# Intro to Open-Source Intelligence

October 14, 2024

CYBER SECURITY CLUB AT UC DAVIS

# Preview For The Day

## Intro to Open-Source Intelligence

What is Open-Source Intelligence (OSINT), and what does it look like in action?

## Internet Research

How can we use certain keywords to improve our Google searches?

## OSINT in Action

What tools are involved in OSINT, and how do we use them?

How can we use various OSINT tools to build profiles and gather information on targets?

How much of our personal information is online, and what can we do to limit the amount that gets there?

# 1.

# Intro to Open-Source Intelligence

What is OSINT, and what does it look like?

# Doxxing: How does it Happen?

What is doxxing?

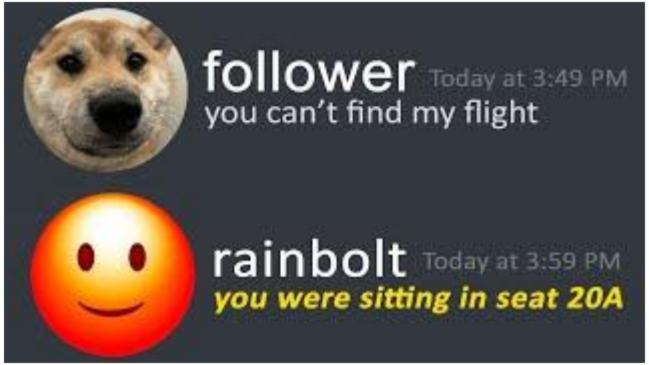
- Finding and posting someone’s personal information (name, address, Social Security number, etc.) online, usually to encourage negative attention towards them

How does someone find personal information online?

# What OSINT Looks Like

https://www.tiktok.com/@notkahnjunior/video/7229889153595411758

https://www.youtube.com/watch?v=1OSrinkgJa0



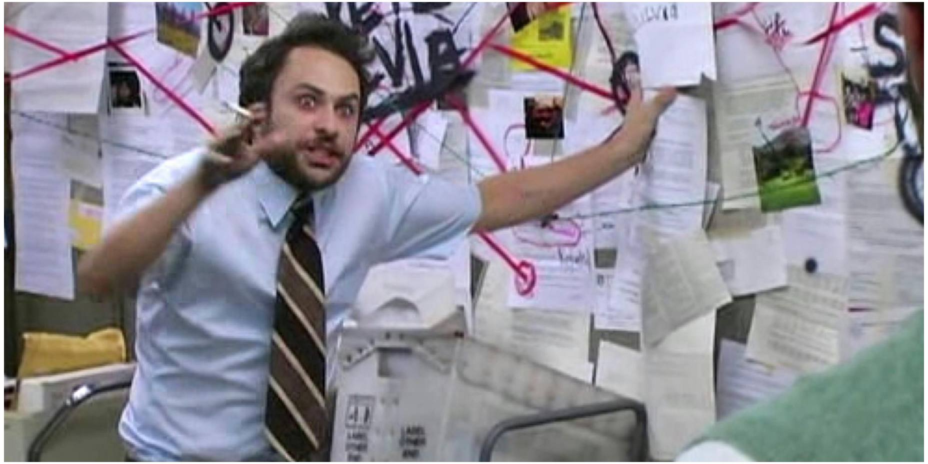
follower Today at 3:49 PM
you can't find my flight

rainbolt Today at 3:59 PM
*you were sitting in seat 20A*

# So What Is OSINT?

**Open-Source Intelligence (OSINT)**

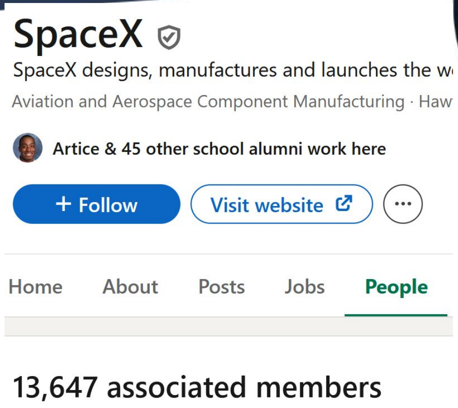
1) The gathering of information from open / publicly available sources
2) Using this open information to make inferences and gain insights/gather intelligence



