

Suspicious Account: First Steps

Use this if you see an unexpected sign-in, MFA prompt, or unfamiliar account activity. For a work account, contact your IT or security team first and follow their instructions.

Act safely

- ☐ **Do not approve an unexpected MFA request.**
Do not share a one-time code with a caller or enter it at a link sent to you.
- ☐ **Open the service from your own bookmark or app.**
Avoid links and phone numbers in the suspicious message.
- ☐ **For a personal account, change the password from a trusted device.**
If you cannot sign in, use the service's official account recovery flow.
- ☐ **Review active sessions, devices, recovery details, and connected apps.**
Sign out unfamiliar sessions and remove access you did not authorize.

Record and report

- ☐ **Save the time, screenshots, message, and sign-in details.**
For a work account, preserve the evidence requested by your response team.
- ☐ **Check for changes to mail forwarding or payment details.**
Contact affected financial services through independently verified channels.
- ☐ **Tell the right person promptly.**
For work, use your incident reporting path. For identity theft, use the FTC recovery plan.
- ☐ **Watch for follow-on impersonation.**
People may use real details from the incident to sound convincing.

Sources and further guidance

[CISA Secure Our World](https://www.cisa.gov/secure-our-world) | <https://www.cisa.gov/secure-our-world>

[FTC IdentityTheft.gov](https://www.identitytheft.gov/) | <https://www.identitytheft.gov/>