

Forum: [Hack Forums](#)

Thread: [OPSEC Checklist for Ethical Hackers: What NOT to Do When Researching Targets](#)

BreachFo - December 8, 2025, 5:37 am

OPSEC failures can reveal your identity, burn your reputation, or even lead to legal trouble—even if you're acting ethically. Avoid these common mistakes:

Reusing personal accounts: Never log into your real Twitter, GitHub, or Google account while researching a target.

Ignoring browser fingerprinting: Use Firefox with privacy-focused configs (or Tor Browser in safe mode) and disable JavaScript when possible.

Forgetting metadata: Screenshots from Windows or macOS often contain user names, system info, or window titles. Use Greenshot (with metadata stripping) or take screenshots in a VM.

Querying APIs from your home IP: Chain requests through rotating proxies or Tor—but be mindful of rate limits and ethical boundaries.

Posting raw findings publicly: Even in “private” Discords, assume anything you share can leak. Redact domains, IPs, and personal info unless part of a coordinated disclosure.

Using your real name or handle across platforms: Create separate personas for bug bounty, OSINT, and forums—but never use fake identities to deceive or social-engineer.

OPSEC isn't paranoia—it's professionalism.