# OSINT in Cyber

## OSINT Is Reconnaissance

- How much information does a company put online?
- What can you determine from it?
    - People & contact info: potential targets!
    - What software do they use?
    - Do they badge and have security?
    - The list goes on…



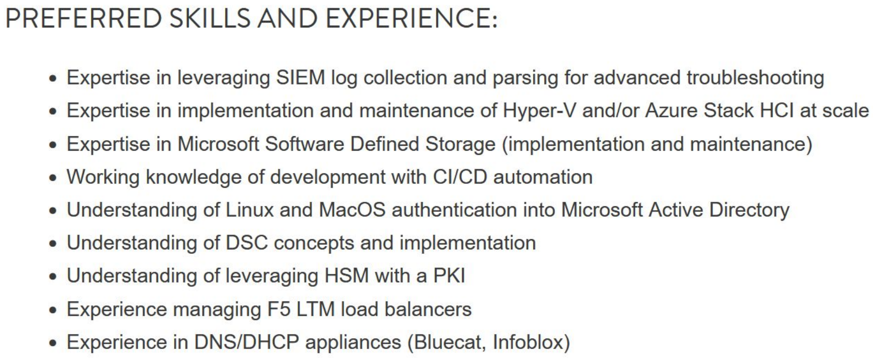
SpaceX

SpaceX designs, manufactures and launches the w

Aviation and Aerospace Component Manufacturing · Haw

Artice & 45 other school alumni work here

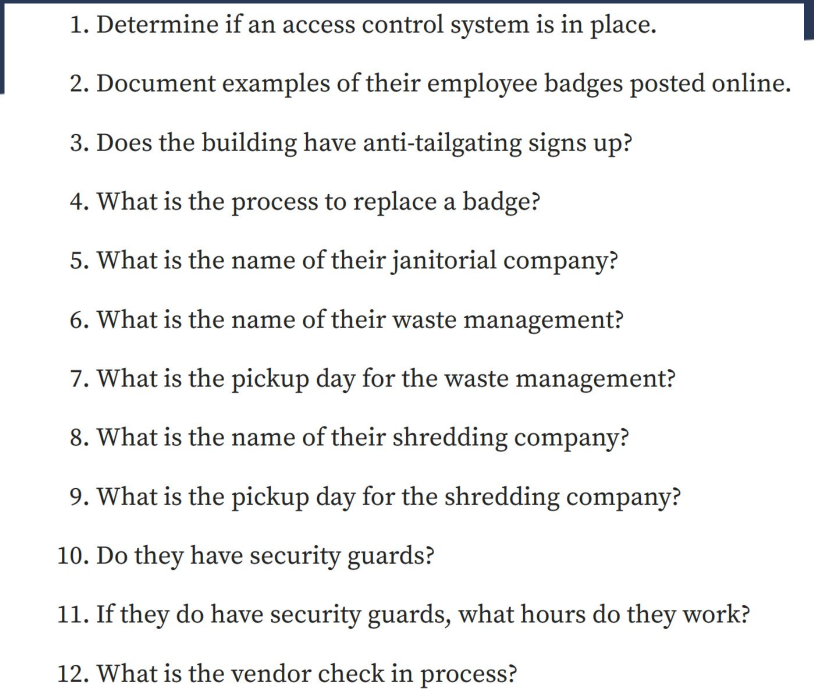
13,647 associated members



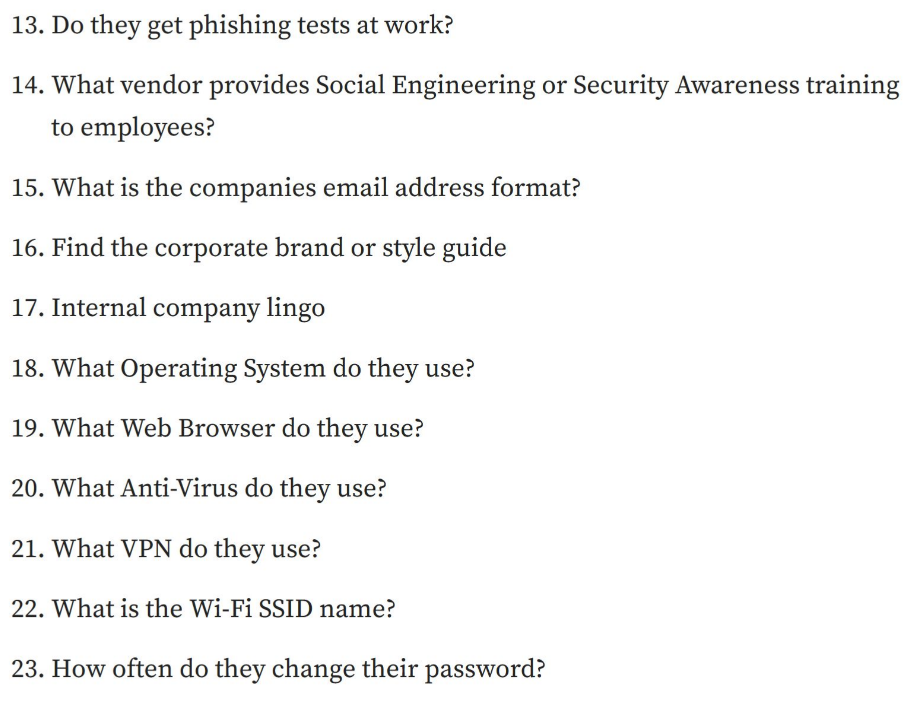
PREFERRED SKILLS AND EXPERIENCE:

- Expertise in leveraging SIEM log collection and parsing for advanced troubleshooting
- Expertise in implementation and maintenance of Hyper-V and/or Azure Stack HCI at scale
- Expertise in Microsoft Software Defined Storage (implementation and maintenance)
- Working knowledge of development with CI/CD automation
- Understanding of Linux and MacOS authentication into Microsoft Active Directory
- Understanding of DSC concepts and implementation
- Understanding of leveraging HSM with a PKI
- Experience managing F5 LTM load balancers
- Experience in DNS/DHCP appliances (Bluecat, Infoblox)

# OSINT in Cyber



1. Determine if an access control system is in place.
2. Document examples of their employee badges posted online.
3. Does the building have anti-tailgating signs up?
4. What is the process to replace a badge?
5. What is the name of their janitorial company?
6. What is the name of their waste management?
7. What is the pickup day for the waste management?
8. What is the name of their shredding company?
9. What is the pickup day for the shredding company?
10. Do they have security guards?
11. If they do have security guards, what hours do they work?
12. What is the vendor check in process?



13. Do they get phishing tests at work?
14. What vendor provides Social Engineering or Security Awareness training to employees?
15. What is the companies email address format?
16. Find the corporate brand or style guide
17. Internal company lingo
18. What Operating System do they use?
19. What Web Browser do they use?
20. What Anti-Virus do they use?
21. What VPN do they use?
22. What is the Wi-Fi SSID name?
23. How often do they change their password?

Could you find enough info to sneak in?

