ccount Hijacking: What it is, signs to spot, and how to stop it

Gridinsoft Help Center

What it is (in plain words): Account hijacking is like someone slipping into your online life and wearing your name tag. They post as you, peek at your messages, even lock you out. It often starts small - a fake login page, a weak password - and suddenly a stranger is in your space.

How it happens:

- Phishing pages that look real
- Malware that steals saved logins
- Weak or reused passwords
- Stolen 2FA codes (SIM swap, fake prompts)

Signs to watch for:

- New logins or devices you don’t recognize
- Password or recovery info changed
- Posts, messages, or purchases you didn’t make

If it happens, do this now:

- Change the password from a clean device
- Turn on 2-step verification (MFA)
- Sign out of other sessions; remove unknown devices
- Scan your device and update it
- Tell contacts that recent messages might be fake

Prevent it:

- Use strong, unique passwords (a manager helps)
- Keep MFA on; prefer an app or security key over SMS
- Double-check the web address before logging in
- Keep your system and apps up to date