LESSON GUIDE

INTRO TO CYBERSECURITY

Human Factor

2.2.2 - OSINT

Lesson Overview:

Students will:

- Investigate open source-online tools (OSINT) used to perform reconnaissance

Guiding Question: How and why is Open-Source Intelligence used legally to gather free, public information?

Suggested Grade Levels: 8 - 12

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

GALANTECH — with — GARDEN STATE CYBER

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

OSINT

Slide 1 - Intro Slide

Slide 2 - OSINT - Open-Source Intelligence Tools

So, think about it – HOW do malicious actors gather information to create compelling emails that seem realistic and ideally target the right individuals? One of their tools is to use OSINT – Open-Source Intelligence – tools. The key with OSINT is to mine the Internet for publicly available information.

No need to hack into anyone's accounts because most people have a fairly deep online presence, and most of that information is open to the public!

Slide 3 - OSINT Definition

In reviewing the OSINT definition, it's helpful to emphasize these characteristics:

- Free - if you have to pay a fee to get the information, then it isn't OSINT
- Public - it must be available to anyone. If you need membership in an organization then it isn't OSINT. Example: if I want to find all the computer science teachers that belong to CSTA, I would need to become a member to get a list. That's not OSINT.
- Legal - you cannot take any action to bypass controls that protect the information. If you crack a password or use phishing to get credentials or hack into an organization's database then you have broken the law.

BUT here is a gray area of OSINT…if someone else steals information and posts it online publicly then technically that is OSINT. Good chance to discuss ethical boundaries. If you are the police investigating a criminal, would it be ethical to use home address/phone info posted after a data breach? If you are a marketer looking to sell video games to children, is it okay to use school data posted after a data breach?

Slide 4 - What's Online About You?

Short video to give students an idea of how intrusive it can be for strangers to be looking at your "private" online information. Video: 2:47 minutes link: https://www.youtube.com/watch?v=YLWmjpPoJHk&ab_channel=BuzzFeedVideo

Slide 5 - OSINT Tools

The obvious place to start is a plain Google Search for someone's name BUT make sure to use proper search technique - John Doe will return information on John, on Doe, on John Doe. Instead put your search term in quotations so that it returns information only to the full name, John Doe. Encourage students to try different search engines besides Google as this will often produce different top results.

Ask the students what info do you think you could find from:

- Google Streetview or Satellite view? (Possible answers could be - what kind of car does the target drive? How many cars do they have - could this indicate teenagers? Do they have a pool? Etc.)

- Google Reverse Image search - if you have a pretty good picture of the target, you can easily find websites that include photos of the target

- Archive.org - old websites that are no longer online

- Social media sites - many people post information and don't restrict it to their friends.

Slide 6 - OSINT Tools (Continued)

- A LinkedIn search will not only show career information, but may also have information about the target's business contacts.

- During an election season, a spear-phishing campaign might target people who support one of the candidates or political parties

- Shopping - it's kind of fun to see what people have on their wish lists!

- Contact info - how to find their phone number, kids, spouse, age, etc. - Pipl and Spokeo will usually give a good start on that info.

- Real Estate - do they own a house? More than one house? Did they recently buy or sell - how much money was involved? This info could help fine-tune a spear phishing concept.

Slide 7 - Example OSINT

Let's go through an example of how we can apply these tools for an Open-Source Intelligence search. The activity for this lesson is an OSINT/Phishing project so this example will help them visualize how to approach their own OSINT investigation. Starting with just the target's name and town, we will begin looking for online public information about their personal life.

Slide 8 - ACTIVITY: OSINT Report on Tony Stark

Students will practics using OSINT tools. They will complete a report on the target, Tony Stark, by looking at mock online info in the OSINT Personal Data Challenge E-mate Activity.
https://d2hie3dpn9wvbb.cloudfront.net/osint-pd/OSINT_PD_Challenge.html

See student worksheet and teacher answer key.

Once students have completed their report, use Slide #9 to demonstrate how the OSINT info could be crafted into phishing emails. If you have time, you can use slides 9 - 13 to review what info is found in each OSINT item.

Slide 9 - Possible phishing emails from this OSINT

Now we have plenty of information to create some phishing emails to send Tony.

- On the left we used the following info to craft the phish: they want a bigger house, they need enough bedrooms for at least kids (plus a guest room), their previous house had a pool and a dock, probably want to stay close their area. When you click on the pictures link it takes you to a Realtor.com article about online scams.

- On the right we used the following info to craft phish: they have a new puppy, they live in Southfolk, they used to live in Malibu, they have kids. We know that they lived in Malibu but it was a while ago, so they probably won't really remember who was in pre-school with their child. When you click on the coupon it takes you to an article about coupon scams.

Slide 10 - Review info found from this OSINT - Spokeo

A search at Spokeo.com results in several "Tony Starks" but we can narrow it down to this one because the current residence is in Southfolk, VA. Notice that he used to live in Malibu. Point out to the students that we are gathering as much info as possible to see where it leads. Since the first listed family member is a femal and has a hyphenated last name, that could be Tony's Wife

Slide 11 - Review info found from this OSINT - Facebook

This is Tony's wife and her Facebook has some public postings. This one includes a lot of information including a link to their recent Zillow listing!

Slide 12 - Review info found from this OSINT - Zillow

By going to the Zillow link, we can get a bit more insight into their family details.

Slide 13 - Review info found from this OSINT - Twitter

We haven't done much searching for Tony's OSINT so let's look on Twitter. If someone uses their real name then it's fairly easy to find their account and all postings are public. We are able to find Tony's Twitter with a recent Tweet about his new dog.

Slide 14 - Review info found from this OSINT - Instagram

Find Tony's Instagram account info which tells us his favorite baseball team.

Slide 15 - Review info found from this OSINT - Tony's Blog

Find Tony's Blog info that has a picture. We can use that picture to pinpoint where he was. (See next slide)

Slide 16 - Review info found from this OSINT - the Metadata

Every photo and file have info saved with it to identify things like who created the file, when it was created, what software was used, etc. This is called "metadata" and with pictures, there is a LOT of info. Using an "Exif" tool, this data can be recovered by anyone with access to the original file or photo. We don't cover Metadata in this course but since it was an item in the E-Mates challenge the students will get a small look at this additional type of data that can be gathered.