Raytheon

Exploiting Your Digital Footprint

Addy Moran & Vidya Murthy

Tuesday, March 3, 2020

Disclaimer

All information in this presentation is for educational purposes only. Neither Raytheon, nor the presenters suggest or condone any of the methods mentioned in this presentation. Our emphasis is on security awareness and being able to defend from multi-faceted attacks. Raytheon accepts no liability, express or implied, in any matter related to this presentation.

About Us

Vidya Murthy

Raytheon Intern

Graduate Student at Carnegie Mellon University, Information Security

Fun Fact: This hacker's been hacked

Addy Moran

Raytheon Employee for 3+ years

Colorado State University, Bachelor's in Comp Sci

Certified Ethical Hacker

Fun Fact: This hacker's been scammed

What is a Digital Footprint?

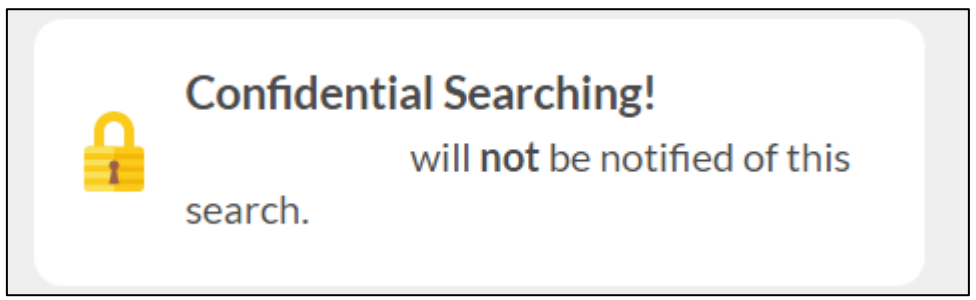
"A digital footprint is a trail of data you create while using the Internet. It includes the websites you visit, emails you send, and information you submit to online services."

Source: https://techterms.com/definition/digital_footprint

Pixabay/geralt

Example Sources of a Digital Footprint

- LinkedIn
- Facebook
- Voting Records
- Court Records
- Twitter
- Dating Apps
- Satellite Images
- Google Maps
- Venmo
- Criminal Records (for a fee)



Black Box Test

Raytheon

Goal: Compromise target's accounts

Motivation: Personal, financial, reputational

Pixabay/TheDigitalArtist

Data Gathering

Raytheon

addy moran

All Images Videos News Maps More Settings Tools

About 1,700,000 results (0.52 seconds)

www.linkedin.com › addy-moran-7b7875116

Addy Moran - Cyber Threat Hunter - Raytheon | LinkedIn

Addy Moran - Cyber Threat Hunter - Raytheon | LinkedIn. Join nowSign in. **Addy Moran**.

addymmoran.github.io

Addy Moran

Quick Facts. My name is **Addy Moran**. I have my bachelor's in Computer Science. I'm not your typical software engineer. I'm a problem solver. I want to make a ...

www.facebook.com › public › Addy-Moran

Addy Moran Profiles | Facebook

View the profiles of people named **Addy Moran**. Join Facebook to connect with **Addy Moran** and others you may know. Facebook gives people the power to ...

www.facebook.com › addy.moran.5

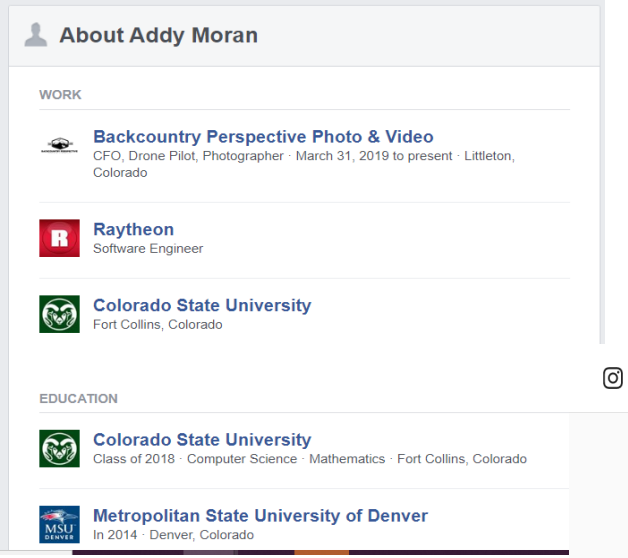
Addy Moran | Facebook

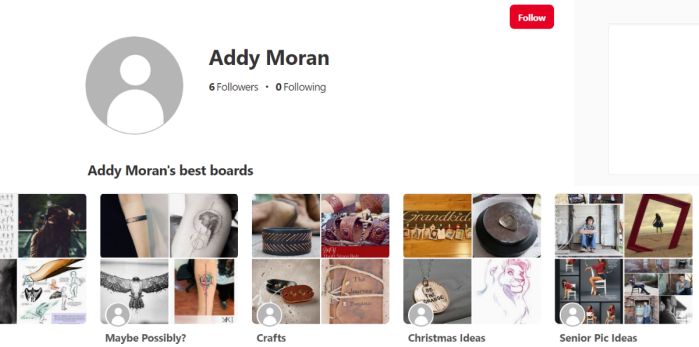
Addy Moran is on Facebook. Join Facebook to connect with **Addy Moran** and others you may know. Facebook gives people the power to share and makes the ...

