed and you are logged in.

Why passkeys are more secure



Cannot be phished - the passkey only works on the genuine website, not on a fake login page



Cannot be stolen in a data breach - the private key never leaves your device



Cannot be guessed - there is no password to crack or reuse



Easier to use - no password to remember, no code to enter



Authentication Methods Compared



Weak

Password only

A single text string that can be guessed, stolen, or reused across sites.

The baseline. Always use a strong, unique password - but a password alone is not sufficient for important accounts.



Good

Password + SMS code

A code is sent to your mobile number after you enter your password.

A significant improvement. Can be intercepted in rare SIM-swap attacks. Simple to set up and far better than a password alone.



Better

Password + Authenticator app

An app generates a fresh six-digit code every 30 seconds. No SMS involved.

The recommended choice for members who are not yet using passkeys. Not vulnerable to SIM-swap attacks.



Best

Passkey

Device unlock (fingerprint, face, or PIN) confirms identity. No password. No code.

Resistant to phishing and data breaches. Increasingly available on all four platforms. Easiest to use once set up.



Passkeys & 2FA - Platform by Platform

	Facebook 2FA SMS code; authenticator app; physical security key	Passkey Available on iOS and Android (June 2025). Set up via Accounts Centre. Also works on Messenger.
	Instagram 2FA SMS code; authenticator app. 2FA is now mandatory for all accounts.	Passkey Arriving via Meta Account system (announced April 2026). Set up via Accounts Centre.
	Amazon 2FA SMS code; authenticator app	Passkey Available on website (amazon.co.uk) and major browsers. A separate passkey is required for each marketplace domain.
	Google 2FA SMS code; authenticator app; push notification prompt; physical security key	Passkey Fully supported and actively encouraged. Bypasses the second login step entirely. Set up at myaccount.google.com > Security.



Passwords & Two-Step Verification

Password Guidance

Use a different password for every account

At least 12 characters: upper/lower case, numbers, punctuation

Three or four unconnected words work well - e.g.
Harbour42Pencil!

Consider a password manager: Bitwarden (free) or 1Password

Never share passwords by email, text, or telephone

Two-Step Verification (2SV)

SMS text message

Good

A code is sent to your mobile number each time you log in

Authenticator app

Better

App generates a fresh 6-digit code every 30 seconds

Passkey

Best

Unlock your device as normal - no password, no code needed



Summary Checklist

Facebook

- ☒ Posts: Friends only
- ☒ Friends list: Friends/Only me
- ☒ Search engine linking: No
- ☒ Tag review: Enabled
- ☒ 2FA: Enabled
- ☒ Passkey: Consider setting up
- ☒ Remove unused apps

Instagram

- ☐ Account set to Private
- ☐ Activity status: Off
- ☐ Location: Never/While using
- ☐ 2FA: On (now mandatory)
- ☒ Passkey: Arriving 2026
- ☐ Ads from partners: Off
- ☐ Hidden Words: On

Amazon

- ☐ Two-step verification: On
- ☒ Passkey: Set up (website)
- ☐ Interest-based ads: Off
- ☐ Browsing history: Off
- ☐ Remove unused cards
- ☐ Alexa: auto-delete 3m
- ☐ Revoke unused app access

Google

- ☐ Web & App Activity: Paused
- ☐ Location History: Paused
- ☐ YouTube history: Paused
- ☐ Auto-delete: 3 months
- ☐ 2-Step Verification: On
- ☒ Passkey: Set up (recommended)
- ☐ Security Checkup: Done

Key Reminders



Platform settings change - review them every six months.



Two-step verification is the minimum security step for every account.



Passkeys are now available on all four platforms and offer the highest protection.



A full printable guide and checklist is available as a PDF.

Passkey Device Requirements

Part 1: Operating Systems & Browsers

Operating System Requirements

Apple:

- iOS 16+ (Sept 2022)
- macOS Ventura 13.0+ (Oct 2022)

Android:

- Android 9+ (Aug 2018)
- Google Play Services required

Windows:

- Windows 10 v1903+ (May 2019)
- Windows 11 (all versions)

ChromeOS:

- ChromeOS 109+ (Jan 2023)

Browser Compatibility

- Chrome: 109+ (Jan 2023)
- Edge: 109+ (Jan 2023)
- Safari: 16+ (Sept 2022)
- Firefox: 122+ (Jan 2024)
- Brave: 1.48+ (Feb 2023)

Most devices purchased in the last 3-4 years will be compatible

Passkey Device Requirements

Part 2: Essential Requirements & Checking Compatibility

Essential Device Requirements

- ✓ Screen lock must be enabled (fingerprint, face recognition, or PIN)
- ✓ Secure hardware chip: Secure Enclave (Apple), TPM (Windows), or TEE (Android)
- ✓ Device must be signed in to an account (iCloud, Google Account, or Microsoft Account)

How to Check if Your Device Supports Passkeys

iPhone/iPad: Settings → Passwords → Password Options (look for 'Passkeys')

Android: Settings → Passwords & accounts (or Security → Passwords)

Windows: Press Windows key, type 'Windows Hello' (if available, passkeys supported)

Easiest test: Try Google's Security Checkup at myaccount.google.com