

# From OSINT to Phishing Campaign

A creepy online story as told  
by M4x

> 10000000

1000000

100000

10000

1000

100



[ 2020-08-26 | 18:30:01 | EDT | 127.0.0.1 ]

nobody@osint-server:~\$ nc -vklnp 1337

Ncat: Version 7.80 ( <https://nmap.org/ncat> )

Ncat: Listening on :::1337

Ncat: Listening on 0.0.0.0:1337

Ncat: Connection from 127.0.0.1.

Ncat: Connection from 127.0.0.1:53722.

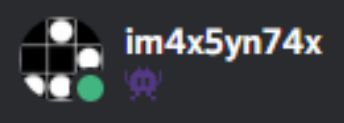
whoami

m4x



## TL;DR

- Security Consultant for Coalfire Systems
- Offensive Security and Social Engineer
- OSINT and Sleuthing Enthusiast
- Usually found on the internet...
- <https://github.com/im4x5yn74x>
- [im4x5yn74x@protonmail.com](mailto:im4x5yn74x@protonmail.com)
- [@im4x5yn74x#9967](#)



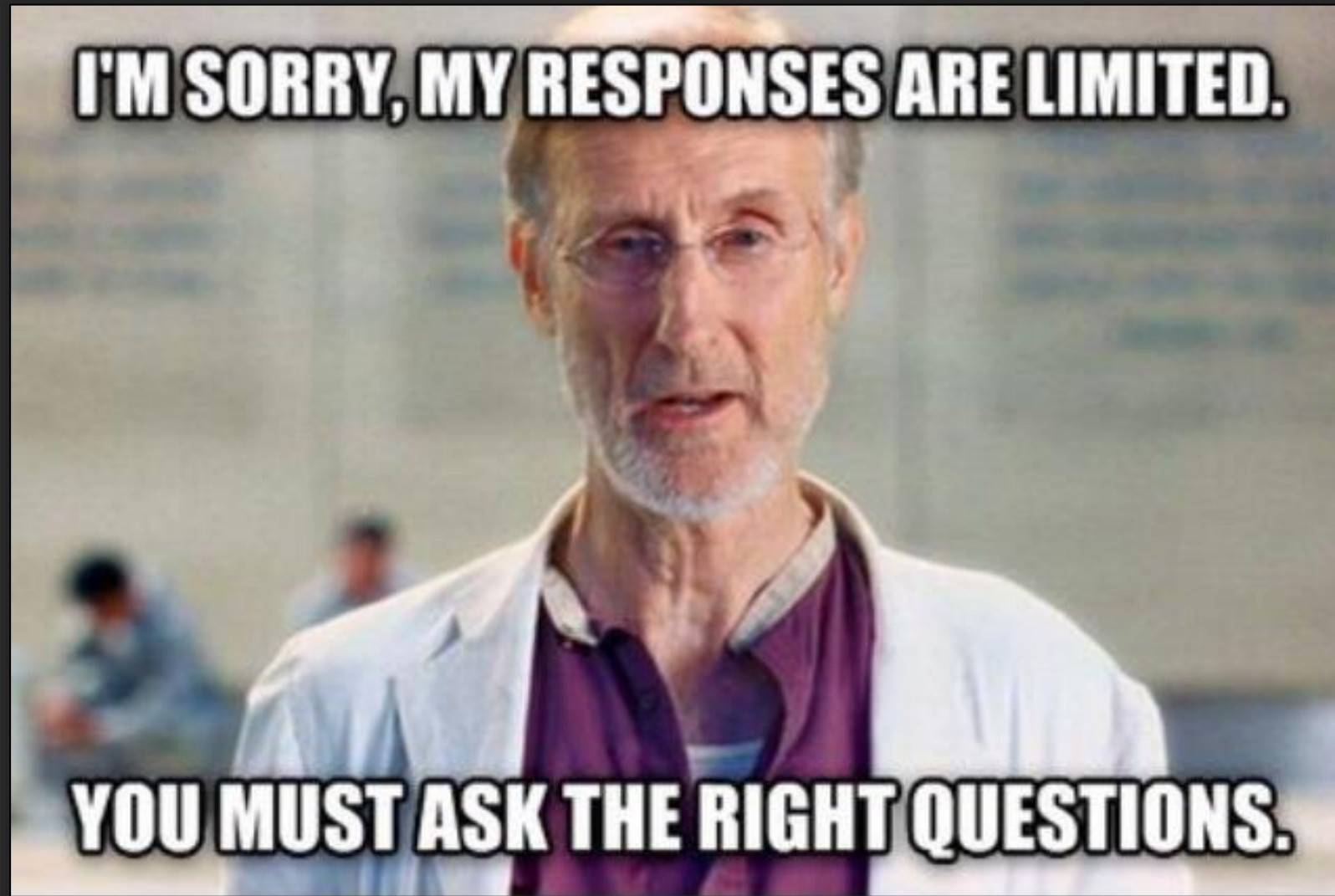
# What is OSINT?