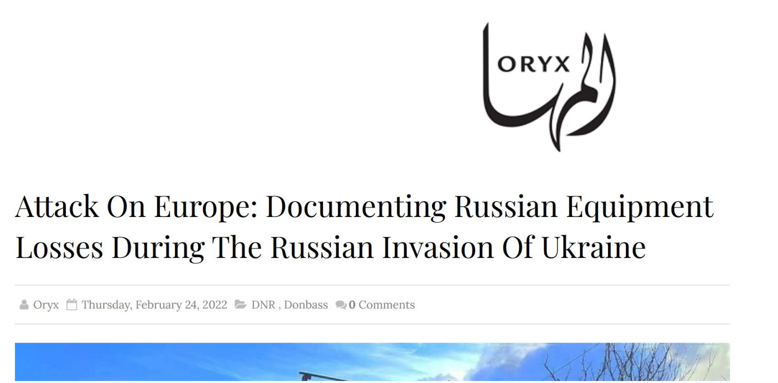
# OSINT Beyond Cyber

## OSINT Investigations

Investigators use OSINT to dig deeper into what's going on

- Track people/things
- Analyze global conflict
- Investigate criminals

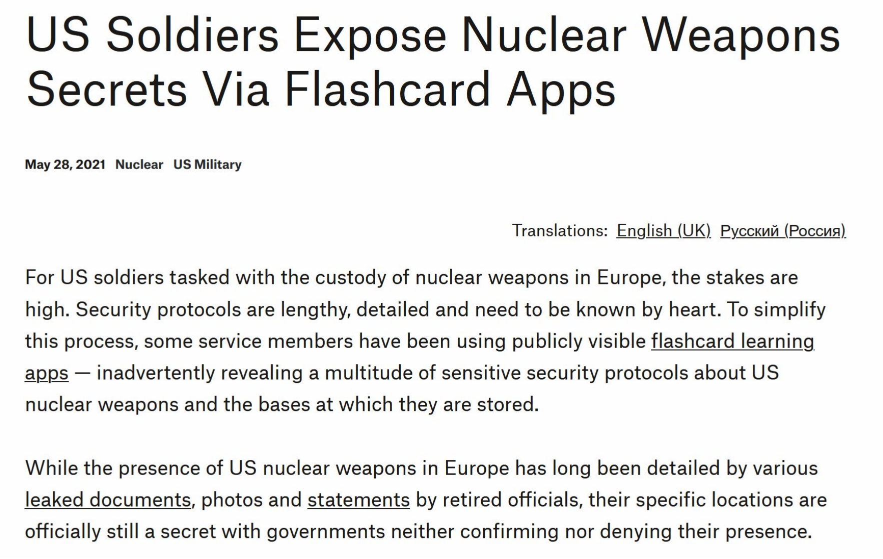
The list goes on and on!



ORYX

Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine

Oryx Thursday, February 24, 2022 DNR , Donbass 0 Comments



US Soldiers Expose Nuclear Weapons Secrets Via Flashcard Apps

**May 28, 2021 Nuclear US Military**

Translations: English (UK) Русский (Россия)

For US soldiers tasked with the custody of nuclear weapons in Europe, the stakes are high. Security protocols are lengthy, detailed and need to be known by heart. To simplify this process, some service members have been using publicly visible flashcard learning apps — inadvertently revealing a multitude of sensitive security protocols about US nuclear weapons and the bases at which they are stored.

While the presence of US nuclear weapons in Europe has long been detailed by various leaked documents, photos and statements by retired officials, their specific locations are officially still a secret with governments neither confirming nor denying their presence.

# 2.

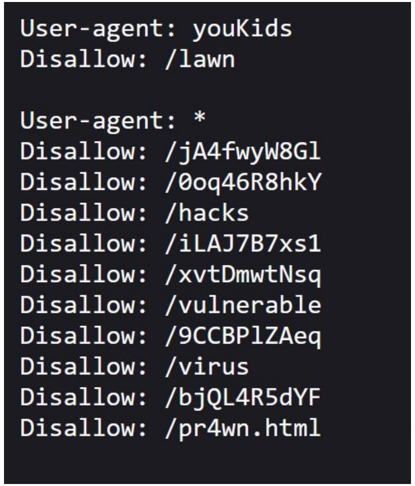
# Internet Research

How do I unlock the power of my browser?

# Web Crawling Around The Net

How does Google “find a website?”

