EMAIL SCAM CHECK

Microsoft Account Recovery Email — Scam Check

Print this. Stick it on the fridge. Or save it to your phone.

Quick Risk Checklist — Tick Any That Apply

- [ ] The sender's domain isn't exactly @microsoft.com (look for typos: microsft, micr0soft, microsoft-support.com).
- [ ] The "Secure Account" or "Review Activity" button hovers to a non-microsoft.com URL.
- [ ] The email mentions a foreign sign-in attempt (Russia, China, Brazil) to spike urgency.
- [ ] It says your account will be suspended in under an hour if you don't click.
- [ ] It includes a screenshot or table of fake login details to look legitimate.
- [ ] You don't use the email address it was sent to for any Microsoft service.

What To Do Right Now

- [ ] Don't click the link in the email. Even a single click can fingerprint your device.
- [ ] Open a new browser tab and type account.microsoft.com directly. Sign in.
- [ ] Check Recent Activity at account.microsoft.com/security/signinactivity. Real sign-ins (yours or attempted) show up there.
- [ ] Forward the email to Microsoft at phish@office365.microsoft.com, then delete it.

How To Verify Safely

- [ ] Hover over the button (don't click). The URL should start with https://account.microsoft.com, https://login.microsoftonline.com, or https://security.microsoft.com. Anything else is fake.
- [ ] Check the full sender address, not just the display name. Real Microsoft emails come from @microsoft.com, @accountprotection.microsoft.com, or @email.microsoft.com.
- [ ] Log into account.microsoft.com directly and check your sign-in activity yourself. Real attempts will be logged there.
- [ ] Turn on Microsoft Authenticator for sign-in approval, so attempted sign-ins prompt your phone — much harder to phish.

Where To Report It

- [ ] Microsoft Phishing Team — Forward To phish@office365.microsoft.com
- [ ] Your Email Provider — Mark As Phishing (Gmail, Outlook, Yahoo, iCloud)
- [ ] FTC Consumer Fraud — reportfraud.ftc.gov ■
- [ ] Anti-Phishing Working Group — reportphishing.apwg.org ■

If You Already…

- [ ] Clicked The Link — see /recovery/clicked-a-link/
- [ ] Logged In On A Fake Page — see /recovery/shared-a-password/
- [ ] Entered Payment Info — see /recovery/shared-bank-info/
- [ ] Shared A Code — see /recovery/shared-a-code/
- [ ] Installed Software — see /recovery/installed-remote-access/
- [ ] Sent Money — see /recovery/sent-money/