OSINT: Common Tools and How to use them Safely

Siobhan Kelleher
Senior Security Analyst
Boston College
OSINT: Common Tools and How to use them Safely

Topics

• What is OSINT
• Using OSINT
• Tools and Resources
• Staying Safe
• Using Your Skills for Good
OSINT: Common Tools and How to use them Safely

What is OSINT?

“Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.”
What is OSINT?

- The Internet
- Media (e.g. television, radio, newspapers, magazines)
- Professional Publications (journals, conferences, studies)
- Photos
- Geospatial information (e.g. maps and commercial imagery products)
- ...and more
OSINT: Common Tools and How to use them Safely

How am I using OSINT?

- User Awareness Training
- Malicious email
- Missing People
- Domestic Abuse
This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

http://www.hisutton.com/OSINT_Landscape.html
OSINT: Common Tools and How to use them Safely

Tools & Resources

• Social Media
  • Tiktok, Twitter, Facebook, Snapchat, dating apps...

• Email

• Reverse Image Search

• Public Records
  • Address, arrest records, death certificates

• Other
OSINT: Common Tools and How to use them Safely

Tools and Resources

- Mind Mapping
- Hunchly
- Excel
- Trello
- Session Buddy
<table>
<thead>
<tr>
<th>What</th>
<th>Link</th>
<th>Artifact</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number</td>
<td><a href="https://www.theirnumber.com">www.theirnumber.com</a></td>
<td>8675309</td>
<td>found through this link,</td>
</tr>
<tr>
<td>Mother</td>
<td><a href="https://www.mothers">www.mothers</a></td>
<td>Janet Doe</td>
<td>facebook page is open lists other relatives found through facebook search</td>
</tr>
<tr>
<td>Artifacts Found</td>
<td>Under Investigation</td>
<td>Good Artifact</td>
<td>Bad Artifact</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Account</td>
<td>Second username</td>
<td>Images</td>
<td>potential account</td>
</tr>
<tr>
<td>Account</td>
<td>+ Add another card</td>
<td>+ Add another card</td>
<td>+ Add another card</td>
</tr>
<tr>
<td>Images</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Association</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OSINT: Common Tools and How to use them Safely

Tools and Resources

Maltego

https://medium.com/@raebaker/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc
Cybersecurity tip: To best protect your business you'll need both antivirus and anti-malware programmes. Antivirus software offers protection against classic ...
You visited this page on 8/10/20.
OSINT: Common Tools and How to use them Safely

Tools and Resources

- SpiderFoot
  - Free hobby edition- web based
  - Free open source downloadable

https://www.spiderfoot.net/
OSINT: Common Tools and How to use them Safely

Tools and Resources

Scylla Project

https://scylla.sh/

https://twitter.com/_hyp3ri0n
OSINT: Common Tools and How to use them Safely

Tools and Resources

• Reverse Image Search
  • Find other accounts

https://tineye.com/

https://images.google.com/
OSINT: Common Tools and How to use them Safely

Tools and Resources

• Social Media Search
  • Simple is sometimes better

OSINT: Common Tools and How to use them Safely

Staying Safe

• Why it's important!
  • Protect yourself
  • Isolate the target, protect the investigation
OSINT: Common Tools and How to use them Safely

Staying Safe

• Passive recon or “no touch”:
  • No interaction with target
  • Not invasive
  • No illegal hacking

• Active recon:
  • Logging into targets accounts
  • Contacting target/friends/family
OSINT: Common Tools and How to use them Safely

Staying Safe

• Use a VM (virtual machine)
  • Burn it when you are done
• VPN (virtual private network)
  • Proton
  • Brave
  • Nord
  • PrivateInternetAccess (PIA)

https://www.privacytools.io/
OSINT: Common Tools and How to use them Safely

Staying Safe

• Sock Puppet Accounts
  • Fake account used for recon
  • Never use your personal social media accounts for OSINT investigations
  • Insulate your personal information
OSINT: Common Tools and How to use them Safely

Staying Safe

- Sock Puppet Accounts
- Burner Phone
- Smart Proxy
- Wifi
- Fake Identity Generators

https://www.thispersondoesnotexist.com/

https://www.fakenamegenerator.com/
OSINT: Common Tools and How to use them Safely

Using Your Skills for Good

• TraceLabs
  • CTF- prizes, and glory!
  • Monthly collaborative cases

Image: https://www.tracelabs.org/resources/trace-labs-wallpapers/
OSINT: Common Tools and How to use them Safely

Summary

• If you can google you can do this
  • Getting started:
    • VM
    • VPN
    • Google
    • Notebook
    • Desire to help
  • Keep organized
Thank You

Siobhan Kelleher
siobhan.kelleher@bc.edu