Hidden Universes of Cybersecurity Awareness

Anonymizer.com
Privacy is your right.

FISSEA Conference 3/2018
Russ Haynal
Instructor & Speaker
Internet: Search, OSINT, Infrastructure, Cybersecurity Awareness
navigators.com
Give a person a Phish, 
you feed them for a day
Teach a person how to Phish, 
you feed them for a lifetime

Today’s session shows how to quickly find the best 
resources for any topic, using several very clever 
and efficient search techniques

All example searches – and links to some great 
search results are posted online:

http://navigators.com/fissea.html
• This session illustrates several clever search techniques and research methods

• Consult your organization’s policies to verify if these methods are approved for your type of Internet connections
Search Engines
( google.com, bing.com)

• Search engine’s robot clicks through Internet
• TEXT of web pages are cached and indexed
• Supports detailed keyword searches
• Learn the features & options of each search engine

You must envision the target page
“Use your imagination”
Advanced Search = Efficient Search!

**basic search**

**advanced search**

- Limit search to specific sites or domains
- `filetype:pdf` = detailed content from great web sites

- Bottom right of Google home page: Settings → Advanced Search
- Top right of Google search results: Settings → Advanced Search
- Also choose 100 results per page: Settings → Search Settings
### Search Examples

<table>
<thead>
<tr>
<th>Query</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>cybersecurity framework</td>
<td>51,000,000 - both words anywhere</td>
</tr>
<tr>
<td>“cybersecurity framework”</td>
<td>203,000 - words adjacent, correct order</td>
</tr>
<tr>
<td>“cybersecurity framework” filetype:pdf</td>
<td>126,000 - research papers / presentations</td>
</tr>
<tr>
<td>“cybersecurity framework” filetype:ppt</td>
<td>36 - Powerpoint presentations</td>
</tr>
<tr>
<td>“cybersecurity framework” site:slideshare.net</td>
<td>1,600 - presentations</td>
</tr>
<tr>
<td>“cybersecurity framework” site:nist.gov</td>
<td>4,750 – hits from just nist.gov</td>
</tr>
<tr>
<td>“cybersecurity framework” site:nist.gov filetype:pdf</td>
<td>1,310 – pdf’s hosted at nist.gov</td>
</tr>
<tr>
<td>“cybersecurity framework” site:edu filetype:pdf</td>
<td>19,000 – pdf’s hosted at U.S. universities</td>
</tr>
<tr>
<td>“cybersecurity framework” site:linkedin.com/in</td>
<td>7,430– linkedin profiles</td>
</tr>
<tr>
<td>site:linkedin.com/in cissp ts sci</td>
<td>20,200 – certified security professionals revealing they have Top Secret clearance</td>
</tr>
<tr>
<td>site:linkedin.com/in your_agency job-title eg. system administrator</td>
<td>= spear phishing targets at YOUR agency</td>
</tr>
</tbody>
</table>

- When using “site:” command, do **not** include “http://www”
Cautions about Social Media

- Confirm policies for viewing, joining, or interacting on social media.
- Understand each site’s different levels of interactions:
  - viewing, following, group member, connecting, friend, messaging.
- What information is shared to the other end user?
- What information is shared with 3rd party advertisers / data brokers?
- ALL interactions are known to the owner of the social media site.
  --> learn who owns the site.
- Who has “jurisdiction” over the site? (VK --> Russia, QQ --> China)
  - Linkedin example:
  - Different membership levels have various capabilities:
    - free ($0/month), premium, premium personal, premium career, sales navigator, recruiter lite, recruiter ($900/month)
    - “recruiter” has unlimited access to everyone’s full profiles, and leaves no “hits” on the people they view.

Free account = YOU are the “product” being sold!
Compare level of detail in these two Linkedin profiles

Reveals security defenses and procedures, and recipe for spear phishing

Reveals JPMorgan is a bank (this is posted by MANY JPMorgan employees)
Forums of people who know your topic

• Forum – discussion focused on a particular topic
• Many users can participate by posting messages
• Moderators may “police” comments that are considered off-topic
• Try searching for:
  • Your topic forum post replies = forum of users that discuss your topic
• Use search terms that would be used by people in that industry: acronyms, slang, jargon, etc

• “cybersecurity framework” forum post replies = 11,100
• specific publication numbers: “800 53” forum post replies
• name of a product/vendor and forum post replies
• etc
Surfing Upstream vs. Downstream

#1 Most researchers follow the links “downstream” from an interesting page

#2 Shows pages that link towards the target (=upstream) This is an Indication of the page’s “popularity” = who knows about target.com

#3 Shows pages that link to both target sites ... = “user pages” for that topic
Be Creative When Surfing Upstream
Example: Washington DC Tourist Sites

- Theatre links:
  - www.fordstheatre.org

- DC Tourism:
  - www.nasm.si.edu (air & space museum)
  - www.kennedy-center.org

- Museums / Educational:
  - www.spymuseum.org

- Any combination of these target pages will lead you to “DC Tourism” pages, but certain pairings may also lead you to subject-specific pages.
Surfing Upstream Details

- search format at google or bing
  - www.example.com
  - www.example.com/pageA.html
  + www.example1.com
  + www.example2.com

- search results
  - contain text: www.example.com
  - contain text of the specific page address
  - contain text of both example site addresses
  - This is a great way to discover “user pages”
    (e.g. Joe's guide to many example-sites)

- You need to decide which scenario makes more sense;
  Row #1 or Row #2
  e.g. who links to the home page of the entire site vs,
       who links to a specific webpage within the site

- A 3rd and 4th site can be added if they are popular enough

- Note: do not include “http://”

- Who links to: 2 anti-phishing vendors, 2 animation products, 2 security conferences, etc.
Web Analytics

alexa.com    similarweb.com
urlm.com    urlm.co.uk

Each of these tools offer a sampling of analytics for free:

- Popularity of a web site
- Audience demographics
- Search terms used to find the site
- Visitor engagement levels
- Traffic history
- Related sites = more sites

Enter a domain name (not search terms)
Your Homework Mission, Should You Decide To Accept It…

- Google settings -> 100 hits
- Use clever search techniques
- Find “people without a life” who have already done the research:
- They post PDFs and PPTs, participate in forums, share on linkedin, link to many resources

Contact Information
Russ Haynal  russ @ navigators.com  703-729-1757
www.linkedin.com/in/russhaynal

Note: If you send me an email, and it’s not from .gov or .mil, put “internet training” in the e-mail's subject