

Privacy and Security Settings Guide

Facebook • Instagram • Amazon • Google

Prepared May 2026

This guide has been prepared for members of the University of the Third Age (u3a). It sets out, in plain terms, the key privacy and security settings available on four widely used digital platforms: Facebook, Instagram, Amazon, and Google. The aim is to help members reduce unwanted exposure of personal information, limit targeted advertising, and strengthen account security, without requiring technical expertise.

Platform interfaces change periodically. The pathways described below were accurate as of May 2026, but menu names or locations may have shifted slightly. If a setting cannot be found exactly as described, use the platform's built-in search function within its settings area, or consult the platform's own Help Centre.

Contents

1. General Principles
2. Facebook
3. Instagram
4. Amazon
5. Google
6. Passkeys and Authentication Options
7. Passwords and Two-Step Verification
8. Summary Checklist

1. General Principles

Understanding what these platforms collect

Facebook, Instagram, Amazon, and Google are free or low-cost services whose commercial model depends, to a greater or lesser extent, on collecting data about users and using that data to serve targeted advertising or to personalise recommendations. This is not necessarily harmful, but it means that default settings tend to favour broad data collection rather than privacy. Adjusting settings puts the member back in a more informed position.

Key concepts to bear in mind

Default settings favour the platform. When you first join a service, most data-sharing options are switched on. You must actively switch them off.

Privacy and security are related but distinct. Privacy concerns what others can see about you and how your data is used. Security concerns whether your account can be accessed by unauthorised persons.

Two-step verification (2SV) is the single most effective security measure available to ordinary users. It means that even if someone obtains your password, they cannot log in without a second code.

Passkeys go further still. Where available, passkeys replace the password entirely. You simply unlock your device as normal and are logged in. They are resistant to phishing in a way that passwords and even SMS codes are not.

Review settings periodically. Platforms update their terms and reset certain options after policy changes. A review every six months is prudent.

Less is more. Where a setting's purpose is unclear, the safer course is to restrict rather than permit.

A note on mobile apps versus desktop browsers

The full range of settings is usually available only through a desktop or laptop browser, not through smartphone apps. Where this distinction is important, it is noted in the relevant section. As a general rule, it is worth visiting each platform's settings through a browser at least once to ensure you have seen all available options.

2. Facebook

Accessing settings

Step 1. Log in to Facebook in a desktop browser.

Step 2. Click the small downward arrow (or your profile picture) in the top-right corner.

Step 3. Select Settings & privacy, then click Settings (the gear icon).

Facebook has reorganized its settings under Meta's unified Accounts Centre. Security settings (passwords, two-factor authentication, passkeys) and advertising preferences are now accessed through Accounts Centre. Privacy settings for posts and profile visibility remain in the main Settings panel.

Step 4. The left panel shows key sections: Accounts Centre (for security and ads), Profile and tagging, Apps and websites.

Profile and audience settings

Under Profile and tagging and Followers and public content, you can control who sees your posts, your friends list, and your personal details.

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. A public list can be exploited by scammers.
Who can look you up by email or phone?	Set both options to Friends or Only me.
Do you want search engines to link to your profile?	Select No. This stops your profile appearing in Google or Bing searches.
Who can send you friend requests?	Set to Friends of friends rather than Everyone.
Who can post on your timeline?	Set to Friends or Only me.
Review posts you are tagged in?	Enable Tag review so that tags must be approved before appearing on your timeline.

Advertising preferences

Navigate to Accounts Centre then Ad preferences (or Ad Preferences).

Setting	Recommended Action
Ads based on data from partners	Under Ad settings, set to Not allowed.
Ads based on your activity on Facebook products	Set to Not allowed where presented.
Social interactions in ads	Set to No one so your name does not appear alongside adverts seen by friends.
Ad topics	Review and select See fewer for any category you find intrusive.

Security settings

Navigate to Accounts Centre then Password and security.

Setting	Recommended Action
Two-factor authentication	Enable this. Use an authenticator app if possible, otherwise SMS. See Section 6 for passkey options.
Authorised logins	Review the list of devices that have logged into your account. Remove any you do not recognise.
Login alerts	Enable alerts for unrecognised logins.
Apps and websites	Under Apps and Websites, review and remove third-party apps no longer in use.

