

06.02.2026

OSINT and identity theft – when publicly available data become a danger

Personal information is more easily accessible today than ever before. Something many people aren't aware of: cyber criminals make targeted use of Open Source Intelligence (OSINT) to collect identities, create profiles and prepare scams. In combination with identity theft, this creates a serious threat.

What is Open Source Intelligence (OSINT)?

OSINT is the term used for systematically collecting and analysing publicly available information. This does not involve hacked data, but content freely available on the Internet, frequently published by victims themselves. Such data usually appear innocuous, but could provide a detailed personal profile if combined.

Some typical OSINT sources:

- Social networks (Facebook, Instagram, TikTok etc.)
- Public registers and lists
- Websites, forums and comments
- Images, videos and metadata
- Earlier data leaks and published records

How does OSINT work in practice?

Cyber criminals make targeted use of OSINT in a structured manner. Their starting point is the systematic collection of publicly available information such as names, e-mail addresses, telephone numbers or user names. These data are then linked to each other by analysing social media content, for instance posts, images or comments. Information on employers, hobbies or frequent whereabouts is also incorporated into their analysis. Step by step, an extensive profile of a person is thus created from seemingly innocuous data, enabling scammers to draw conclusions on habits, social contacts and relationships of trust. On this basis, scammers then prepare targeted attacks, for instance particularly credible scamming attempts or identity theft. The whole process is based on legally available information, which is abused for illegal purposes.

How to reduce your OSINT risk

It is hardly possible to protect yourself completely against OSINT-based attacks, yet you can considerably reduce the risks. The important point is to regularly check your social network privacy settings and to only share personal information in a mindful and sparing manner. Older profiles, posts and images should also be checked regularly and removed if necessary. In addition, we would recommend you do not use identical e-mail addresses and user names across all platforms. Special care should be taken with requests or messages containing a noticeably large amount of personal details. Basically, the fewer data are publicly available, the more difficult it will be to abuse them.

Conclusion

OSINT shows just how powerful publicly available information can be, both for good and for bad. In the wrong

hands, they can become the basis for identity theft and targeted scam attacks. If you are aware of the tracks you leave behind online, you can sustainably boost our digital security.