Understand and Protect Against Open Source Intelligence

Presented by Anastacia Webster
About me...
What is Open Source Intelligence?

• What are open sources?
• What is intelligence?
• How do the two meet?
• Why should we care?
OSINT Workflow

1 to ∞

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone Number</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address (All of them)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job Address</td>
<td>Job Telephone Number</td>
<td>Relative</td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td>Civil and Public Court Records</td>
<td>Criminal Records</td>
</tr>
<tr>
<td>Photos</td>
<td>Photos of Address</td>
<td></td>
</tr>
<tr>
<td>Marriage</td>
<td>Divorce</td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>Past Employment</td>
<td></td>
</tr>
<tr>
<td>Drivers License</td>
<td>Voter Registration</td>
<td></td>
</tr>
<tr>
<td>Tax Filings</td>
<td>Accidents</td>
<td></td>
</tr>
<tr>
<td>ETC…</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy vs. Information Privacy

• Privacy is NOT absolute...
• Information Privacy...NON-EXISTANT

Privacy Arguments
• Pro:
  • “I have nothing to hide.”
• Con:
  • Those stories we don’t want our bosses knowing about
Autumn Matacchiera

• Allegedly threw five year old girl in front of a train...

• Within hours, comments appeared on her personal blog from users using OSINT techniques to find her online.

• **Note: By this time her FB was already deactivated.**
Suitable For Framing

• Store allegedly refused to frame a customers inauguration pics...

• Within hours of the story, yelp site was flooded with poor reviews and nasty comments.
Some grey areas...

Some Ethical Issues
- Disinformation
- Accuracy
- Credibility
- Reliability
- Abuse of Power
  - Integrity
- Exploitation
- Privacy
- Aggregation
  - Confidential and Classified Data/Info
FBI Warns of Online Dating Scams

• Targeting women 40+ who are divorced, widowed, and/or disabled…but everyone at risk..

• Scam: Contacted by someone online that appears interested

• Attacker/scammer build rapport, may even send items (i.e. flowers)

• Asks you for money, to cash checks, or to forward packages
On February 3, 2016, Law Enforcement, in conjunction with the Los Angeles Times, released a statement against the wave of false deportation checkpoints on popular platforms like Facebook, Instagram and Twitter.
Using OSINT to Find the Scammers

https://blog.haschek.at/2016/how-a-scammer-stole-500-dollars-from-me

• SUCH AN AMAZING STORY . . .
Open Source Intelligence and Research Association (OSIRA) Code of Ethics

1. Responsibility
   • Take responsibility for your actions.

2. Professionalism
   • Always continue to learn and strive for moral high ground.

3. Credibility
   • Be objective and verify the credibility of sources/accuracy of information.

4. Personal Example
   • Be a role model to others by displaying honesty, integrity, and selflessness.

5. Sense of Mission
   • Advance OSIRA and uphold professionalism.

6. Comradeship
   • Help out other OSINT researchers.
...Cool story, bro...But why should I care?
HACKERS CARE... That’s why...
Recon Village

An Open Space with Talks, Live Demos, Workshops, Discussions, CTFs with a common focus on Reconnaissance.

Get Involved..
Data + Information = Knowledge = POWER!

- Name
- DOB
- SSN
- Address (Current and past)
- Employers/Coworkers (current and the past, hierarchy, friendliness)
- Phone Number (Cell, home, work)
- Family (Names, #, POB, DOB, SSN)
- Friends (Names, #, DOB, SSN)
- Likes/Dislikes (Movies, music, newspapers, etc.)
- Political/Religious Views
- Relationships (Wife, mistress, girlfriend...)
- System Information (operating systems, IP, software configurations)
- Personnel Information (employees, position, emails, etc.)

- Interests/Hobbies
- Photos
- Videos
- Purchases
- Car/Truck/Boats
- Important Life Dates (First Child, Graduation, etc)
- Bank
- Favorite Places
- All aliases online
- Social Medias
- Volunteerism/ Activism
- Personas Online (Avatars)
- Files (.ppt, .xls, .xlsx, .doc, .docx, .csv, .pdf, .txt, .rtf, .odt, .ods, .odg, .odp, .wpd
Hypothetical Situation

(I had permission to show collect the information I collected and show you what I can...there is going to be a lot of black)
<div>(914)<span style="filter: blur(2px);">767</span></div>
<div>(401)<span style="filter: blur(2px);">766</span></div>
<div>(619)<span style="filter: blur(2px);">216</span></div>
<div>(914)<span style="filter: blur(2px);">846</span></div>
<a href="/people">
Business Profile