3. Instagram

Instagram is owned by Meta (the same company as Facebook). Many privacy principles are similar, but the settings interface differs. As of 2025, Instagram has made two-factor authentication mandatory for all accounts.

Accessing settings

Step 1. Open Instagram and go to your profile (the person icon, bottom right).

Step 2. Tap the three horizontal lines (menu) in the top right corner.

Step 3. Select Settings and Privacy.

Account privacy

Setting	Recommended Action
Private account	Set your account to Private under Account privacy. Only approved followers can then see your posts and stories.
Activity status	Under Messages and story replies, disable Show activity status.
Story sharing	Under Stories, consider disabling Allow sharing to stories.
Location permissions (mobile)	In your phone's own settings, restrict Instagram's access to location to Never or Only while using the app.

Advertising on Instagram

Setting	Recommended Action
Ads based on data from partners	Set to Not allowed.
Ads based on your Instagram activity	Set to Not allowed where presented.
Ad topics	Review and select See fewer for unwanted categories.

Security settings

Setting	Recommended Action
Two-factor authentication	Enable under Accounts Centre then Password and Security. This is now mandatory. See Section 6 for passkey options.
Login activity	Review active sessions and log out of any unrecognised devices.
Blocked accounts	Use the Block function freely for accounts that appear suspicious.
Hidden words	Enable filters under Hidden Words to reduce unwanted contact.

4. Amazon

Amazon's privacy concerns differ from those of social media platforms. The principal issues are: the data Amazon holds about your purchasing behaviour; interest-based advertising; Alexa voice recordings if you own an Echo device; and account security given that payment card details are stored.

Accessing settings

Step 1. Log in to amazon.co.uk in a browser.

Step 2. Hover over Account & Lists in the top menu.

Step 3. Select Account.

Advertising and personalisation

Setting	Recommended Action
Interest-based ads	Go to Advertising preferences. Select Do not personalise ads from Amazon for this internet browser. Note: this must be repeated on each device/browser.
Browsing history	Under Account then Browsing History, turn off history recording or delete items.

Communication preferences

Setting	Recommended Action
Marketing emails	Under Communication preferences, unsubscribe from marketing emails.
SMS messages	Opt out of promotional text messages in the same section.

Alexa and Echo devices

Setting	Recommended Action
Voice recordings	Under Alexa Privacy then Review Voice History, enable Automatically delete recordings. Select a retention period of three months or less.
Help improve Alexa	Under Alexa Privacy then Manage Your Alexa Data, disable options to use your recordings to improve Amazon's services.
Mute microphone when idle	Press the mute button on the device. The ring turns red, confirming the microphone is off.

Account security

Setting	Recommended Action
Two-step verification	Go to Account then Login & security. Enable Two-step verification (2SV). Particularly important as your account is linked to a payment card. See Section 6 for passkey options.
Saved payment cards	Under Payment options, remove any cards no longer in use.
Saved addresses	Under Addresses, remove any out-of-date entries.
Third-party apps	Under Login & security, revoke access for any apps not currently in use.

Important: Because Amazon stores payment card details, it is one of the higher-risk accounts to have compromised. A strong, unique password and two-step verification are strongly recommended. Do not use the same password for Amazon as for any other service.

5. Google

Google is the most pervasive of the four platforms in terms of data collection, because its services extend across Gmail, Google Search, YouTube, Google Maps, Google Photos, Google Drive, and Android phones. Managing a Google account's privacy settings therefore has broad effects.

Accessing settings

Step 1. Go to myaccount.google.com in a browser.

Step 2. The Data and Privacy section is the most important starting point.

Step 3. The Security tab covers authentication options.

Activity controls

Setting	Recommended Action
Web and App Activity	Consider pausing. This stops Google saving your searches and browsing activity to your account.
Location History	Pause unless you actively use Google Maps route history.
YouTube History	Pause Watch History and Search History if you prefer YouTube not to use your viewing habits for advertising.
Auto-delete	Set auto-delete to 3 months if you prefer to keep activity controls on.