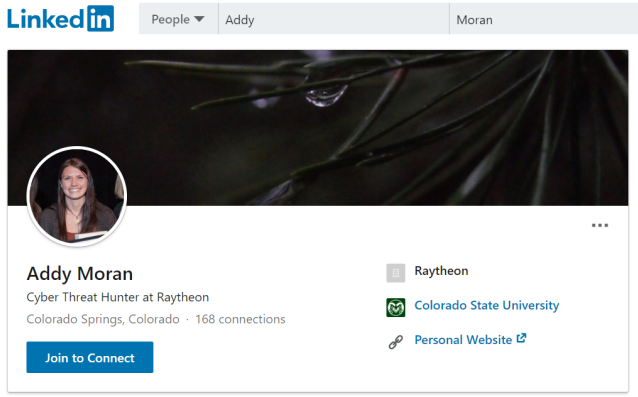
www.instagram.com › aboutaddy

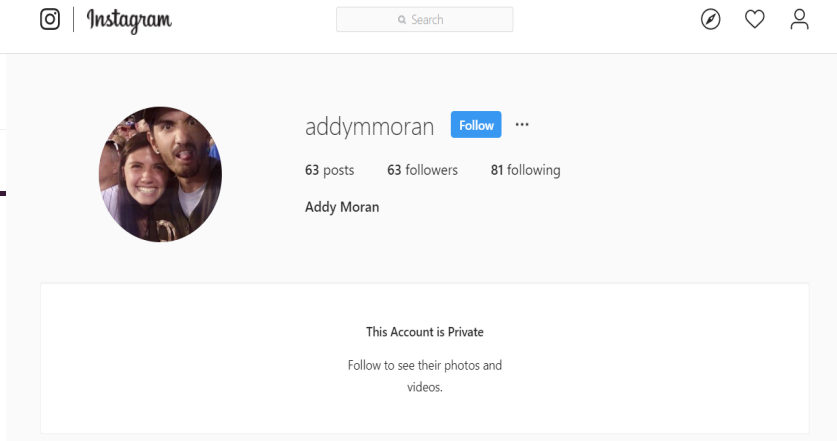
Addy Moran (@aboutaddy) • Instagram photos and videos

