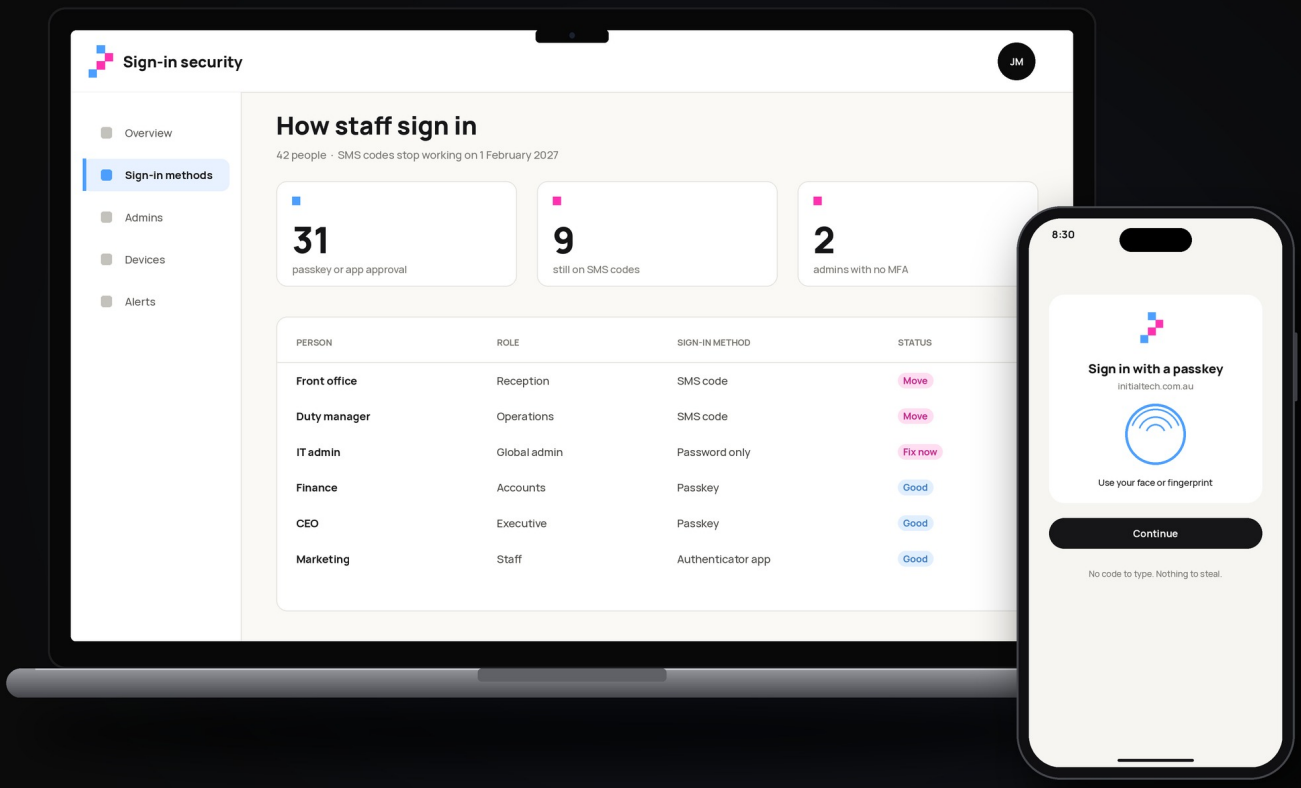


MICROSOFT 365 · AS OF NOVEMBER 2026

Microsoft 365 security. Simplified.

The settings that stop most break-ins, including passwords, passkeys and multi-factor sign-in. Written for clubs and small businesses.

John Morgan · Initial Technology · November 2026

THE ONE THING TO KNOW

Most break-ins start with a stolen sign-in.

Someone gets a password, signs in as a staff member, and quietly reads email or changes bank details. Strong sign-in, a few locked-down settings and someone checking the alerts stop most of it.

SIMPLIFIED

Passkeys for everyone. Fewer, separate admin accounts. Tight sharing. Someone reads the alerts.

SIX STEPS AT A GLANCE

01
Strong sign-in
Passkeys or app approval for everyone.

02
Protect the admins
Few, separate, extra-strong.

03
Switch on the basics
Security defaults or policies.

04
Lock down email
Stop forwarding and fake senders.

05
Tame sharing
Specific people, links that expire.

06
Watch and review
Alerts read, access checked.

DATES THAT MATTER

1 Sep 2026
Passkeys became the default sign-in in Microsoft Entra

1 Feb 2027
Microsoft stops sending SMS and voice sign-in codes

4+ words
ASD's advice for a strong passphrase, 14+ characters

STEP 01

Strong sign-in for everyone

A password alone isn't enough any more.