Advertising settings

Setting	Recommended Action
My Ad Centre	Visit myadcenter.google.com to see and edit the interest categories Google has assigned to you.
Personalised ads	You may turn off personalised ads entirely. You will still see advertisements, but not ones targeted using your personal data.

Security settings

Setting	Recommended Action
2-Step Verification	Under the Security tab, enable 2-Step Verification. See Section 6 for passkey options, which Google supports particularly well.
Security Checkup	Google's guided Security Checkup reviews recent activity, connected devices, saved passwords, and third-party access. Worth completing once.
Third-party apps	Under Security then Third-party apps and services, revoke access for any service no longer in use.
Signed-in devices	Under Security then Your devices, remove any old, lost, or unrecognised devices.

6. Passkeys and Authentication Options

What is a passkey?

A passkey is a modern method of logging in to an account that replaces the password entirely. When you set up a passkey on a device, the platform stores a public key on its server whilst a corresponding private key is stored securely on your device and never leaves it. When you log in, you simply unlock your device as you normally would (fingerprint, face recognition, or PIN), and that act confirms your identity. No password is typed. No code is sent by text message.

Passkeys are built on an open standard (FIDO2/WebAuthn) developed by the FIDO Alliance, whose members include Apple, Google, and Microsoft. Because the private key never leaves your device and is bound to the specific website for which it was created, passkeys are resistant to phishing in a way that passwords and SMS codes are not. A criminal who tricks you into visiting a fake login page gains nothing, because your passkey simply will not work on any site other than the genuine one.

Authentication options across all four platforms

All four platforms now support passkeys in addition to traditional two-factor authentication. The table below summarises the current position as of May 2026.

Platform	Two-Factor Authentication methods	Passkeys
Facebook	SMS text code; authenticator app; physical security key.	Passkeys introduced June 2025, available via iOS and Android apps. Set up through Accounts Centre in Settings. The same passkey also works on Messenger.
Instagram	SMS text code; authenticator app. 2FA is now mandatory for all accounts (rolled out 2025).	Passkeys arriving as part of Meta's unified Meta Account system, announced April 2026. Set up through Accounts Centre.
Amazon	SMS text code; authenticator app.	Passkeys available on the website (amazon.co.uk) and major browsers. Set up via Account > Login & Security > Passkeys. Note: a separate passkey is required for each Amazon marketplace (e.g. .co.uk and .com).

Google	SMS text code; authenticator app; physical security key; Google push notification prompt (recommended over SMS).	Passkeys fully supported and actively encouraged. When a passkey is set up, it bypasses the second authentication step entirely, since device possession is sufficient verification. Set up at myaccount.google.com > Security.
---------------	--	--

Comparison of authentication methods

Method	How it works	Protection level
SMS text code	A one-time code is sent to your mobile number each time you log in.	Good. Significantly better than a password alone, though SMS can in rare cases be intercepted.
Authenticator app	An app (e.g. Google Authenticator, Microsoft Authenticator) generates a fresh six-digit code every thirty seconds.	Better. Not vulnerable to SMS interception. The recommended choice for most users.
Passkey	You unlock your device as normal (fingerprint, face, or PIN). That act itself logs you in. No code is required.	Best. Resistant to phishing. The private key never leaves your device and is never shared with the platform.
Physical security key	A small USB or NFC hardware device you plug in or tap to confirm identity.	Best (device-bound). Rarely necessary for home users but the most robust option available.

Platform-specific notes

Facebook and Instagram

Because both are owned by Meta, the authentication settings for the two platforms are managed through a shared Accounts Centre. If you set up a passkey for Facebook, it will in due course also work for Messenger, and passkey support for Instagram is following. If you change your two-factor authentication settings for one platform, check whether the change has also affected the other.

Amazon

Amazon's passkey implementation is fully functional on its website through a desktop browser but does not yet extend to all Amazon mobile apps. If you set up a passkey for amazon.co.uk, be aware that you will need a separate passkey for amazon.com or any other Amazon marketplace. Amazon also currently requires a one-time verification code for high-risk payment transactions even when a passkey is in use, which is an additional layer of protection given the financial data held.

