Your Identity

WHAT CAN PEOPLE FIND ABOUT YOU BY SOME SIMPLE SEARCHING

This presentation centers around Open-Source Intelligence (OSINT) to find out what others can learn about you – the first step to personal identity management.

HOW TO PROTECT YOUR IDENTITY BY UNDERSTANDING WHAT DATA IS ACCESSIBLE AND HOW TO LIMIT THAT ACCESSIBILITY

Why Identity Management Matters

1

Enterprise Growth in Identities

81% of IT security professional said the number of identities in their organizations has at least doubled over the past decade.

2

Preventable Identity Breaches

79% of organizations have experienced an identity-related security breach in the last two years.

99% believe their identity-related breaches were preventable.

3

Privileged Identities a Top Target

74% of data breaches involve access to a privileged account.

4

Poor Password Habits

73% of people use the same password for multiple sites.

33% use the same password every time.

5

Cost of Identity Mismanagement

$51-$72 billion in losses to the worldwide economy could be eliminated through the proper management and protection of identities.

What would you call…..

- Searching for a coffee shop on Google Maps?
- Researching a business you want to invest in?
- Finding that long lost friend?

We call it

OSINT – Open-source Intelligence

Who Uses OSINT?

- Parents researching caregivers
- Those looking for love
- Businesses
  - Competitive Intelligence
  - HR
- Media
- Law Enforcement / Intelligence Agencies

- Bad Actors

Open-source Intelligence

(OSINT) – the practice of collecting and analyzing information from published or otherwise *publicly available* sources.

Key Takeaway about OSINT:

- This intelligence is derived from data that is available to the general public. It is not limited to a “Google Search”.
- Information overload can be concerning. Data still needs to be verified
- There is a dark side to OSINT, anything you can find can be found and used by bad actors

What Do You See?

Hawaii Emergency Management Agency

Twitter Goes to Work

Michael Henriksen
@michenriksen
Following

Attempted to identify things in the picture that could be interesting to an attacker, apart from the password on the post-it note. What did I miss?

- Camera Placement
- Phone Numbers
- Software Usage
- Badge
- Bluetooth Headset…
- etc.

https://twitter.com/michenriksen/status/953616091368099840

Movie time

This widely known video titled “Data To Go” looks at how quickly your data can be obtained with a quick Facebook search.

How private is your personal information?

How this goes beyond Google

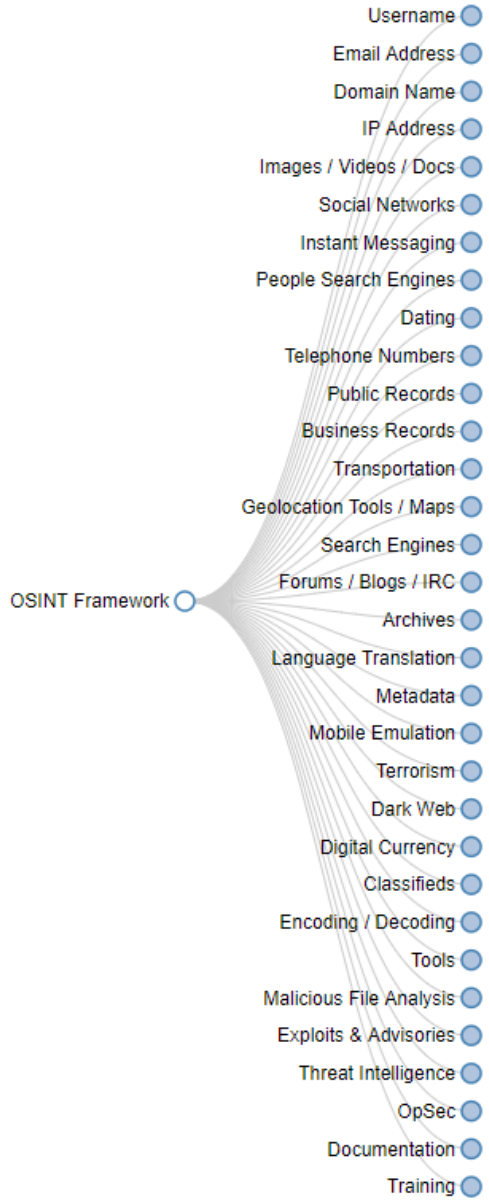
There is an entire framework around open-source intelligence and what resources are available to those searching:

https://osintframework.com

https://osintframework.de

https://intelx.io/tools

https://yoga.osint.ninja



Let's talk Search Engines

- Use multiple search engines for different perspectives
  - DuckDuckGo.com 
  - Bing.com 
  - Yandex.com Yandex
  - Google.com Google

Let's go Searching!

I'll use myself as a quick example of what type of results you can get. Take the time to start searching yourself.

Things to remember:

- People may have more than one "name"
- Information should always be verified and not taken at face value

Operators to help in the Search

Operators	Function	Example
"" (quotes)	Group terms together.	"Security Awareness"
- (dash)	Negates the term. Do not show results with this content.	-lawyer
site:	Results must come from the URL specified	site:uthsc.edu
filetype:	The filetype or file extension of the results	filetype:pdf
OR	One term or another	teacher OR lawyer

How to Protect and Manage your Online Identity

1. Limit the personal information you share on social media
2. Browse in private mode
3. Use a different search engine
4. Use a virtual private network (VPN)
5. Be careful where you click
6. Secure your mobile devices, too
7. Use quality antivirus software

How to FIND and DELETE Old, Unused Accounts

The first problem is finding these old accounts. Then you must take the time to delete the account.

