

SHARE THIS AROUND

Multi-factor authentication

The extra step when you sign in — a prompt on your phone, an app, or a code. It is mildly inconvenient, and it is the single most effective thing protecting your accounts.

Passwords leak. They get guessed, reused, phished, or exposed when some unrelated website is breached. Multi-factor authentication means a password alone is no longer enough to get in — so when yours does get out, and one day it probably will, nothing happens.

THE ONE RULE THAT MATTERS MOST

If you did not start the sign-in, deny it.

An approval request you were not expecting means somebody already has your password and is trying to use it. Deny it, then tell someone — your password needs changing today.

SIX THINGS TO REMEMBER

01 Never approve a prompt to make it stop

Repeated prompts mean somebody is trying repeatedly. They only need you to tap Approve once out of irritation. Deny every one, then report it.

02 Never read a code out to anyone

No bank, supplier, colleague or IT provider will ever ask for one — not by phone, email or message. Anyone who asks is attacking you.

03 Use an app rather than text messages

An authenticator app is quicker and considerably harder to intercept than SMS. If you are still on text codes, ask to be moved.

04 It is not only for work

Turn it on for personal email, banking and social media too. Personal email is often the route used to reset everything else.

05 Tell someone before you change phone

Your authenticator needs moving across. Sorting it beforehand takes minutes; afterwards it can lock you out entirely.

06 Report it even if you denied it

A denied prompt is still evidence that your password is out there. Denying it protects the account; reporting it fixes the cause.

Which method, and why it matters

All of these are far better than a password alone. Some are noticeably stronger than others, so if you have a choice, choose from the top.

MethodStrengthWorth knowing Passkey or security key**Strongest**Cannot be intercepted or phished the way codes can. Quickest to use once set up. Authenticator app**Strong**The sensible default for most people. Approve a prompt, or read a rotating code. App with number matching**Strong**You type a number shown on screen, so you cannot approve absent-mindedly. Prefer this if offered. Text message code**Adequate**Better than nothing, and the weakest of these. Codes can be intercepted or redirected. Email code**Weakest**If your email is compromised, so is this. Avoid where any alternative exists.

Common worries, answered

“It will slow me down all day”

It will not. On your own device you are usually prompted occasionally rather than every time.

“I don’t want work on my phone”

An authenticator app holds no company data and cannot be used to read your files. A physical key is an alternative.

“What if I lose my phone?”

Say so straight away and access can be restored. Do not let this stop you enrolling.

If you approved something by mistake

1. Tell whoever handles your IT immediately – minutes genuinely matter here.
2. Change your password, from a different device if you can.
3. Deny any further prompts, however many arrive.
4. Nobody is in trouble for reporting quickly. The harm comes from the hours nobody knew.

FILL THIS IN BEFORE SHARING

THE APP WE USE IS

REPORT UNEXPECTED PROMPTS TO