What is Open Source Intelligence (OSINT)?

Open Source Intelligence refers to the action of gathering and analyzing publicly available data in order to gain information about a specific target.

What is open source data?

Open source data is any information that is either publicly available or can be made available: by request, through a paywall, or by physically being present at a place or event. Plenty of open source data can easily be discovered with the help of a search engine, but a lot of the pages that aren't indexed (which make up what's called the "deep web") may still be accessible to the general public, and so are still considered open source. Open source data doesn't just mean the obvious, either: you can get a user's name, birthday, and friends from their social media, but you can also find out when and where an image was taken, what device was used to make a post, and mine similar information from the metadata of specific posts.

What types of open source data are there?

There are a lot, but some useful ones include:

- Social media posts
- Newspaper and magazine articles
- Government reports
- Academic journals
- Information at public conferences
- Data leaks and breaches
- And more!

How can OSINT be helpful?

Open source intelligence is used by a number of different organizations. Government bodies are considered the biggest consumers of OSINT information, which they use to track global events and collect information for national security. Law enforcement and international regulatory organizations use OSINT for similar reasons. Businesses also

make good use of OSINT to investigate markets, collect information on consumers, and keep track of their competitors.

How can OSINT be dangerous?

OSINT is one of the first tools used by hackers to gain information on their targets. For attackers trying to enter a system, knowing what kind of security flaws may exist and what kind of approaches aren't worth trying is hugely valuable information, and specific searches can unearth that type of sensitive data without much effort. OSINT is also commonly used for social engineering, either to gather information on potential victims or impersonate similar people, which can later be used for phishing and to extract information from the targets. Finally, many passwords and accounts can be breached with enough personal information, especially if you don't put effort into keeping your accounts secure.

What are some useful tools for learning about OSINT? A good website for both planning how to gain open source intelligence and understanding the different types of sensitive personal information is the OSINT Framework. You can narrow down the specific data you are looking for and find the different, generally open source applications that are commonly used to scope out that information.