- Crawling hyperlinks with a web crawler
    - Go to a page, record all the links, go to a link and repeat the process
- You can tell Google to not index certain sites, but it doesn’t mean it’s invisible



```
User-agent: youKids
Disallow: /lawn

User-agent: *
Disallow: /jA4fwyW8Gl
Disallow: /0oq46R8hkY
Disallow: /hacks
Disallow: /iLAJ7B7xs1
Disallow: /xvtDmwtNsq
Disallow: /vulnerable
Disallow: /9CCBPlZAeq
Disallow: /virus
Disallow: /bjQL4R5dYF
Disallow: /pr4wn.html
```

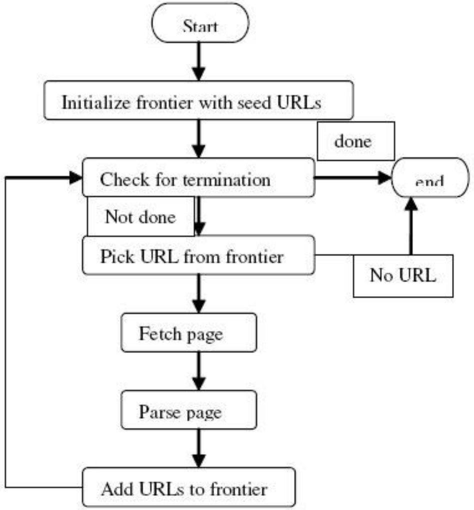


Fig. 2: Flow chart representing a web crawler

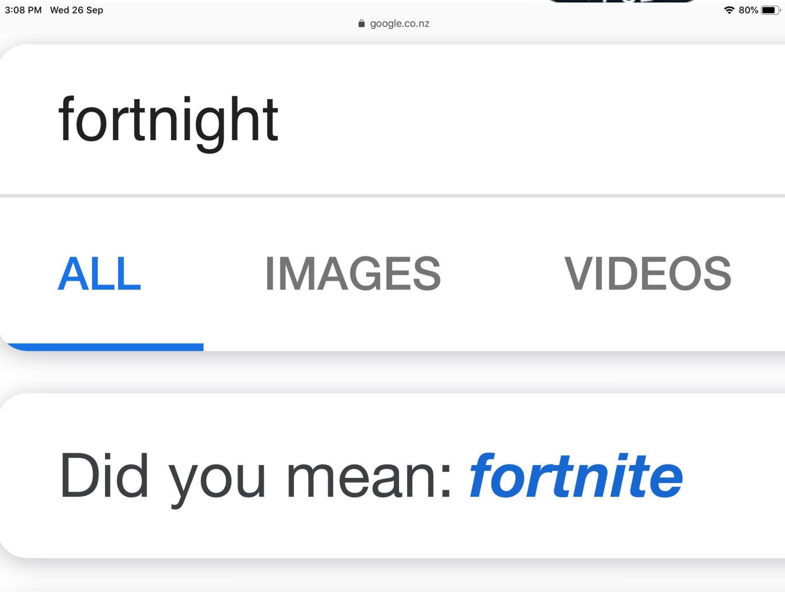
# Google Sucks Sometimes

Did you ever look something up but Google thought it was something else?

How did you solve it?

- Add more relevant search terms?

What if you're looking for something REALLY REALLY specific?



fortnight

Did you mean: *fortnite*

# Google Operators: Pro Searching

## How To Tell Google To Look At Specific Things:

- *site:* - Tells Google to only look search in that website
  - *site:stackoverflow.com segmentation fault* - Searches for segfault related pages on Stack Overflow
- *“ ”* - Forces Google to find an exact match for that word in your results
  - *“To be, or not to be”* - Searches for pages that has that exact phrase in it (AKA the text of Hamlet)

MORE: https://ahrefs.com/blog/google-advanced-search-operators/

# The Thing I Want is Gone!

Oops, the thing I want is too old and it’s disappeared from the Internet!

Try the WayBack machine.

UC Davis

Residence Halls 2023-2024

Fee SCHEDULE

*Not on the Internet anymore, but I can find it on Wayback!*

# 3.

# OSINT in Action

What tools can I use to gather open information, and what can it tell me?