- Web site: www.[redacted].com
- Number of Employees: 20 to 49
- Annual Revenue: $5 to 10 Million
- Years in business: 10 or More Years
- Type of business: [redacted]
- SIC: [redacted]
- Square Footage: 10,000 to 49,999
- No. of PCs: 10 to 24
- Small Business: Yes

Executives

- [redacted]
- Manager
- President
- President

Business Credit Rating

95 / Excellent
Suggested Credit Capacity: $6,000

Company Expenses

- Accounting Expenses: $25,000 to $99,999
- Advertising Expenses: $5,000 to $14,999
- Business Expenses: $20,000 to $49,999
- Legal Expenses: $25,000 to $99,999
- Office Equipment Expenses: $10,000 to $24,999
- Rent Expenses: $25,000 to $99,999
- Technology Expenses: $25,000 to $99,999
- Telecom Expenses: $10,000 to $24,999
- Utilities Expenses: $20,000 to $49,999
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>NJ</td>
<td>07506</td>
<td>US</td>
<td>973-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NV</td>
<td>89431</td>
<td>US</td>
<td>775-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>12779</td>
<td>US</td>
<td>845-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11221</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11101</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>12962</td>
<td>US</td>
<td>518-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11357</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>13902</td>
<td>US</td>
<td>607-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11214</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>14304</td>
<td>US</td>
<td>716-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10701</td>
<td>US</td>
<td>914-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11726</td>
<td>US</td>
<td>631-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>142170306</td>
<td>US</td>
<td>716-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>14424</td>
<td>US</td>
<td>585-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>12054</td>
<td>US</td>
<td>518-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10550</td>
<td>US</td>
<td>914-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>14210</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11003</td>
<td>US</td>
<td>516-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11232</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>131661240</td>
<td>US</td>
<td>315-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>11747</td>
<td>US</td>
<td>631-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10553</td>
<td>US</td>
<td>914-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>14120</td>
<td>US</td>
<td>716-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>12801</td>
<td>US</td>
<td>518-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>13202</td>
<td>US</td>
<td>315-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10706</td>
<td>US</td>
<td>914-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10455</td>
<td>US</td>
<td>718-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>13790</td>
<td>US</td>
<td>607-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>10128</td>
<td>US</td>
<td>212-</td>
<td>NY</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NY</td>
<td>13202</td>
<td>US</td>
<td>315-</td>
<td>NY</td>
</tr>
</tbody>
</table>
Data + Information = Knowledge = POWER!

- Name
- Age
- Location
- Relatives
- Phone Numbers
- Position at Work
- Likes
- Possible Addresses
- Place of Work Address
- Files (List of suppliers)
- Network
- Other Employees

- #of Employees
- Business Line
- Photos
- Aliases
- Website
- Company Worth
- Estimated # of PCs
- Years in Business
- Annual Revenue
- Estimated Expenses
- And much, much more!
Digital Dossier Assignment

- Almost all of the students are able to find information about themselves, even those with the most common names.
- Those who cannot find information about themselves, usually try to get away with not doing the assignment. (I know this because then I search them).
- Almost all don’t reach the full amount of information available about them online. (I know this because I randomly select assignments for review and realize many miss a lot of information).
- Almost all of the students are terrified of what they find and how easy it is for them to find it. Most of them are unaware that the information exists.
Digital Dossier Assignment

• Some students find shocking things about themselves online. One of my students was unaware his criminal DUI from just a mere 4 months before the assignment was given out was available online.

• Most students reveal that the information they find about themselves online does indeed make them vulnerable. (Many surprised by addresses and phone numbers).

• After the assignment all students recognize the power of OSINT research and how they can use it to find information about themselves and others.
so, Bro... what do I do now?
How can I protect myself and others?

• Keep your systems updated....exploit Tuesday, patch Wednesday
• Implement a strong password policy
  • Make sure users have a strong password that changes regularly (password management system)
• Protect your privacy...
  • Limit the amount of personal information you share online
  • Do NOT post anything work related online... (sometimes even your position)
  • Be weary of giving your information to others
• Humans are the weakest link in any security policy...
  • Mandatory Staff Training
  • Bottom Up Approach not Top Down
    • Cybersecurity is everyone’s business
Comments/Questions?

Contact us at anastacia.webster@csusb.edu