111 Followers, 100 Following, 99 Posts - See Instagram photos and videos from **Addy Moran** (@aboutaddy)



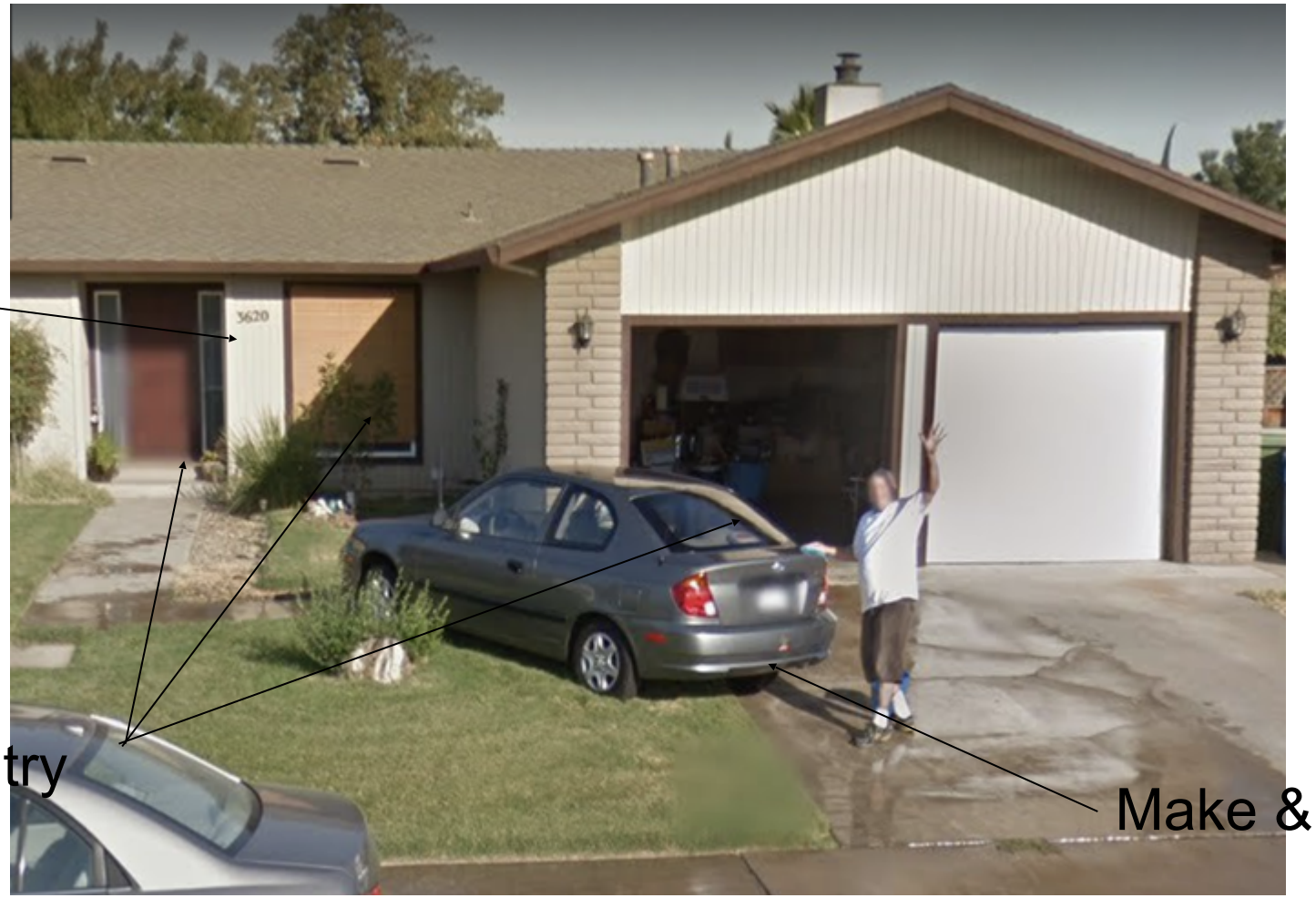




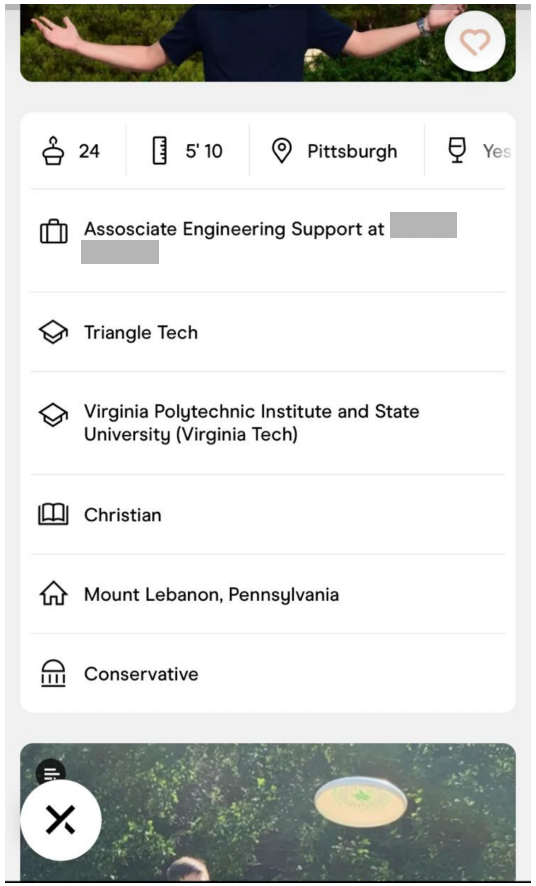


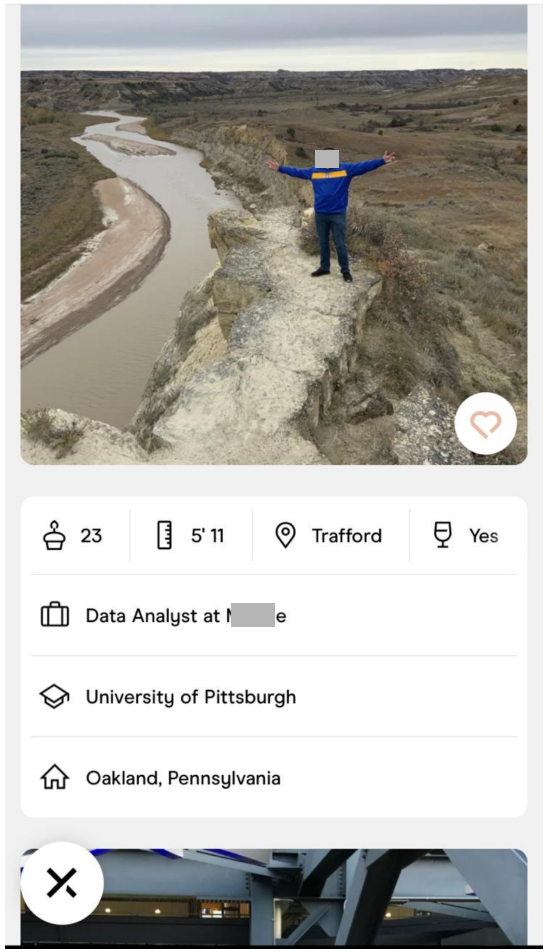
Data Gathering

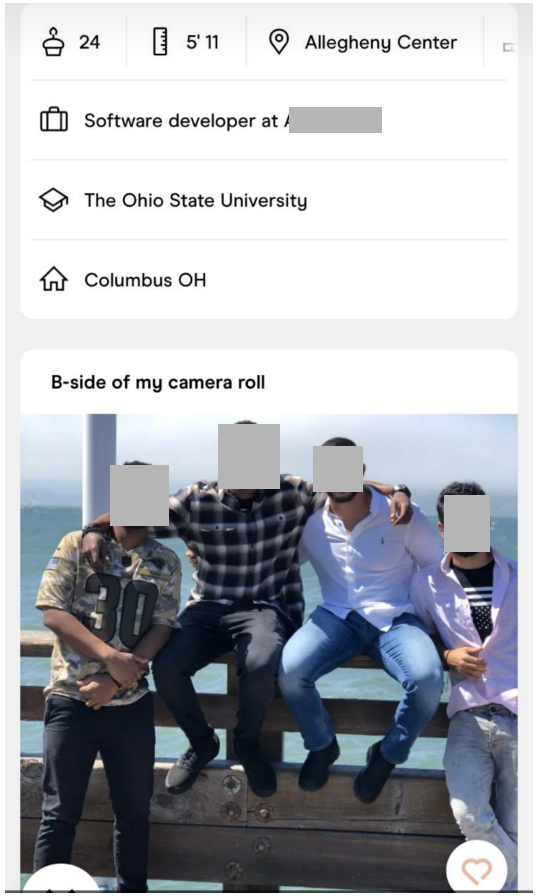
Raytheon



Data Gathering

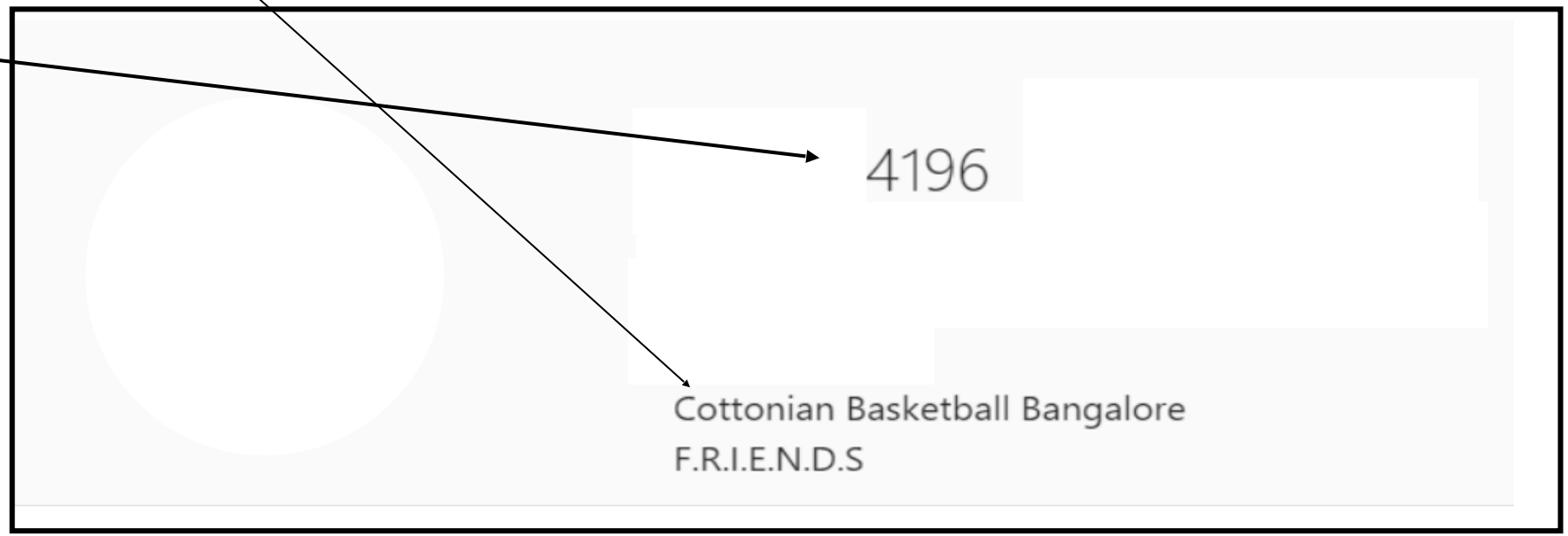






Data Gathering

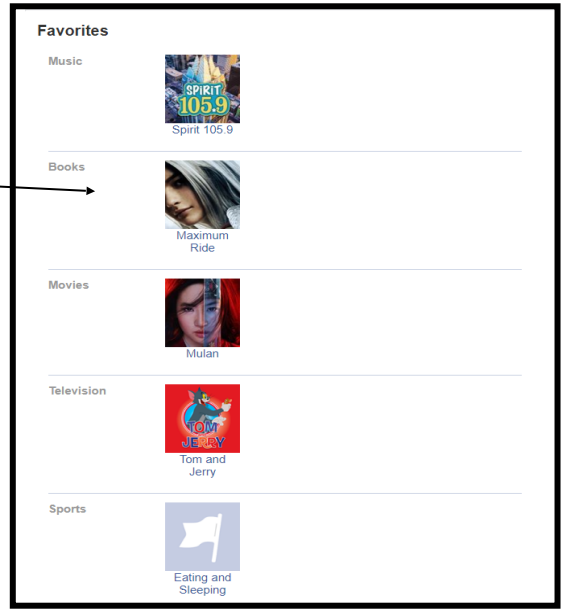
- Things of interest
- Place of residence
- Place of birth
- Birthdays

