Security Software - what it is, why it matters, and the essentials to turn on

Gridinsoft Help Center

What it is

Security software is a set of apps and services that protect your devices and data from hackers, malware, and mistakes. It covers tools like antivirus/anti-malware, firewalls, VPNs, email and web filters, intrusion detection/prevention, and encryption. Together, they help keep your information confidential (only the right people see it), intact (not altered), and available (there when you need it).

Why it matters

One bad download or phishing click can leak logins, drain accounts, or lock files. Good security software blocks common attacks, warns you about risky actions, and gives you tools to recover if something slips through.

How it works

- Antivirus/anti-malware: scans files, apps, and memory for known and suspicious threats.
- Firewall: controls inbound/outbound network connections.
- Web/email protection: blocks phishing sites, malicious links, and dangerous attachments.
- VPN & encryption: scramble traffic and files so snoops can’t read them.
- Updates: keep definitions and engines fresh to catch new threats.

Red flags

- Constant pop-ups to "pay now to remove 100 threats" (could be scareware).
- Security tools disabled without you doing it.
- Browser search/homepage changed or new extensions you didn’t add.
- You’re still getting infected often - settings may be weak or software outdated.

Do it right

- Keep one reputable security suite enabled and up to date.
- Turn on real-time protection, web/mail filtering, and automatic updates.
- Use a password manager and MFA alongside your security tools.
- Schedule regular scans and review alerts; don’t ignore warnings.
- Back up important files so you can recover even if something goes wrong.