Hi, I'm Elaine Haigh, and I'm a lecturer in Cyber Security at the University of South Wales. In this short video I'm going to introduce Open Source Intelligence

Open source intelligence is often abbreviated to OSINT, but what exactly is it, and what is it used for?

It's open source – that means any legitimate source of information that's publicly available, often with free access. This can include any information that individuals or companies publish, either online or other public records such as telephone directories.

It's intelligence – and that can be any Information about a group or an individual that can be put to use for political, military, legal, commercial or malicious reasons.

So how can you find this information? While you are probably most familiar with Google as a way to 'google' or to find information on the Internet, there are a number of other search engines available that may give different results.

Search engines crawl the Internet looking for webpages, which they then index in a database, so that when someone searches for information it can quickly find the most relevant results. It also ranks the pages using a number of algorithms, such as how recent the website is and how often it's visited.

Metasearch engines use multiple existing search engine databases and categorise the results, so you don't have to. Some, like eTools, Dogpile and Yippy perform general searches, but many are used for specific categories, like holiday booking metasearch engines that just look for holiday bookings

Even deleted information can sometimes still be searched.

The Wayback Machine is a digital archive of saved webpages. You can search archives, and request a website to be saved.

Google Advanced Search allows you to build and filter specific searches, to narrow down results and help you find exactly what you're looking for. Find this under 'Settings' below the search bar. You can perform the same advanced searches by using search operators, known as Google dorks, along with the keywords in your search. For example you can search for specific file types or search certain sites.

Image searches are very powerful, using a combination of mathematical pattern matching, machine learning and metadata. Search engines can also categorise an image using context, such as captions, tags and text that appears next to an image

Reverse image is a great tool that allows you to upload an image and the search engine will return other instances of that image or similar images on the web.

There are specialist image search tools, but standard search engines, as well as stock image sites have powerful reverse image search capabilities.

Metadata is information about data, such as an image, including the file name and where and when it was produced. Some social media sites like Facebook strip the metadata from an image, but others don't. You can view metadata by file properties, or image data including location data by using an Exif viewer.

If you take an image using a smartphone with location services switched on and then you post images on Snapchat or Twitter, your images can be mapped. Anyone can search this information, even without using the app.

While search engines search files stored on webservers, Shodan searches the internet for connected devices, including IoT devices such as webcams. It's not illegal to look for devices on Shodan – but accessing private data is.

Even private information can become public. If a site with your username and password on it is breached, then those details can be sold or made public.

This can be a big risk if you use the same email address and password to sign up to different sites!

There are many other OSINT tools available, but who uses them, and why. OSINT techniques are widely used by hackers during the initial reconnaissance stages of an attack. . Criminals often spend a lot of time gathering information beforehand to plan the attack, using any number of unusual OSINT sources

Job adverts, social media posts and images, or CVs on LinkedIn can often provide clues to a company's computer systems, to allow hackers to target specific operating systems.

Google Maps Street View and other location-based social media images can often provide clues to physical security and working patterns.

Social engineering and targeted phishing attacks rely on trust – so finding out about somebody's habits, friends, interests and networks can make it much easier to trick a person into clicking a link on an email or giving out private information in person.

It's not all bad news – OSINT techniques are used more and more as a legitimate source of intelligence in criminal investigations.

'OxyMonster' was known for selling drugs on the dark web, but he had registered his bitcoin payments under his own name, Gal Vallerius.

The US Drug Enforcement Agency searched for social media accounts linked to Gal Vallerius. When they spotted an Instagram post that said he was making his first-ever trip to the US to attend the 2017 World Beard and Mustache Championships, they met him at the airport.

He is now serving 20 years in prison.

On July 17th 2019, Capital One received an email informing them of a possible data breach that had been spotted on Github. The linked Github account was registered with Paige Thompson's real name and address. Searching for other social media accounts linked to Paige’s name revealed Twitter and Slack messages where she admitted to hacking Capital One.

Paige is currently awaiting sentencing.

If you’ve ever used Google maps, or found somebody’s Instagram account, you have used OSINT techniques. If you’re interested in developing those skills and using them for good, it’s easy to get involved

The OSINT Framework is a useful website that brings together available tools and resources to help you find specific types of information. But remember that with a lot of these tools, you are giving out more information than you are getting, and you must have a legitimate reason for using them.

Tracelabs is a platform that uses crowdsourcing techniques to bring people together to look for missing people, passing any data to law enforcement agencies. Events are run as CTF competitions, and anyone can join.

If youre interested in finding out more, get in touch with the university of South wales and consider booking a place on one of the upcoming open days. In the meantime, use some of the techniques shown in this video to find out what the internet knows about you