# Too Much Info Online!

**Data Brokers** - Companies that collect available information on people to build profiles about them

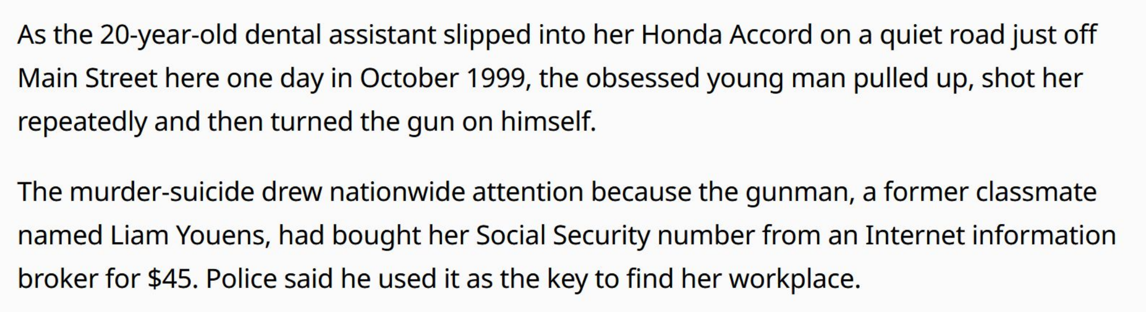
- Request "publicly available" personal data on people
- Use web trackers like cookies to keep track of your habits, leanings, etc.

cardlytics
Forbes
Albertsons
BeenVerified.com
The Weather Company
An IBM Business
checkmate
tripadvisor
FOURSQUARE
mylife
radaris
acxiom
EQUIFAX
TiVO
spokeo
experian
EPSILON
truthfinder
LiveRamp
whitepages
SEARCH. FIND. KNOW.
neustar
nielsen
INTELIUS
VISA
ORACLE
MasterCard
TransUnion
AT&T

incogni

DeleteMe®

# Too Much Info Online!



As the 20-year-old dental assistant slipped into her Honda Accord on a quiet road just off Main Street here one day in October 1999, the obsessed young man pulled up, shot her repeatedly and then turned the gun on himself.

The murder-suicide drew nationwide attention because the gunman, a former classmate named Liam Youens, had bought her Social Security number from an Internet information broker for $45. Police said he used it as the key to find her workplace.

# Good Info Segment

https://www.youtube.com/watch?v=wqn3gR1WTcA

# Evidence and Techniques

## Photos

- Check the EXIF metadata to see if any was left behind
- Reverse image search to see if you can find any clues as to what it is

## Social Media

- Check posts for any other types of “evidence” that reveal information

## Websites

- View the WHOIS registration data to see who owns it
- Use the Wayback Machine to check archived versions of the site

# Evidence and Techniques

### Usernames

- See if any other accounts with the same username have more info

### Email Addresses

- Plug them into tools to see if more accounts pop up!

### Anything!

- What can you infer from details people leak about their life?

# How to Defend Yourself From OSINT?

- **STOP POSTING EVERYTHING ON SOCIAL MEDIA!!!**
  - Stuff put on the Internet STAYS there. Be mindful of what you put out there
  - You don’t know who could be watching. Act like someone is

# How to Defend Yourself From OSINT?

- Don’t link your online identity to your real one!
  - Avoid mixing your name and your online name together!
- Private any accounts you use and ONLY allow people you know to see them!

# OSINT Demos

https://cryptokait.com/workshops/national-cyber-league-coaching-guide-v-2-1/ncl-coaching-guide-resources-by-category/open-source-intel/metadata/

https://gralhix.com/list-of-osint-exercises/

https://sector035.nl/quiz/beginners/

# Review

## Intro to Open-Source Intelligence

OSINT:

Using publicly available information to gain new insights

## Internet Research

How to improve searches?

Keywords, Wayback, etc.

## OSINT in Action

There’s a scary amount of information out there.

It’s up to you to connect the dots.

# Thanks!

## Any questions?

CYBER SECURITY CLUB AT UC DAVIS