Lab - Employee Intelligence Gathering

Objectives

Use social media to collect personal identifiable information (PII).

- Gather Information Through Social Media.

Background / Scenario

Unfortunately, people often post too much information about themselves online for anyone to see. This makes them very vulnerable to attacks. Threat actors can easily collect a lot of PII about a victim simply by conducting reconnaissance on social media sites such as Facebook, LinkedIn, Twitter, WhatsApp, and Instagram. They can then use this information to identify victims and to steal PII to be used for nefarious purposes.

Because of this, it is important for individuals to monitor their social media footprint and to be aware of the data that is publicly accessible.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of, and compliant with, computer use and privacy laws.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1: Gather Information Through Social Media.

For this lab, you will play the role of a cybercriminal and investigate your own social media to see how much PII you can obtain. Alternatively, you can get permission from someone you know well, such as a friend or relative, and investigate their social media. At the end of the exercise, you can share with them what you discover.

Step 1: Conduct the investigation.

Conduct a search for your name and usernames, using different search engines. Open an incognito or private window for this lab. This will prevent any of your saved login information from populating and you should not see any cached content as you search. Use variations of your name as well, with and without a middle name or initial, married, and maiden names, etc.

This will allow you to see what is indexed.

Step 2: Perform an audit as a stranger.

a. Create a “bogus” social media account to view your own profiles as a stranger would.
b. Conduct an audit of all the social media sites and accounts you have used.

Look for identifiable information and behavioral patterns that could be helpful to an attacker. This includes things like your place of employment, where you live, online shopping preferences, your daily schedule, vacation plans, political beliefs, interests, hobbies, education, cultural beliefs, family members, pets, etc.

Items to investigate include:

1. All your social media profiles - name, birthdate, contact information, etc.
2. Your status updates - life events, work relationships and status, political and religious beliefs.
3. Location data - hometown information and geo check-ins.
4. Shared content - pictures and comments you have posted and those where you are mentioned or tagged.
5. Posts from friends and family.
6. Any online discussions you have joined or participated in.

What type of information about you was revealed from your investigation?

Answer Area

<!----><!---->

Part 2: Reflect on Your Findings.

1. Reflect on ways a cybercriminal may use the following information:

a. Your workplace information.

Answer Area

<!----><!---->

b. Your interest in particular hobbies or interests.

Answer Area

<!----><!---->

c. Your public conversations with friends or relatives.

Answer Area

<!----><!---->

2. Based on the findings of your social media footprint analysis, what would you recommend as social media best practices to keep your identity safe on Social Media?

Answer Area

<!----><!---->