- Open-Source INTelligence
  - The reconnaissance of publicly available information regarding an organization or individual(s)
  - The Internet (Google, Bing, Yahoo, Facebook, LinkedIn, Twitter, ect...)
  - Traditional mass media (television, radio, newspapers, magazines)
  - Specialized journals, whitepapers, conferences, and think tank studies (Thanks CIA!)
  - Photos (Pinterest, Instagram, Google Images)
  - Geospatial information (maps, blueprints, commercial imagery products)

# Who uses OSINT?

- Law Enforcement
  - FBI, NSA, CIA (other alphabet agencies not mentioned here)
- Private Investigators
  - Detectives, Lawyers, Bounty Hunters, and Bail bondsmen
- Amateur Internet Sleuths
  - You and me! 😊
- Stalkers, creeps and perverts
  - Ex-husbands/wives/boyfriends/girlfriends with a grudge or vendetta
  - Not you or me (hopefully)

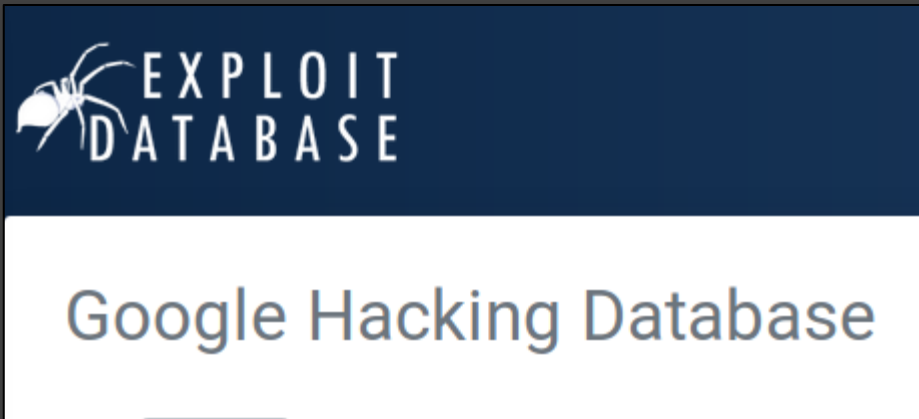
So M4x, How does one “OSINT”?



The correct question is...

## Where does one “OSINT”?

- Google
  - First name and last name
  - Company name
  - Location
  - Email address
  - Phone number (a little tricky)
  - Dorks!



<https://www.exploit-db.com/google-hacking-database>



# What does a Google Dork look like?

phonebook:"+1 [REDACTED]"

[All](#) [Images](#) [News](#) [Shopping](#)

1 result (0.28 seconds)

intext @gmail.com password filetype.txt

[All](#) [News](#) [Images](#) [Videos](#) [Shopping](#)

About 69,800 results (0.67 seconds)

?intitle:index.of? pdf

[All](#) [News](#) [Images](#) [Videos](#) [Maps](#)

About 2,700,000 results (0.50 seconds)

site:"pastebin.com" netflix

[All](#) [News](#) [Books](#) [Images](#)

About 6,090 results (0.29 seconds)

intitle:"index of"

[All](#) [Images](#) [Books](#) [Videos](#) [News](#)

About 28,600,000 results (0.44 seconds)

site:"facebook.com"

[All](#) [Images](#) [News](#) [Shopping](#)

About 2,900,000 results (0.36 seconds)

A word of caution...

# Google doesn't like you! (it only likes your data. SSHHH! It's a secret!)

- Are you a robot!?
  - Seriously, are you tho'?