- [ ] **Turn on multi-factor for everyone.**
  No exceptions for the CEO, the board or shared mailboxes.
- [ ] **Get off SMS codes.**
  Microsoft stops sending them on 1 February 2027.
- [ ] **Never approve a prompt you didn't start.**
  Unexpected sign-in requests mean someone has the password.
- [ ] **Move to passkeys.**
  A face or fingerprint on a phone or laptop. Nothing to type, nothing to steal.
- [ ] **Use passphrases.**
  Four or more random words. A password manager for the rest.
- [ ] **Stop forced password changes.**
  Long and unique beats changed every 90 days.

HANDY TIP

Start with the people who handle money and member data. They're the ones criminals target first.

WRITE IT DOWN

PEOPLE STILL ON SMS CODES _____

PASSKEYS DONE BY (DATE) _____

WHO'S CHECKING _____

STEP 02

Protect the admin accounts

One stolen admin account can undo everything else.

- [ ] **Keep global admins to a handful.**
  Two to four is plenty for a club.
- [ ] **Separate admin accounts.**
  Not the same account people use for email and browsing.
- [ ] **Two emergency accounts.**
  Stored safely, excluded from lock-outs, checked every quarter.
- [ ] **Know who your IT provider is signed in as.**
  Their access should be named, strong and reviewed.

HANDY TIP

Ask your IT provider for a list of every admin account in your tenant. If they can't produce it in a day, that's your answer.

WRITE IT DOWN

ADMIN ACCOUNT	WHO	LAST CHECKED

STEP 03

Switch on the protective basics

Most of this is free, or already in Business Premium.

- [ ] **Security defaults or Conditional Access.**
  Defaults are free. Business Premium lets you set rules by user and device.
- [ ] **Block old sign-in methods.**
  Old email apps can skip multi-factor. Turn them off.
- [ ] **Manage devices with Intune.**
  Updates, encryption and a remote wipe for lost laptops and phones.
- [ ] **Keep the audit log on.**
  You can't investigate what wasn't recorded.

HANDY TIP

If you're on Business Standard and have more than a few staff, Business Premium usually pays for itself in security features.

STEP 04

Lock down email

Email is where most club scams land.

- [ ] **Block automatic forwarding outside.**
  A classic sign of a hijacked mailbox.
- [ ] **Set up your domain's sender records.**
  SPF, DKIM and DMARC stop others pretending to be you.
- [ ] **Turn on safe links and attachments.**
  Checks links at the moment someone clicks.
- [ ] **Tag outside emails.**
  A simple banner helps staff pause.

HANDY TIP

Have your provider check your DMARC record today. It takes minutes and stops criminals sending email as your club.

WRITE IT DOWN

SPF, DKIM and DMARC set up?	☐ Yes	☐ No
External forwarding blocked?	☐ Yes	☐ No

STEP 05

Tame sharing

Old sharing links are how private files end up in the wrong hands, and in AI answers.

- [ ] **Default to “specific people”.**
  Not “anyone with the link”.
- [ ] **Review guest access.**
  Remove guests who no longer need it.
- [ ] **Make links expire.**
  30 to 90 days for anything shared outside.
- [ ] **Lock down sensitive sites.**
  HR, payroll, board, members, gaming and AML.

HANDY TIP

Getting ready for Copilot or any AI tool? This step matters twice. See our Copilot readiness guide (no. 07).

STEP 06

Watch and review

Settings drift. Someone has to look.

- [ ] **Someone reads the alerts.**
  Impossible travel, mass downloads, new forwarding rules.
- [ ] **Review access every quarter.**
  Leavers, guests, admins and shared mailboxes.
- [ ] **Check Secure Score monthly.**
  Microsoft's own to-do list for your tenant.
- [ ] **Test a leaver.**
  Disable an account the day someone leaves. Every time.

HANDY TIP

Essential Eight is still Australia's baseline. ASD is moving to a new 'Essentials' series over the next two years, but nothing here goes out of date.

WRITE IT DOWN

Q1 REVIEW	Q2 REVIEW	Q3 REVIEW	Q4 REVIEW

Want to know where you stand?

A Microsoft 365 security check shows, in plain English, what's set up well, what isn't, and what to fix first. Independent, fixed price.

0401 539 456 · info@initialtech.com.au · initialtech.com.au

THE SIMPLIFIED GUIDES

Free at initialtech.com.au/resources

01 Microsoft 365 security

02 Cyber basics and phishing

03 Ransomware readiness

04 Backup and recovery plan

05 Incident response

06 Working from home securely

07 Copilot readiness

08 Choosing an IT provider

09 Buying a major system

10 The board technology report

11 Copilot vs ChatGPT vs Claude

Sources, checked November 2026. Microsoft: passkeys by default and retirement of Microsoft-provided SMS and voice MFA (Entra notice, July 2026); security defaults; Conditional Access. ASD's ACSC: Creating strong passphrases; Small business cyber security guide; Essential Eight maturity model (November 2023) and the Essentials transition (June 2026). General information only, not legal, insurance or financial advice. Check current details with your IT provider before acting.