# Web Protection - what it is, why it matters, and easy ways to stay safe online

Gridinsoft Help Center

## What it is

Web protection is a bundle of tools and settings that keep you safer while you browse. It blocks dangerous sites and downloads, warns about fake logins, filters sketchy links, and helps keep your info private. It can run on your device (browser/security app), on a home/school network, or from your internet provider.

## Why it matters

Most attacks start on the web - a bad link, a fake page, or a shady download. Web protection catches many of these before they reach you, helping prevent malware, account theft, and tracking.

## How it works

- URL checks: compares sites you visit against known-bad/reputation lists.
- Phishing guards: spots look-alike login pages and blocks them.
- Download scanning: inspects files for malware before they open.
- Safe connection: enforces HTTPS and flags insecure forms.
- Content rules: optional filters for risky categories (pirated software, adult, gambling).

## Red flags

- Your browser shows "Not secure" on a page asking for a password or card.
- A site forces unexpected downloads or "update your browser" pop-ups.
- Short links that hide the real site, or URLs that look almost right (extra letters, weird endings).
- Your security app is off or can’t update its web protection module.

## Do it right

- Keep your browser, OS, and security app updated with web protection enabled.
- Don’t enter passwords on pages that look off; type the site address yourself.
- Let the blocker work-don’t bypass warnings unless you’re 100% sure.
- Use a password manager and MFA; they reduce damage if a site is fake.
- Download apps only from official stores or vendor sites.