Please show you're not a robot

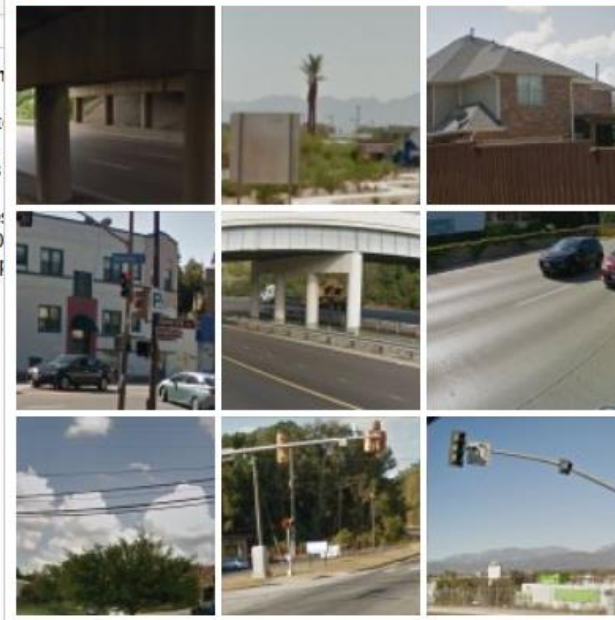


I'm not a robot



reCAPTCHA  
Privacy - Terms

Select all images with  
**crosswalks**  
Click verify once there are none left.



⌂ About this challenge Our system uses a network of requests to verify you are not a robot. IP address: Time: 20 URL: http

⌂ ⌂ ⌂

VERIFY

# Tools and Frameworks

## More well-known

- Maltego - <https://www.maltego.com/>
- Shodan - <https://www.shodan.io/>
- theHarvester - <https://github.com/laramies/theHarvester>
- Metagoofil - <https://github.com/laramies/metagoofil>
- TinEye - (Reverse Image search) - <https://tineye.com/>

## Less well-known

- TruePeopleSearch (Doesn't like VPNs ☹️) - <https://www.truepeoplesearch.com/>
- Pipl - <https://pipl.com/>
- PimEyes - (SUPER creepy but very awesome!) - <https://pimeyes.com/en/>
- Skiptracer - (Open-source, like theHarvester) - <https://github.com/xillwillx/skiptracer>
- LittleBrother - (Requires French or Google Translate. 😊) - <https://github.com/lulz3xploit/LittleBrother>

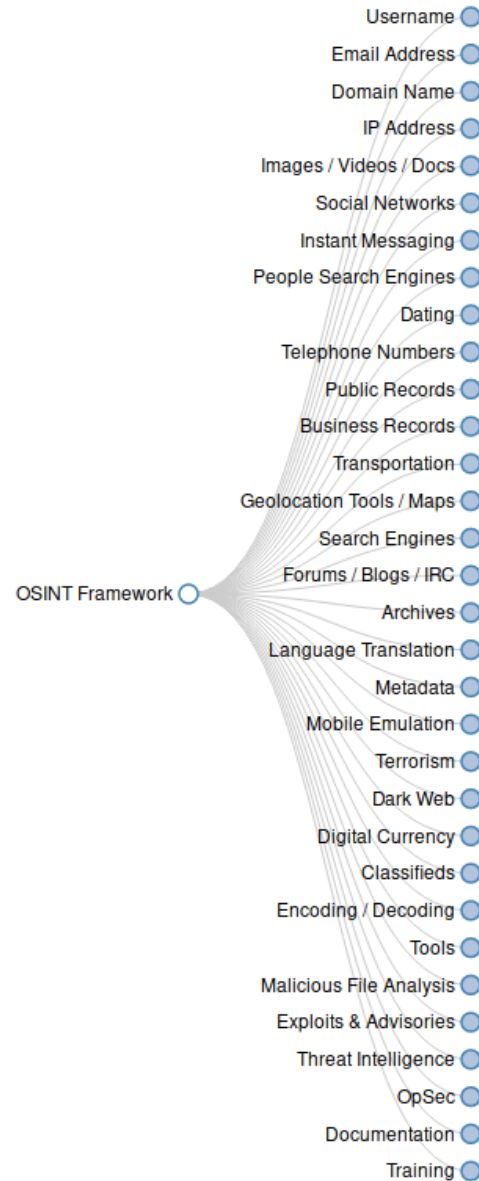


# My all-time favorite one-stop-shop... the OSINT Framework

<https://osintframework.com/>

## OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally  
(D) - Google Dork, for more information: [Google Hacking](#)  
(R) - Requires registration  
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



Now, with your newly acquired OSINT skills, there's only one thing left to discuss...

Phishing!



# You might be asking yourself, “What type of people go Phishing”?

The Answer is: **Terrible People!**

...and here's why you should!

- Phishing is an “art”
- Good phishing takes good research (and a little luck but mostly research)
- You can learn a lot about yourself from a great phishing email.

HOLY COW!

Bob, if you haven't already, you gotta see this website! It's a little less “safe-for-work” so you'll want to visit it when you get home.