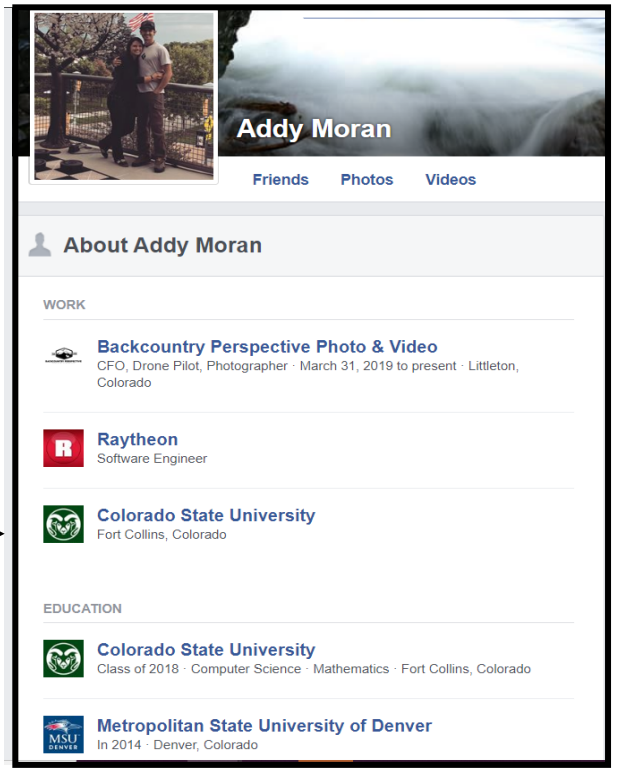


Option 1: Reset Password Using Security Questions

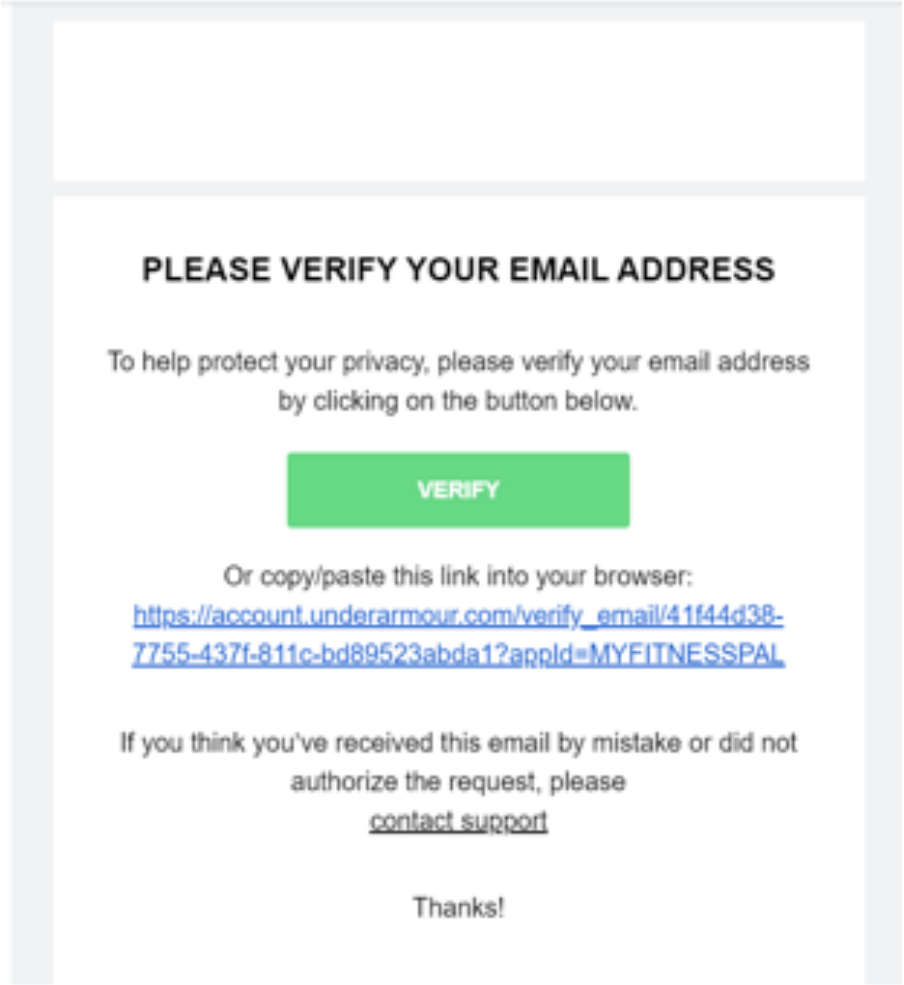
- What is your favorite book?
- What is the name of the road you grew up on?
- What is your mother's maiden name?
- What is your favorite food?
- What city were you born in?
- What was the first company that you worked for?
- Where did you go to college?
- What was the name of your first/current/ favorite pet?
- Where did you meet your spouse?
- Where is your favorite place to vacation?

