

Passkey Setup and Safety Checklist

Create a safer sign-in method without losing your recovery route

1. Before Setup

- ☐ Trusted personal or assigned device
- ☐ Supported and updated operating system
- ☐ Device screen lock enabled
- ☐ Recovery email checked
- ☐ Recovery telephone checked
- ☐ Another secure access method retained



Scan for the full guide
itclub.work/knowledge-centre

2. Choose the Correct Account

- | | |
|---|---|
| ☐ Personal Microsoft | ☐ Microsoft work or school |
| ☐ Personal Google | ☐ Google Workspace |

Personal and organisational accounts use different management pages — follow the correct route.

3. Create and Test

- ☐ Use the official account-security page
- ☐ Select the correct passkey option
- ☐ Confirm where the passkey is stored
- ☐ Approve creation locally (PIN, fingerprint or face)
- ☐ Sign out
- ☐ Test passkey sign-in

4. Recovery

- ☐ Alternative recovery method available
- ☐ Lost-device process understood
- ☐ Remote lock or erase configured
- ☐ IT reporting route known for business devices

5. Review

- ☐ Every passkey recognised
- ☐ Old devices removed
- ☐ Shared-device credentials removed
- ☐ Account activity checked
- ☐ Business policy followed

Trust the device. Test the sign-in. Protect the recovery route.

IT Club

Technology Intelligence — Plain-English guidance for business owners

<https://itclub.work/knowledge-centre>