<https://naughtypandasinbikinis.com/register>

You won't regret it! I can't stop laughing!!! 😂

Tim

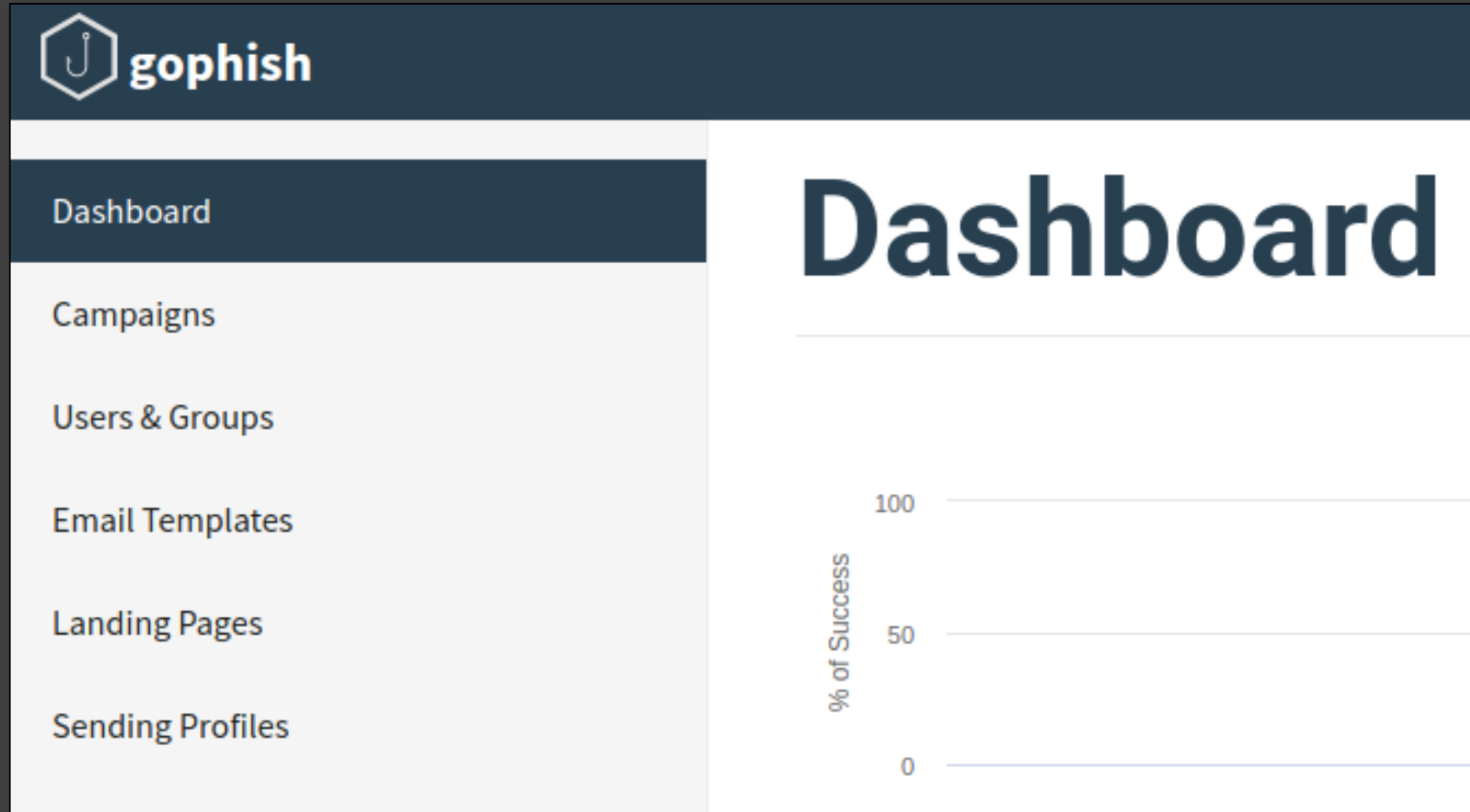
# Tools and Frameworks

- Prerequisites
  - Stand up a basic LAMP stack server on your favorite hosting provider
  - Register your “Phishing” domain at your favorite registrar
  - Use Certbot to generate a LetsEncrypt SSL certificate (Everyone trusts SSL, don’t you?)
  - Don’t forget to point your DNS to your webserver
- Manual Approach
  - Write your own web application to capture user submitted data
  - Scrape/clone an existing website
  - Create a log file/database etc. to house all captured information
- Automated Approach
  - Opensource frameworks
    - Modlishka - <https://github.com/drk1wi/Modlishka>
    - GoPhish - <https://getgophish.com/>



# GoPhish

- Campaigns
- Users & Groups
- Email Templates
- Landing Pages
- Sending Profiles



# Email To Bob Template

- Subject
- Body
- Just like a regular email

## New Template

Name:

Email To Bob

 Import Email

Subject:

Check this out!