From StumbleForward (2012)





Option 2: Spear Phishing for Account Information



PLEASE VERIFY YOUR EMAIL ADDRESS

To help protect your privacy, please verify your email address by clicking on the button below.

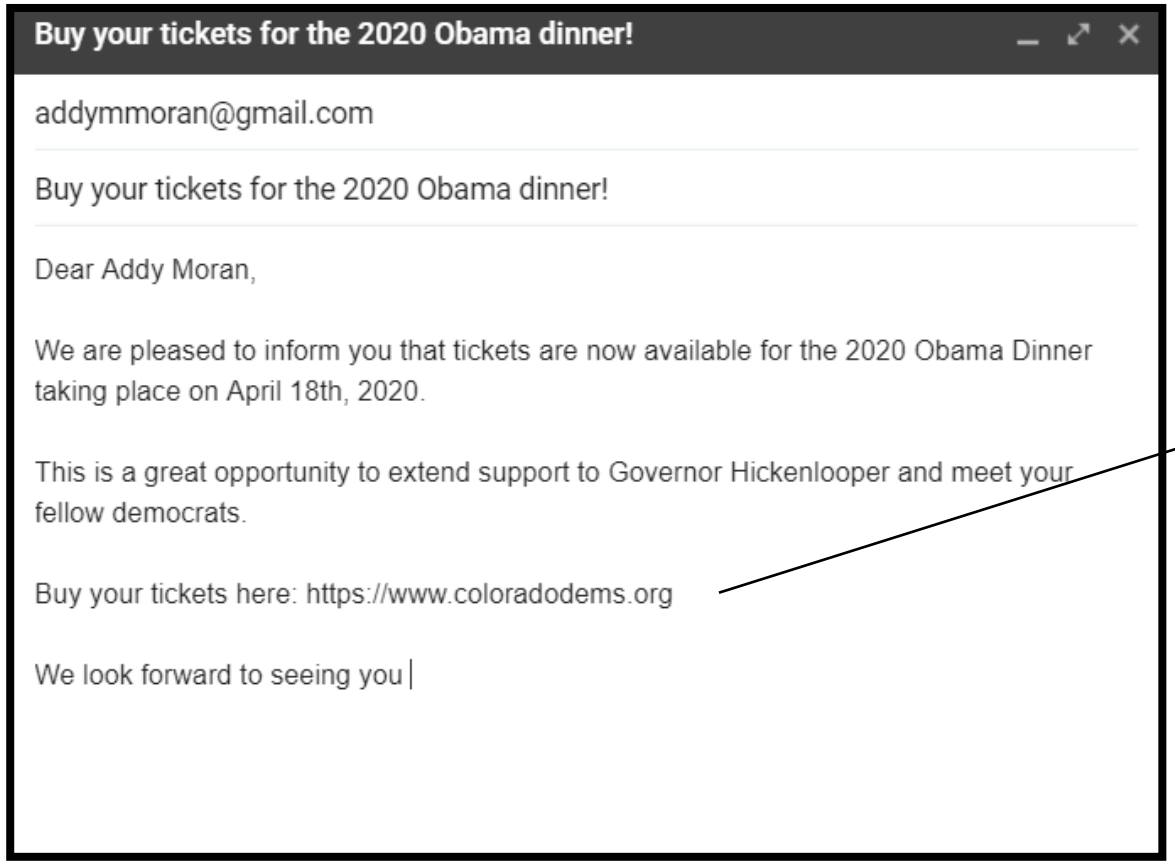
VERIFY

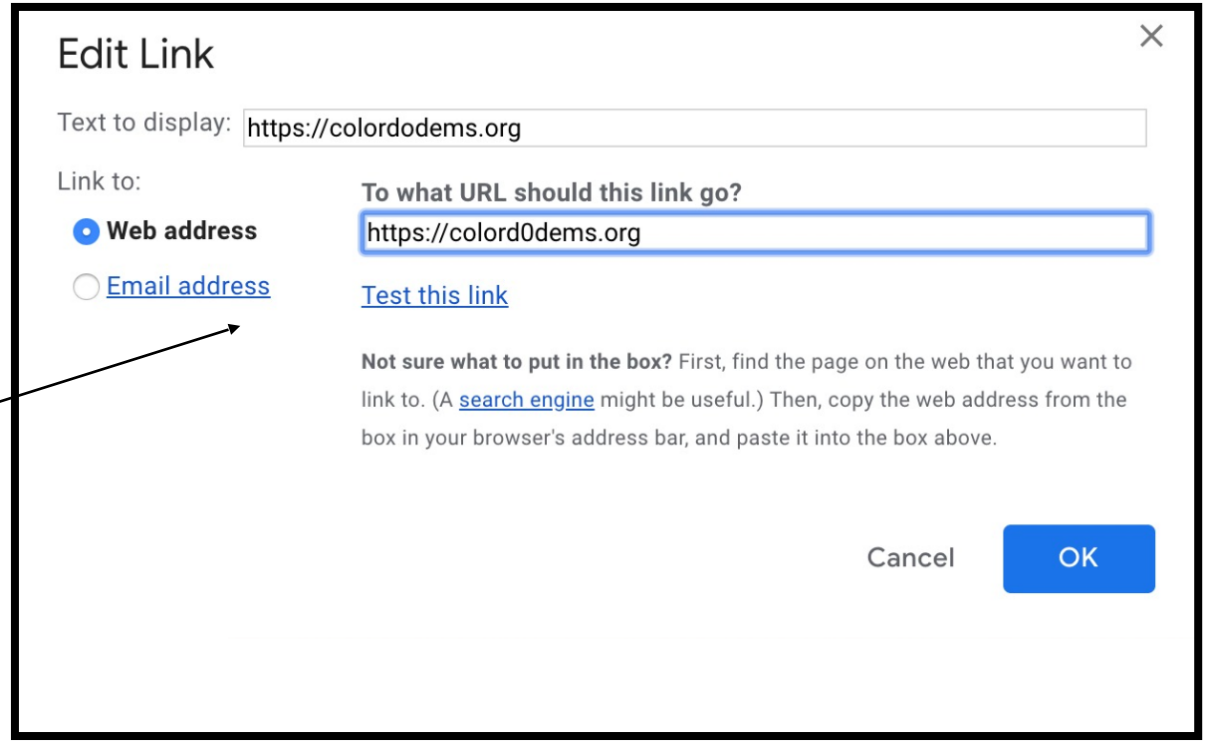
Or copy/paste this link into your browser:
https://account.underarmour.com/verify_email/41f44d38-7755-437f-811c-bd89523abda1?appId=MYFITNESSPAL

