Cybercriminal: What it is, what they do, and simple ways to stay safe

Gridinsoft Help Center

What it is

A cybercriminal is someone who commits crimes using computers or the internet-either as the weapon, the target, or both. Think data theft, online scams, and break-ins that happen through screens instead of doors.

What they do (common plays)

- Data & identity theft: steal logins, personal info, or payment data to cash out later.
- Online scams & fraud: fake stores, phishing emails, tech-support cons.
- Malware campaigns: ransomware, keyloggers, info-stealers, botnets.
- Denial-of-Service (DoS/DDoS): flood a site or app so it goes offline.
- Cybervandalism: defacing sites, deleting data, or leaking content.

How they operate

- Social engineering: trick people into clicking, paying, or sharing secrets.
- Exploiting weak spots: unpatched apps, exposed remote access, reused passwords.
- Dark-web markets: buy/sell stolen data, malware kits, and "hacking as a service."

Protect yourself (quick basics)

- Use strong, unique passwords + MFA everywhere you can.
- Keep devices, browsers, and apps updated.
- Be skeptical of links, attachments, and sudden "urgent" messages.
- Back up important files offline; consider DNS filtering/AV.
- Verify money or account changes out of band (call the sender).