

Hacking: What it is, how it happens, and how to stay safe

Gridinsoft Help Center

Hacking is finding a way into a system that wasn't meant to be used as a door. Sometimes it's done to fix problems (ethical hacking); other times it's to steal data, spy, or cause damage (malicious hacking).

Common ways it happens:

- Phishing and fake login pages
- Weak or reused passwords
- Unpatched bugs in apps, VPNs, or websites
- Insecure Wi-Fi or exposed remote access

What hackers might do:

- Steal logins, personal or payment data
- Take over accounts or devices
- Plant malware or backdoors
- Lock files for ransom or sell access

If you think you've been hacked:

- Disconnect from the internet; don't log in to sensitive accounts
- Run a full anti-malware scan and remove findings
- Change passwords from a clean device; enable MFA
- Review logins, sessions, and recovery options; sign out everywhere

How to prevent it:

- Use strong, unique passwords (a manager helps) + MFA
- Keep systems and apps updated
- Be cautious with links/attachments and public Wi-Fi
- Limit remote access; review who has admin rights

Learn more: [Hacker - who they are and how they work](#)