Google

Google has gone further than the others in its implementation. When a passkey is set up on a Google Account, it is treated as sufficient verification on its own and bypasses the second authentication step. Google stores passkeys through its Password Manager, which means they are available across all devices signed in to your Google Account. Google's Security Checkup (at myaccount.google.com) will prompt you to set up a passkey if one is not already in place.

Device and Browser Requirements for Passkeys

To use passkeys, your device must meet certain minimum requirements. Most devices purchased within the last three to four years will be compatible, but older hardware may not support the necessary security features.

Operating System Requirements

The following operating system versions are required as a minimum:

Apple devices:

- iPhone and iPad: iOS 16 or later (released September 2022)
- Mac computers: macOS Ventura (13.0) or later (released October 2022)

Android devices:

- Android 9 (Pie) or later (released August 2018)
- Google Play Services must be installed and up to date
- Device must have a screen lock enabled (PIN, pattern, fingerprint, or face unlock)

Windows computers:

- Windows 10 (version 1903 or later, released May 2019)
- Windows 11 (all versions)
- Windows Hello must be set up (fingerprint, face recognition, or PIN)

Chromebooks:

- ChromeOS 109 or later (released January 2023)

Browser Compatibility

Even if your operating system supports passkeys, your web browser must also be compatible. The following browser versions support passkeys:

- Google Chrome: version 109 or later (January 2023)
- Microsoft Edge: version 109 or later (January 2023)
- Safari: version 16 or later (September 2022)
- Firefox: version 122 or later (January 2024)
- Brave: version 1.48 or later (February 2023)

On mobile devices, passkeys work through the operating system itself, so the browser version is less critical—but it is still advisable to keep your browser up to date.

Hardware Requirements

Passkeys rely on secure hardware built into modern devices. Specifically:

Secure storage:

- Apple devices use the Secure Enclave, a dedicated chip that stores cryptographic keys separately from the main processor.
- Android devices use a Trusted Execution Environment (TEE) or dedicated security chip.
- Windows devices use a Trusted Platform Module (TPM), either as a physical chip or firmware-based (fTPM).

These components ensure that the private key used by your passkey never leaves the device and cannot be extracted, even if the device is compromised by malware.

Biometric sensors or PIN:

- Passkeys require you to unlock your device using a fingerprint sensor, facial recognition camera, or a PIN code.
- If your device does not have a fingerprint or face sensor, you can still use passkeys—you will simply unlock using your device PIN instead.
- The device must have a screen lock enabled. If you have disabled your screen lock, you will need to re-enable it before setting up a passkey.

What if my device does not support passkeys?

If your device does not meet the requirements above, you will not be able to use passkeys on that device. However, you have two alternatives:

- 1. Continue using two-factor authentication (2FA) with an authenticator app.** This provides strong security and works on nearly all devices. An authenticator app such as Google Authenticator, Microsoft Authenticator, or Authy is the recommended choice for members not using passkeys.
- 2. Use a physical security key.** These are small USB or NFC devices (such as a YubiKey) that can be used for two-factor authentication. They work independently of your phone or computer's operating system and are particularly useful if you have older devices. Physical security keys are available from around £25 and are supported by all four platforms covered in this guide.

Checking whether your device supports passkeys

The simplest way to check is to attempt to set up a passkey on one of the platforms. Google's Security Checkup at myaccount.google.com is a particularly good starting point, as it will guide you through the process and tell you immediately if your device is not compatible.

Alternatively, on an iPhone or iPad, go to Settings → Passwords → Password Options. If you see an option for Passkeys, your device supports them. On an Android phone, go to Settings →

Passwords & accounts (or Security → Passwords, depending on the manufacturer). If passkeys are supported, you will see a Passkeys section.

On a Windows computer, press the Windows key and type 'Windows Hello'. If Windows Hello is available and can be set up, your device supports passkeys.

