

SMART START

Nora Knowhow

Facebook Safety Guide

A practical, step-by-step guide to making Facebook safer, spotting trouble and knowing what to do when something does not look right.

For Melton Mowbray u3a members



Small changes. Stronger security. More confidence.

Before you start Facebook changes its menus from time to time. The wording may vary slightly between the Facebook app, iPhone, Android, tablet and computer. Look for the same setting names shown in this guide.

Nora has changed into her coral cardigan for this edition. Facebook may change its buttons, but the safety principles stay comfortably put.

1. Give your Facebook account a safety check

Facebook's Privacy Checkup brings several important controls together. Start here before changing individual settings.

1

Open Facebook

Sign in to Facebook on your phone, tablet or computer. Make sure you are using your own account.

2

Open Settings & privacy

Select your profile picture or Menu, then choose Settings & privacy.

3

Choose Privacy Checkup

Select Privacy Checkup. Work through the sections Facebook presents to you.

4

Check who can see what you share

Review your profile information and the default audience for future posts. For personal posts, consider Friends rather than Public.

5

Check how people can find you

Review friend requests and how people can look you up. Share only as much information as you are comfortable making discoverable.

Nora's rule of thumb If you would not put the information on a noticeboard in the town centre, think carefully before making it Public.

2. Lock the front door: password and two-factor authentication

A good password protects the door. Two-factor authentication adds a second lock.

1

Use a strong, unique password

Do not reuse the password from your email, banking or other important accounts. A password manager can help you keep unique passwords.

2

Open Accounts Centre

From Settings, open Accounts Centre. Select Password and security. Menu wording can vary by device.

3

Turn on two-factor authentication

Choose Two-factor authentication, select your Facebook account and follow the on-screen instructions. Facebook may offer an authentication app, text message or another available method.

4

Check where you're logged in

In Password and security, review Where you're logged in. Look for phones, tablets, browsers or locations you do not recognise.

5

Log out of anything suspicious

If you see an unfamiliar session, follow Facebook's options to log it out and secure your account. Change your password if you think somebody else may know it.

Important Protect your email account with two-step verification too. Your email is often the route used to reset other account passwords.

3. Friends, followers and unwanted contact

1

Treat unexpected friend requests with caution

A familiar photograph does not prove the account belongs to that person. Cloned accounts can copy names and pictures.

2

Check before accepting

Look at the profile history, mutual friends and recent activity. If the request seems unusual, contact the person another way.

3

Unfriend when needed

Open the person's profile, select the Friends control and choose Unfriend. Facebook does not normally notify someone that you have unfriended them.

4

Block unwanted contact

Open the person's profile or your blocking settings and choose Block. Follow Facebook's confirmation screen.

5

Report suspicious content or accounts

Use the three-dot menu (...) on the post, message or profile and choose the reporting option shown. Follow the questions Facebook asks.

Watch for impersonation A message from a 'friend' asking urgently for money, gift cards, a code or personal details deserves a second check. Contact them using a phone number or method you already trust.

4. Spotting Facebook scams

Scammers thrive on speed, emotion and curiosity. Their favourite button is the one they hope you press before thinking.

- **Urgency:** 'Act now', 'your account will be closed', 'last chance' or 'send this immediately' are prompts to slow down.
- **Unexpected prizes:** Be suspicious of competitions or giveaways you do not remember entering, especially when asked for card details or a fee.
- **Requests for codes:** Never send somebody a login, security or verification code because they ask for it in Messenger.
- **Suspicious links:** Do not open a link simply because it appears to have come from a friend. Their account may have been compromised.
- **Marketplace caution:** Be wary of pressure to move conversations or payment away from the platform, unusual payment requests, or deals that feel implausibly cheap.
- **Fake support:** Do not trust an unsolicited message claiming to be Facebook support merely because it uses a Facebook or Meta logo.

STOP • CHECK • CONFIRM Stop before clicking or paying. Check the account and message. Confirm through a separate trusted route.

5. Help! I think my Facebook account has been hacked

Act promptly, but work methodically. Start with a device you trust.

1

Change your Facebook password

If you can still sign in, change the password immediately and make it unique.

2

Review logged-in devices

Open Password and security and review Where you're logged in. Remove sessions you do not recognise.

3

Check your email account

Secure the email account linked to Facebook. Change its password if necessary and turn on two-step verification.

4

Look for changes

Check whether your email address, phone number, profile information or security settings have been altered.

5

Warn your contacts

Tell friends not to trust unusual messages, links or requests that appear to have come from your account.

6

Use Facebook's recovery help

If you cannot access the account, use Facebook's official hacked-account and account-recovery routes. Avoid 'recovery experts' who contact you offering paid help.

Final safety check • If money is involved Contact your bank or card provider promptly using a trusted number. In the UK, report fraud through the appropriate official reporting service.

Nora's 60-second Facebook checklist

- ☐ My Facebook password is unique.
- ☐ Two-factor authentication is switched on.
- ☐ I have checked where I am logged in.
- ☐ My normal posts are not Public unless I intend them to be.
- ☐ I question unexpected friend requests and urgent messages.
- ☐ I know how to block and report an account.

Digital Friends • Simple help for a safer digital life

Reference points: Facebook Help Centre and the UK National Cyber Security Centre. Settings and menu names may change as Facebook is updated.
Guide prepared September 2026.