Text

HTML

HOLY COW!

Bob, if you haven't already, you gotta see this website! It's a little less "safe-for-work" so you'll want to visit it when you get home.

<https://naughtypandasinbikinis.com/register>

You won't regret it! I can't stop laughing!!! 😂

Tim

☒ Add Tracking Image



## But wait... who's Bob?

- How do we know Bob?
- How does Bob know us?
- How do we even know Bob likes Naughty Pandas in Bikinis?

Answer: OSINT

# STORY



# TIME

## Prelude:

- Based on an actual Phishing Campaign conducted by yours truly
- The names, events, and corporation information have been changed for obvious reasons.
- It's not as bad as it sounds.
- Disclaimers are important.

Alrighty then; on with the story...

Hey team,

In our ongoing commitment to enriching our employee's lives during the COVID-19 pandemic, we are extending our gratitude with a \$50 Visa Gift Card! We may be on quarantine and unable to visit our local watering holes but we can still give you the ability to bring the watering hole to you!

Login to our Internal Rewards Portal to claim your reward for being awesome! [https://\[redacted\]/internalrewards](https://[redacted]/internalrewards)

Stay safe everybody and Cheers!

### Internal Rewards Portal

Email

Password

LOG IN



## Takeaways:

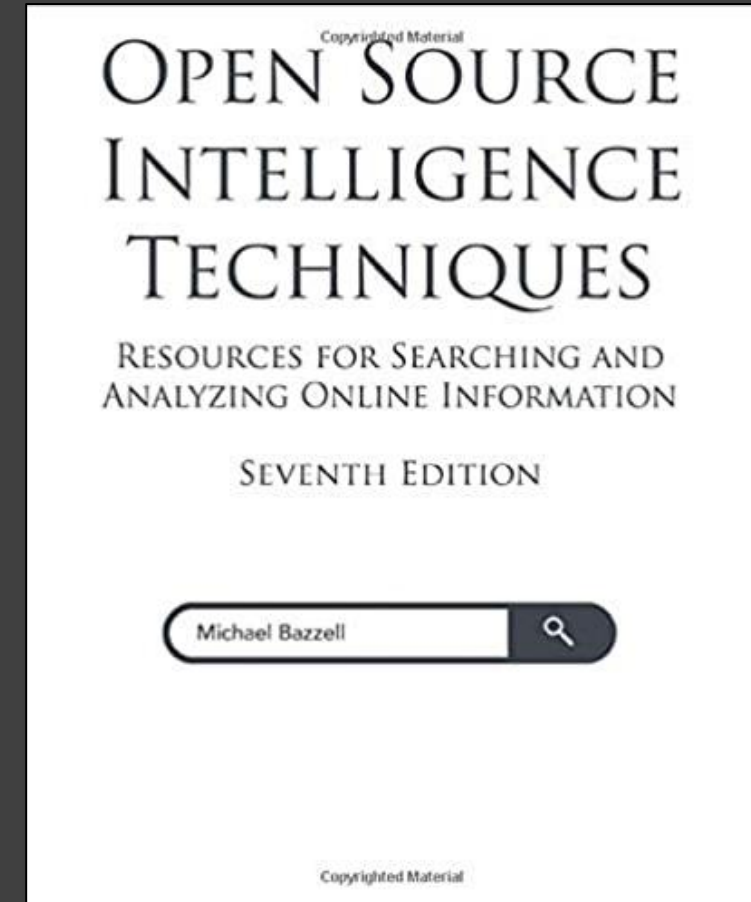
- Be mindful of what your organization shares online.
- Consider how even the simplest information can be used against yourself or the organization.
- What's your internet presence? Can you trace your digital footprints?
- What OSINT could an attacker use against you?
- What type of phish would you fall for?
- Did you click on the link?



# Shoutouts!!! What-what!!

- Q1234567890 – promoting this talk
- Wife – putting up with my late-night research and tech banter first thing in the morning
- Cheeseburgers – always being awesome
- Michael Bazzell and his work on <https://inteltechniques.com/>

BUY HIS BOOK!





# Thanks Alpharetta Pentest!

## Questions?

Find me on Discord  
@im4x5yn74x#9967