Passkey synchronisation across devices

One significant advantage of passkeys is that they can be synchronised across your devices, provided those devices are signed in to the same account:

- Apple: Passkeys are stored in iCloud Keychain and automatically sync across all your Apple devices (iPhone, iPad, Mac) signed in with the same Apple ID.
- Google: Passkeys are stored in Google Password Manager and sync across devices signed in to your Google Account (Android phones, Chromebooks, and any computer where you are signed in to Chrome).
- Windows: Passkeys can be stored in Windows Hello and, as of Windows 11 version 23H2, can sync across Windows devices signed in to the same Microsoft account.

This means that if you set up a passkey on your phone, you will also be able to use it on your laptop—provided both are signed in to the same account. You do not need to set up the passkey separately on each device.

Cross-device passkeys (using your phone to log in on another device)

It is also possible to use a passkey stored on your phone to log in on someone else's computer or a public computer, without the passkey being saved on that computer. When you visit a website and choose to sign in with a passkey, you will see an option such as 'Use a phone, tablet, or security key'. A QR code will appear. You scan the code with your phone's camera, unlock your phone as usual, and the login is completed. The passkey remains on your phone and is not transferred to the other device.

This feature is particularly useful when travelling or when using a shared family computer, as it allows you to log in securely without leaving any credentials behind.

Platform-specific notes on device requirements

Facebook and Instagram:

- Passkeys on Facebook and Instagram currently work through the Meta Accounts Centre and are available on iOS and Android mobile apps.
- As of May 2026, passkey support on desktop browsers for Facebook and Instagram is being rolled out gradually.
- Your iPhone must be running iOS 16 or later, or your Android phone must be running Android 9 or later with up-to-date Google Play Services.

Amazon:

- Amazon passkeys work on the amazon.co.uk website when accessed through a compatible desktop browser (Chrome 109+, Edge 109+, Safari 16+).
- Passkey support in Amazon's mobile apps (iOS and Android) is being introduced gradually and may not yet be available in all regions or app versions as of May 2026.
- Remember that a separate passkey is required for each Amazon marketplace domain (e.g., amazon.co.uk and amazon.com are treated as separate sites).

Google:

- Google has the most mature passkey implementation and actively encourages their use.
- Passkeys work across all Google services (Gmail, YouTube, Google Drive, etc.) and sync automatically via Google Password Manager.
- On Android devices, passkeys are tightly integrated with the operating system and work seamlessly across all apps and browsers.
- Google's Security Checkup will detect whether your device supports passkeys and guide you through setup if it does.

A final note on compatibility

Technology in this area is moving quickly. Device and browser support for passkeys has expanded significantly since 2023 and continues to improve. If your device does not currently support passkeys, it may do so after a software update. It is worth checking for operating system and browser updates periodically, particularly if you are using a device that is three to four years old.

For members who are uncertain or whose devices do not meet the requirements, two-factor authentication using an authenticator app remains an excellent and widely supported alternative. The most important step is to enable some form of second-factor authentication on all four platforms—whether that is an authenticator app, SMS codes, or passkeys.

Should u3a members set up passkeys?

Passkeys are the most secure option currently available for consumer accounts, and are generally easier to use day-to-day than typing a password and then entering a separate code. However, there are a few practical considerations for members to bear in mind:

Your device must support passkeys. A relatively modern smartphone, tablet, or computer is required. Most devices running iOS 16 or later, Android 9 or later, Windows 10 or later, or macOS Ventura or later will support passkeys.

Your device screen lock must be enabled. Passkeys rely on your device's own security (fingerprint, face recognition, or PIN). If your device has no screen lock, you will not be able to use passkeys.

Passkeys are stored on your device. If you lose your device, you will need to log in by another means (your password plus 2FA code). You should therefore always keep your password somewhere safe as a backup.

Two-factor authentication remains an excellent choice. For members who prefer not to use passkeys, or whose devices do not support them, an authenticator app provides very strong protection and is the recommended alternative.

If you are uncertain whether your device supports passkeys, the simplest test is to attempt to set one up on one of the four platforms. The platform will tell you if your device does not meet the requirements. Google's Security Checkup is a particularly convenient starting point, as it will guide you through the process step by step.

7. Passwords and Two-Step Verification

Even as passkeys become more widely available, passwords and two-step verification remain the primary security measures for most users. This section consolidates best practice across all four platforms.