Some of this is complicated, so here is the article from which this information is coming: https://lifehacker.com/how-to-find-and-delete-all-your-old-unused-accounts-1847470037

Step 1 - How to Find Old Accounts

The first place to search is in your web browser. Most modern browsers can save login info for any websites you access, and you can quickly find any accounts you've saved from the settings menu. Here's where to look in Chrome, Edge, Firefox, and Safari:

- **Chrome:** Go to **Settings > Passwords.**
- **Edge:** Go to **Settings > Profiles > Passwords > Saved Passwords.**
- **Firefox:** Go to **Preferences > Privacy and Security > Saved Logins.**
- **Safari:** Go to **Preferences > Passwords.**

Also check social media accounts profiles that you might have used to log into accounts using those credentials:

- **Apple ID:** On your iPhone or iPad, go to **Settings > Password and Security > Apps Using Your Apple ID.**
- **Facebook:** Go to **Settings > Apps and Websites.**
- **Google:** Go to myaccount.google.com then click **"Security."** Check under "Third-party apps with account access" and **"Signing in to other sites."**
- **Instagram:** Go to **Settings > Security > Apps and Websites**
- **Twitter:** Go to **Settings and privacy > Account > Apps and Sessions > Connected Apps.**

How to FIND and DELETE Old, Unused Accounts

Step 2 - Recover Your Passwords

If is has been years, you probably don't remember the password, but you need to be in control of the account in order to delete it. Hopefully, you still have access to the email address used when setting up these accounts, so a "recover username" or "recover password" link is helpful.

Step 3 - Delete the Account

This is where it gets complicated, as different accounts will have different ways of deleting information. And they want to keep your data, so they make it hard to do. Read the article (**https://lifehacker.com/how-to-find-and-delete-all-your-old-unused-accounts-1847470037** - if you didn't see it up top) for suggestions on how to delete some accounts, but if you have no luck, contact that company and have them do the work.

Conclusion

01

Segment your life by using different usernames, passwords and profile avatars

02

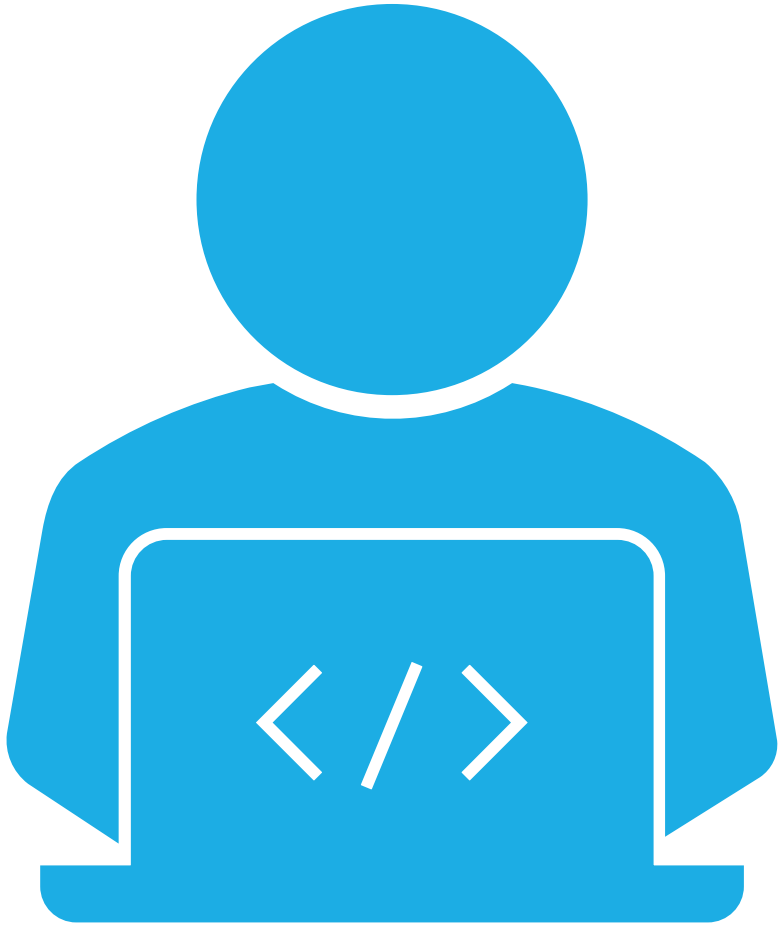
Monitor your email addresses for discovery in breach data

- Change any passwords on sites where breached data was disclosed and on other places you might have used the same usernames and passwords

Final Movie time

For this final video for this talk and this series of talks, let's look at a cyber attack as if it happened in real life.

What would a cyber attack look like in the real world?



CONTACT INFORMATION

Chris Madeksho – Cybersecurity Analyst

mmadeksh@uthsc.edu

901.448.1579

Office of Cybersecurity

itsecurity@uthsc.edu

901.448.1860

https://uthsc.edu/its/cybersecurity/


QUESTIONS?