

Digital Safety & Privacy Guide

A Comprehensive Guide for u3a Members

Staying safe online doesn't have to be overwhelming. This guide focuses on four major platforms—Facebook, Instagram, Amazon, and Google—highlighting the key settings to protect your privacy and secure your accounts using modern tools like 2FA and Passkeys.

The Gold Standard: Passkeys & 2FA

2FA (Two-Factor Authentication): Requires a second step (like a code text to your phone) to log in. It ensures that even if someone steals your password, they can't get in.

Passkeys: A newer, more secure way to sign in without passwords. They use your device's biometrics (fingerprint/face ID) or PIN. They are highly resistant to "phishing" scams.

1. Facebook: Protecting Your Social Life

Facebook is great for staying in touch, but it defaults to sharing a lot of data.

- **Privacy Checkup:** Go to *Settings & Privacy > Privacy Checkup*. This guided tour helps you limit who sees your posts and friends list.
- **Limit Past Posts:** In *Privacy Settings*, select "Limit Who Can See Past Posts" to hide old content from the public instantly.
- **Off-Facebook Activity:** Facebook tracks you on other websites. Go to *Settings > Your Facebook Information > Off-Facebook Activity* to disconnect this tracking.
- **Security:** Enable 2FA in *Security and Login*. Avoid using "Login with Facebook" on unknown websites to keep your accounts separate.

2. Instagram: Visual Privacy

- **Private Account:** If you only want friends and family to see your photos, go to *Settings > Privacy > Account Privacy* and toggle on **Private Account**.
- **Sensitive Content Control:** Reduce the amount of upsetting or "clickbait" content in your feed via *Settings > Suggested Content*.

- **Two-Factor Authentication:** Found under *Settings > Security*. Use an authenticator app (like Google Authenticator) for better security than SMS.

3. Amazon: Secure Shopping

Amazon holds your payment information, making it a primary target for hackers.

- **Login & Security:** This menu allows you to enable **2FA**. Amazon now supports **Passkeys**, which is the safest way to log in on your phone or tablet.
- **Public Profile:** Did you know you have an Amazon public profile? Go to *Your Account > Profile* to see what others see (like your wish lists or reviews) and hide items you want kept private.
- **Alexa Privacy:** If you use an Echo device, go to *Settings > Alexa Privacy* to review and delete voice recordings.

4. Google: The Gateway to Your Data

Since Google handles your email, searches, and often your smartphone (Android), its security is critical.

- **Google Privacy Checkup:** Visit myaccount.google.com. Turn off "Web & App Activity" or set it to "Auto-delete" after 3 months.
- **Location History:** Check your "Timeline" and turn off location tracking if you don't want Google keeping a map of everywhere you go.
- **Passkeys:** Google is a leader in Passkeys. In *Security* settings, set up a Passkey for your primary device. This makes it almost impossible for someone to "hack" your account from a different computer.

General Advice for u3a Members:

- **Beware of Urgency:** If an email or message says you must "act now" or your account will be deleted, it is almost certainly a scam.
- **Don't Overshare:** Avoid posting your full birthdate, home address, or when you are going away on holiday.
- **Use a Password Manager:** Tools like Bitwarden or 1Password can remember complex passwords so you don't have to.