If you think you've received this email by mistake or did not authorize the request, please contact support

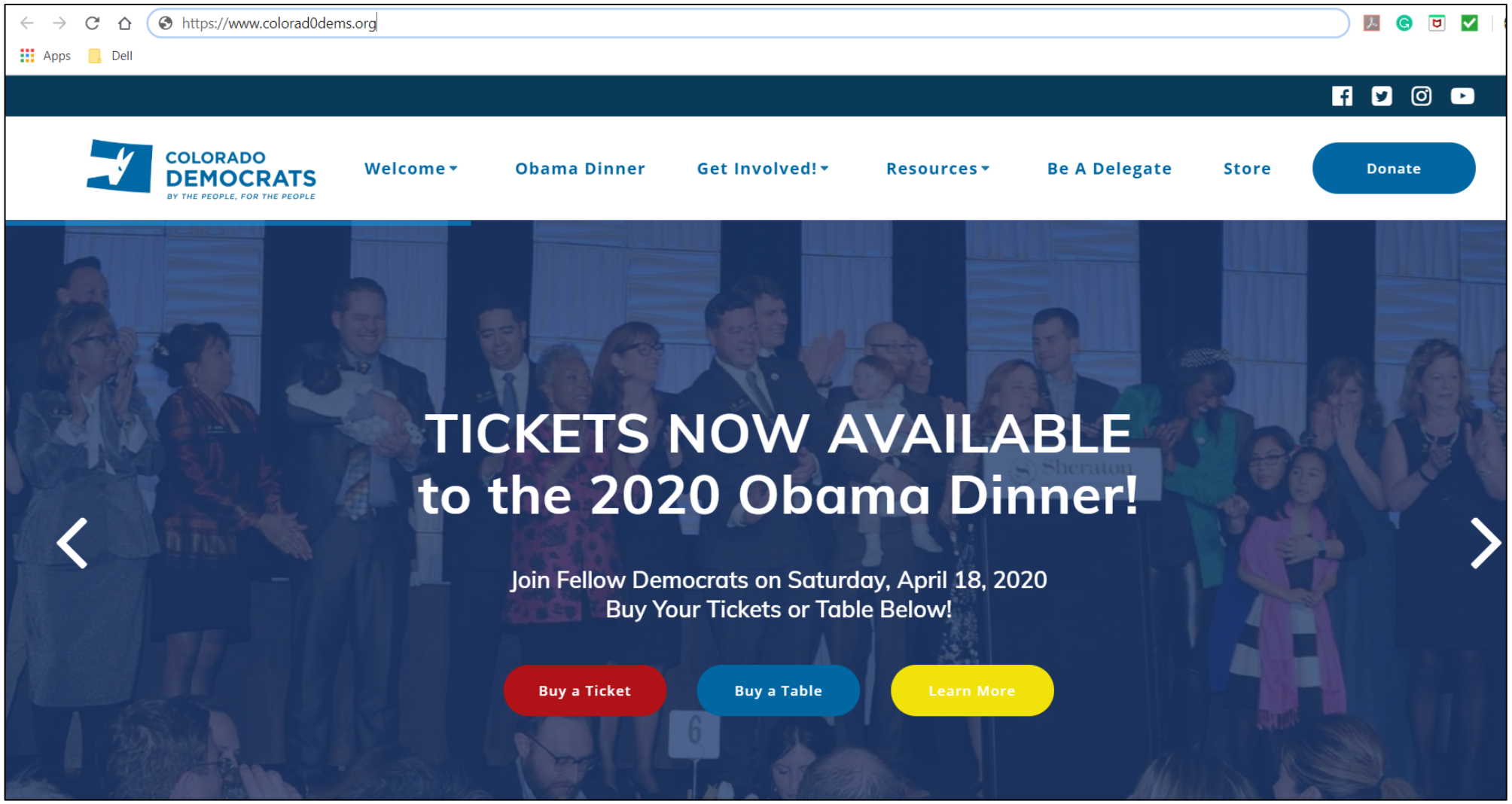
Thanks!

Option 3: Spear Phishing for Monetary Gains

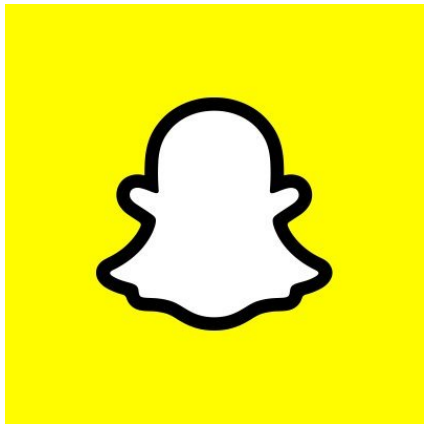




Option 3: Spear Phishing for Monetary Gains



Ammunition for an Insider Threat



venmo

myspace®
a place for friends

LinkedIn

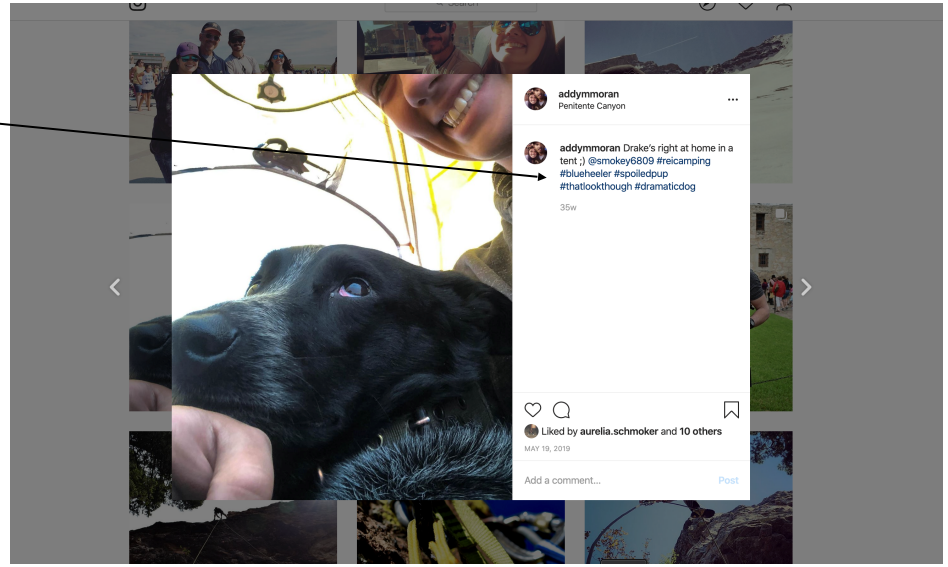
Exploiting “Being Friends” on Social Media

