Threat Landscape - what it is, why it changes, and simple ways to stay ahead

Gridinsoft Help Center

What it is

The threat landscape is the big picture of online risks at a given time - the kinds of attacks happening, who's behind them, and which targets and tricks are most common. It includes everything from phishing and malware to data leaks, scams, and new vulnerabilities.

Why it matters

Knowing the landscape helps you pick the right defenses. If scammers are pushing text-message phishing or a new browser bug is being exploited, you can tighten settings, update devices, and warn people before trouble hits.

How it works - quick tour

- Actors: criminals, hacktivists, insiders, and sometimes state-backed groups.
- Techniques: phishing, ransomware, credential stuffing, social engineering, exploit kits.
- Targets: email, cloud accounts, phones, payment systems, small businesses, and schools.
- Trends: what's rising or fading (e.g., MFA bypass tricks, AI-written lures).

Red flags

- Sudden spikes in phishing texts/emails that mimic your bank or delivery apps.
- News of a major vulnerability affecting software you use - but your devices aren't updated.
- Recycled passwords showing up in breach alerts.
- Friends or coworkers reporting similar scams at the same time.

Do it right

- Update devices and apps quickly; turn on automatic updates.
- Use a password manager and MFA on important accounts.
- Learn common scam tells (urgent tone, weird links, requests for one-time codes).
- Back up important files so you can recover from ransomware or mistakes.
- Follow a trusted source (your security app or vendor blog) for simple, periodic alerts.