Case study: OSINT on a friend or family member

Imagine you are asked to think about a friend or family member and list what publicly available information could be found about them. The goal is to understand OSINT(Open Source INTelligence) risks and how to protect privacy, not to invade anyone's privacy.

Types of information that can often be collected

- **Basic identity**: Full name, nicknames, age or date of birth.
- **Contact details**: Email addresses, phone numbers, home address or previous addresses.
- **Social media profiles**: Accounts on Facebook, Instagram, LinkedIn, Twitter, TikTok.
- **Photographs and videos**: Posted images, tagged photos, event pictures.
- **Employment and education**: Employer name, job title, past workplaces, schools and graduation years.
- **Public records**: Electoral roll, property records, company filings, professional licences.
- **Hobbies and interests**: Membership in clubs, public forum posts, event attendance.
- **Online activity**: Comments, blog posts, forum accounts, GitHub repos.
- **Associations**: Relationships, friend lists, colleagues, organisations they belong to.
- **Geolocation traces**: Geotagged posts, check ins, or images with location metadata.
- **Financial or transactional traces**: Public business ownership records, crowdfunding or marketplace accounts.

Where this information is commonly found and how it is discovered

High level common sources:

- **Social media sites**: People post personal updates, photos, work history and contacts.
- **Search engines**: Public posts, news articles, mentions in blogs or local websites can be indexed.
- **Professional networks**: LinkedIn and industry directories show employment history and contacts.
- **Public records and government sites**: Property registries, company house filings, professional registers.
- **Online marketplaces and forums**: Usernames, item listings, and reviews reveal activity.

- **Image and video platforms**: Photos and metadata can show events or locations.
- **WHOIS and domain registries**: Can reveal domain ownership if not privacy protected.
- **Archived pages and caches**: Old versions of sites and web archives can contain removed info.

I am not giving step by step instructions. In practice investigators and analysts use search, site features and specialised tools to collect and correlate open sources. For ethical reasons you should only collect OSINT with permission or for legitimate, legal purposes.

Factors that make it easier to gather OSINT

- **Public, unprotected social media profiles**: Posts and photos set to public are the easiest to access.
- **Reusing the same username or email across services**: Makes it simple to link different accounts.
- **Frequent location sharing or geotagged images**: Reveals routines and places visited.
- **Published professional profiles and CVs**: Employers, roles and contact details are visible.
- **Online mentions in news, blogs or public documents**: Indexed by search engines and easy to find.
- **Low privacy hygiene**: Old accounts, forgotten posts, or data breaches that exposed personal details.
- **Weak privacy controls on domains and services**: WHOIS info not protected, public listing on directories.

Factors that make it harder to gather OSINT

- **Strict privacy settings** on social platforms and limiting friend lists.
- **Using different, unlinked usernames and emails** for different services.
- **No public sharing of location or photos** with geotags removed or disabled.
- **Minimal presence in public records** or use of business entities with privacy protections.
- **Good operational security** such as not posting identifying details on forums.
- **Use of privacy services for domains and secure email practices**.
- **Removal or minimisation of old public content** and regular clean up of profiles.

Ethical and legal considerations

- Collecting public data for security research, journalism, or consented investigations is different from stalking or doxxing.
- Always consider laws and terms of service. Some actions, even with public data, may be unlawful if used to harass, threaten, or defraud.
- Respect privacy, obtain consent where required, and follow your organisation's code of conduct if you are doing research.

Practical privacy checklist to reduce exposure

Share this with the friend or family member as constructive advice:

1. Set social accounts to private and review friend or follower lists.
2. Remove or limit geotags and location sharing on photos and apps.
3. Use different usernames or emails for public and private services.
4. Enable two factor authentication on important accounts.
5. Use a password manager to avoid password reuse.
6. Check and remove old posts, accounts or comments that reveal personal details.
7. Use domain privacy services if you register websites.
8. Regularly search your own name and email to see what is publicly visible.
9. Be cautious about sharing photos or documents that include personal data or metadata.
10. Know how to request removal from directories or contact site owners when necessary.

Conclusion

OSINT can reveal a lot about a person from publicly available sources. Understanding what can be found helps people protect their privacy and organisations manage insider risk. Always use this knowledge responsibly, focus on defensive measures, and respect legal and ethical boundaries.