Raytheon

Top 10 Security Questions:

- What is your favorite book?
- What is the name of the road you grew up on?
- What is your mother’s maiden name?
- What was the name of your first/current/ favorite pet?
- What was the first company that you worked for?
- Where did you meet your spouse?
- Where did you go to high school/college?
- What is your favorite food?
- What city were you born in?
- Where is your favorite place to vacation?

goodreads



From StumbleForward (2012)

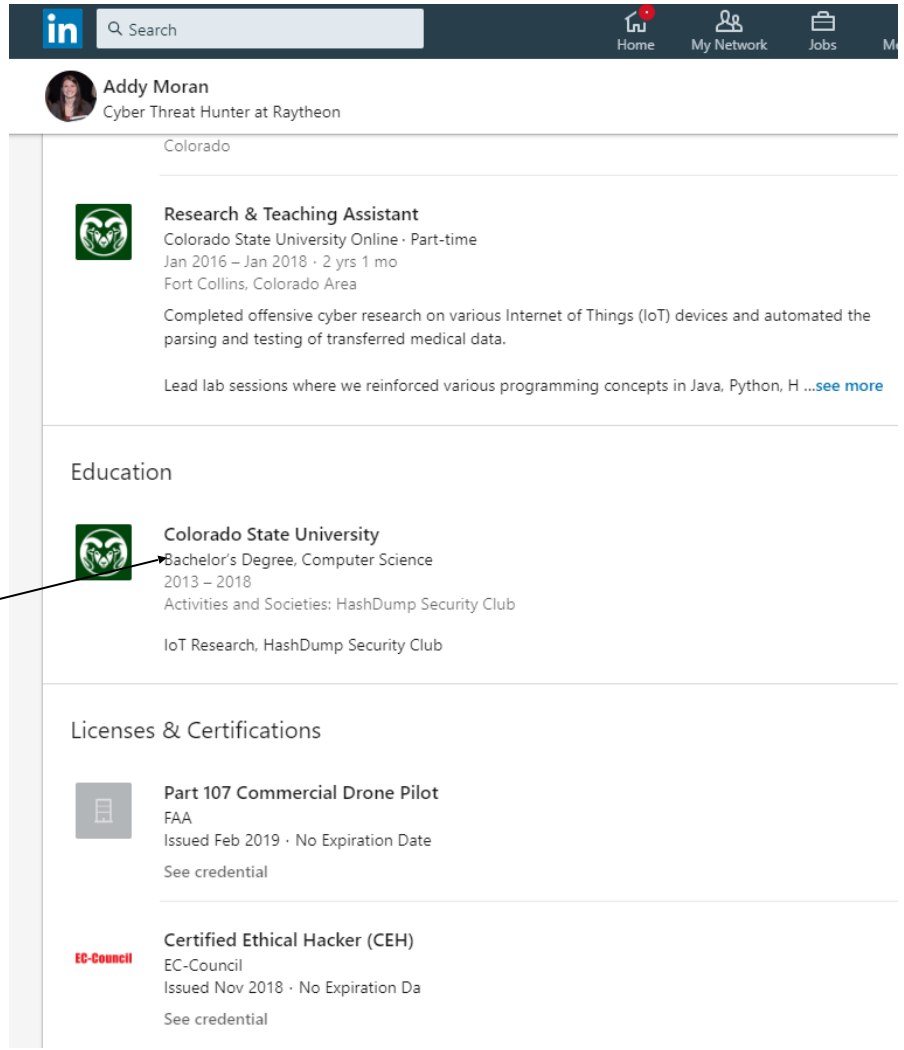
Exploiting “Being Friends” on Social Media

Raytheon

Top 10 Security Questions:

- What is your favorite book?
- What is the name of the road you grew up on?
- What is your mother’s maiden name?
- What was the name of your first/current/ favorite pet?
- What was the first company that you worked for?
- Where did you meet your spouse?
- Where did you go to high school/college?
- What is your favorite food?
- What city were you born in?
- Where is your favorite place to vacation?

From StumbleForward (2012)

