

Free settings first

Everything here works on Basic, Standard and Premium.
Do it in this order, so nobody is caught out on the day.

Check security defaults

Entra ID, then Overview, then Properties.

Manage security defaults.

If they are already on, skip to the admin accounts.

Find what signs in the old way

The scanner that emails scans.

Very old Office programs.

Anything that signs in with a code, such as a smart screen.

Tell staff, then switch on

Staff set up the Authenticator app at myprofile.microsoft.com.

Switch security defaults on.

Sign everyone out once so they all register.

Admin accounts

Do admin work on its own account, never the one you read email on.
Keep two emergency accounts that nobody uses day to day.

Outside apps

Stop staff approving apps that ask to read their mailbox.
Turn on the admin consent workflow for real requests.
Look through the apps already approved.

The one rule for staff

A code you did not ask for never goes into microsoft.com/devicelogin.
It goes to whoever looks after your Microsoft 365.

Only then, Premium

Your own sign-in rules, and link and attachment checks.
Write the rules before you switch security defaults off.
Add the rule that blocks sign-in codes yourself.