OSINT (Open-Source Intelligence) - What it is, good uses, and how to stay safe

Gridinsoft Help Center

What it is

OSINT is the practice of gathering publicly available information - news, websites, social media, forums, government records, maps - and combining it to learn about a person, company, or event. For a quick primer and tool ideas, see our OSINT explainer.

Why it matters

The same open data that helps journalists and defenders can also fuel scams, stalking, and targeted attacks. Knowing what’s exposed helps you protect your footprint and lets security teams investigate threats without breaking the law.

How it works - quick tour

- Collect: grab data from search engines, social networks, WHOIS/DNS, breach dumps, court filings.

- Correlate: link handles, emails, domains, and locations to build a picture.

- Verify: cross-check sources, timestamps, and images to avoid false leads.

- Report: summarize findings with citations and screenshots.

Good uses

- Threat hunting: tie phishing domains and personas to prior campaigns.

- Brand protection: spot impostor sites and fake support accounts.

- Due diligence: validate vendors, incidents, and breach claims.

- Incident response: enrich IoCs with infrastructure and ownership.

Safety & ethics

- Follow local laws and site terms; avoid intrusive or private-data tactics.

- Do not engage with targets from personal accounts; use safe research profiles.

- Protect your team with MFA, VPN, and ad/script blocking while browsing.

- Treat sensitive findings as confidential and minimize what you store.

Reduce your own exposure

- Lock down social privacy settings and remove old posts with PII.

- Use unique emails and aliases for sign-ups; hide domain WHOIS where allowed.

- Strip metadata from files before sharing and delay location-tagged posts.

- Monitor for look-alike domains and fake profiles using alerting tools.