Password guidance

Use a different password for every account. If one platform suffers a data breach, a unique password means your other accounts remain secure.

Passwords should be at least twelve characters long and include a mixture of upper and lower case letters, numbers, and punctuation marks.

A practical approach is to use three or four unconnected words joined together, perhaps with a number and a punctuation mark: for example, Harbour42Pencil!

Consider using a password manager application. Reputable options include Bitwarden (free) and 1Password (subscription). Your browser's built-in password manager (Google, Apple, or Microsoft) is also a reasonable starting point.

Never share passwords by email, text message, or telephone, regardless of who appears to be asking.

Two-step verification explained

Two-step verification adds a second check to the login process. After entering your password, you are asked to confirm your identity by a second means: typically a code sent by text message to your mobile phone, or a code generated by an authenticator app. Even if a criminal obtains your password, they cannot log in without also having access to your phone.

Method	How it works	Security level
SMS text message	A code is sent to your mobile number each time you log in.	Good. Protects against most attacks, though SMS can in rare cases be intercepted.
Authenticator app	An app generates a fresh six-digit code every thirty seconds.	Better. Not vulnerable to SMS interception.
Physical security key	A small USB or NFC device you plug in or tap to confirm identity.	Best. Rarely necessary for general home users.

For most u3a members, SMS text message verification is a significant improvement over password-only protection and is straightforward to set up. An authenticator app provides additional security and is the preferred option where members are comfortable installing one additional application on their smartphone. Passkeys (covered in Section 6) offer the highest level of security and, once set up, are the simplest to use day-to-day.

8. Summary Checklist

The following checklist provides a quick reference. Tick each item once completed. A single session of approximately one to two hours should be sufficient to work through all four platforms.

Facebook

- ☐ Set future posts audience to Friends
- ☐ Set friends list visibility to Friends or Only me
- ☐ Disable search engine linking to your profile
- ☐ Enable tag review
- ☐ Restrict friend requests to Friends of friends
- ☐ Disable ads based on data from partners
- ☐ Set social interactions in ads to No one
- ☐ Enable two-factor authentication
- ☐ Consider setting up a passkey (Accounts Centre > Settings)
- ☐ Review and remove unused third-party apps
- ☐ Check authorised login devices

Instagram

- ☐ Set account to Private
- ☐ Disable activity status
- ☐ Restrict Instagram location access in phone settings
- ☐ Enable two-factor authentication (mandatory from 2025)
- ☐ Consider setting up a passkey (Accounts Centre)
- ☐ Review and remove active sessions
- ☐ Disable ads based on data from partners
- ☐ Use Hidden Words to filter unwanted messages

Amazon

- ☐ Opt out of interest-based advertising
- ☐ Turn off or clear browsing history
- ☐ Unsubscribe from unwanted marketing emails and texts
- ☐ Enable two-step verification
- ☐ Consider setting up a passkey (Account > Login & Security)
- ☐ Remove saved payment cards no longer in use
- ☐ Remove outdated saved addresses
- ☐ Revoke access for unused third-party apps
- ☐ If using Alexa: enable automatic deletion of voice recordings (3 months or less)
- ☐ If using Alexa: disable use of recordings to improve Amazon services

Google

- ☐ Pause or review Web and App Activity
- ☐ Pause Location History
- ☐ Pause YouTube Watch and Search History
- ☐ Set activity auto-delete to 3 months
- ☐ Visit My Ad Centre and remove unwanted interest categories
- ☐ Turn off personalised ads if preferred
- ☐ Enable 2-Step Verification
- ☐ Consider setting up a passkey (myaccount.google.com > Security)
- ☐ Complete the Security Checkup
- ☐ Revoke third-party app access for unused services
- ☐ Review signed-in devices and remove old ones

This guide was prepared for u3a members in May 2026. It represents best practice at the time of writing. Platform interfaces, policies, and authentication options change; members are encouraged to revisit these settings periodically and to consult each platform's own Help Centre for the most current instructions. This document does not constitute professional advice in any technical, legal, or financial capacity.