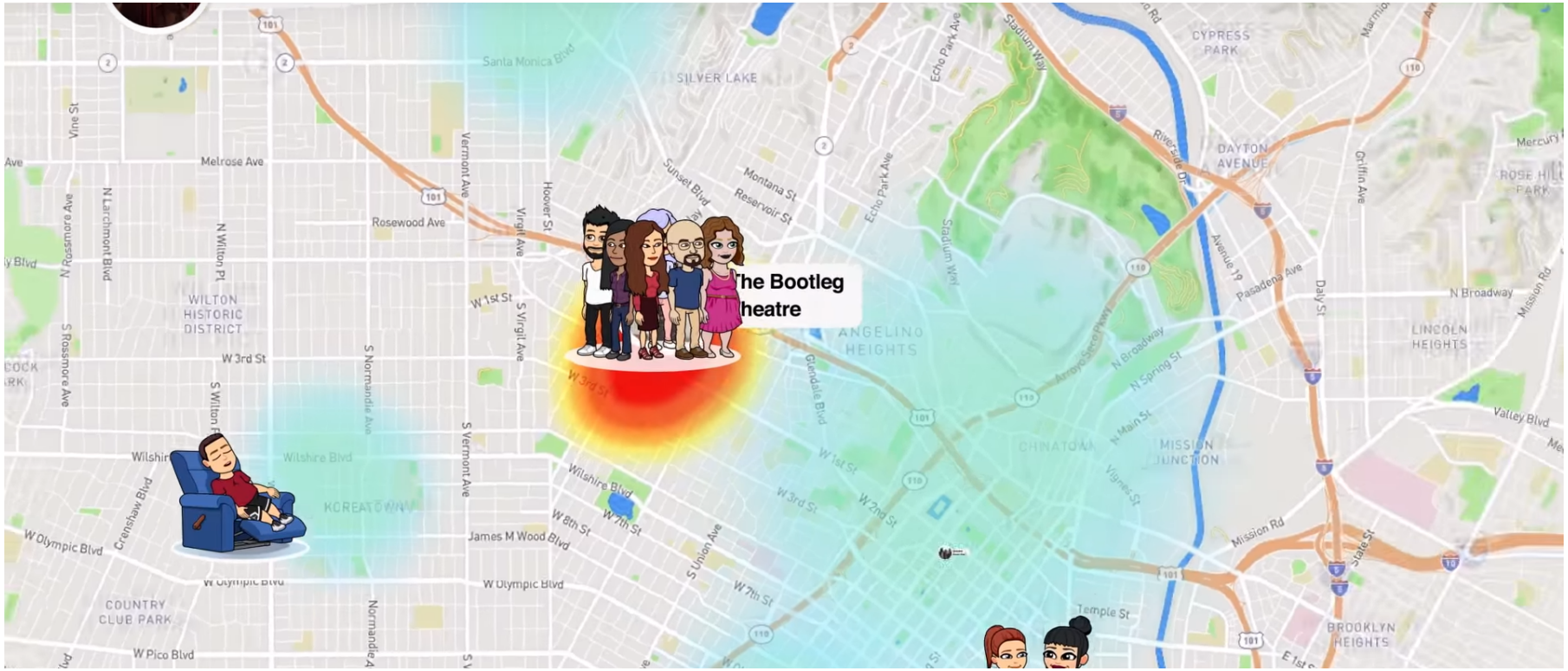


Unconventional Sources of Information

Roommates

Favorite Sports Teams

Unconventional Sources of Information



Snapchat Maps

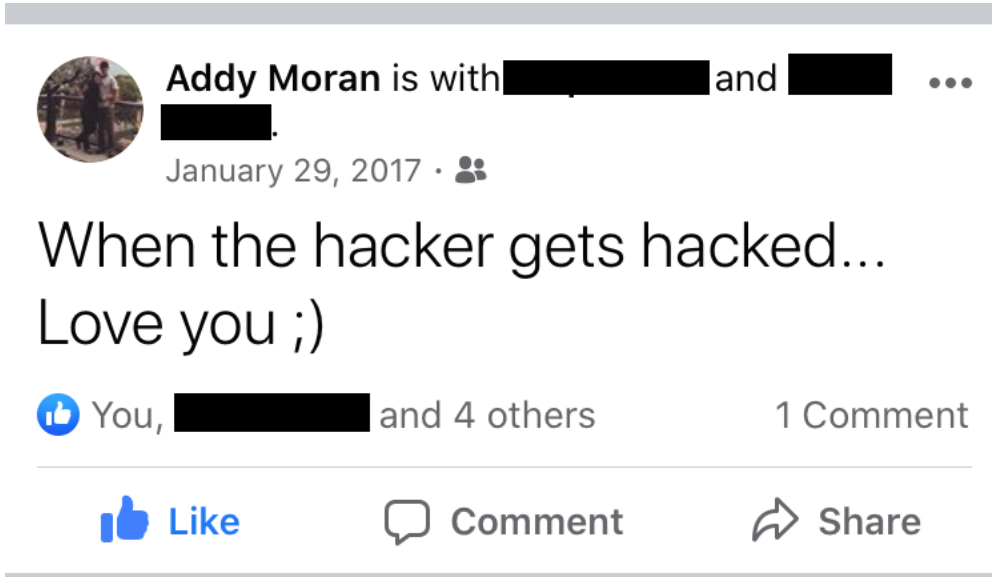
Unconventional Sources of Information

```
GPS Horizontal Positioning Error: 50 m
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2017:07:07 13:22:32
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ca1a9582257f104d389913d5d1ea1582
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2017
Media White Point               : 0.95045 1 1.08905
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extract)
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0.99048 -0.01706 -0.00923 0.01508 0.75168
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extract)
HEVC Configuration Version      : 1
General Profile Space           : Conforming
General Tier Flag               : Main Tier
General Profile IDC             : Main Still Picture Profile
Gen Profile Compatibility Flags : Main Still Picture, Main 10, Main
Constraint Indicator Flags      : 176 0 0 0 0 0
General Level IDC               : 90 (level 3.0)
Min Spatial Segmentation IDC    : 0
Parallelism Type                : 0
Chroma Format                   : 4:2:0
Bit Depth Luma                  : 8
Bit Depth Chroma                : 8
Average Frame Rate              : 0
Constant Frame Rate             : Unknown
Num Temporal Layers             : 1
Temporal ID Nested              : No
Image Width                     : 4032
Image Height                    : 3024
Image Spatial Extent            : 4032x3024
Rotation                        : 270
Image Pixel Depth               : 8 8 8
Media Data Size                 : 809363
Media Data Offset               : 3428
Run Time Since Power Up         : 5 days 9:33:34
Aperture                        : 1.8
Image Size                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 19.0
Shutter Speed                   : 1/10
Create Date                     : 2020:01:20 07:11:44.965-07:00
Date/Time Original              : 2020:01:20 07:11:44.965-07:00
Modify Date                     : 2020:01:20 07:11:44-07:00
GPS Altitude                    :  m Above Sea Level
GPS Latitude                    :  deg 0'  " N
GPS Longitude                   :  deg 48'  " W
Circle Of Confusion             : 0.002 mm
Field Of View                   : 26.6 deg
Focal Length                    : 4.0 mm (35 mm equivalent: 76.0 mm)
GPS Position                    :  deg 0'  " N,  deg  '  " W
Hyperfocal Distance             : 5.61 m
Light Value                     : 5.0
→  tools
```

EXIF Data

Exploiting the Access of an Insider Threat

Exploiting the Access of an Insider Threat



Company/Organization Perspective

Raytheon

- In today's society, organizations advertise and conduct much of their business online.

- At a minimum, a company has:
  - at least 1 domain registered to the company
  - at least 1 email used for the company
  - at least 1 server/computer connected to company assets

In order to advertise and grow as a company, a digital footprint is necessary

Domain Attacks

Raytheon

Real Company: AthenaConsulting.io

AthenaConsultng.io
Typosquatting

AthenaConsulting.tech
Domain Squatting

AthenaConsulting.io
IDN Homograph Attacks

Potential Attacks

- Sharing of inaccurate information
- Distribution of malware/ malicious code
- Exploitation of user credentials

By owning a domain similar to a real and trusted company's, an attacker can destroy a company's reputation

Hashtags

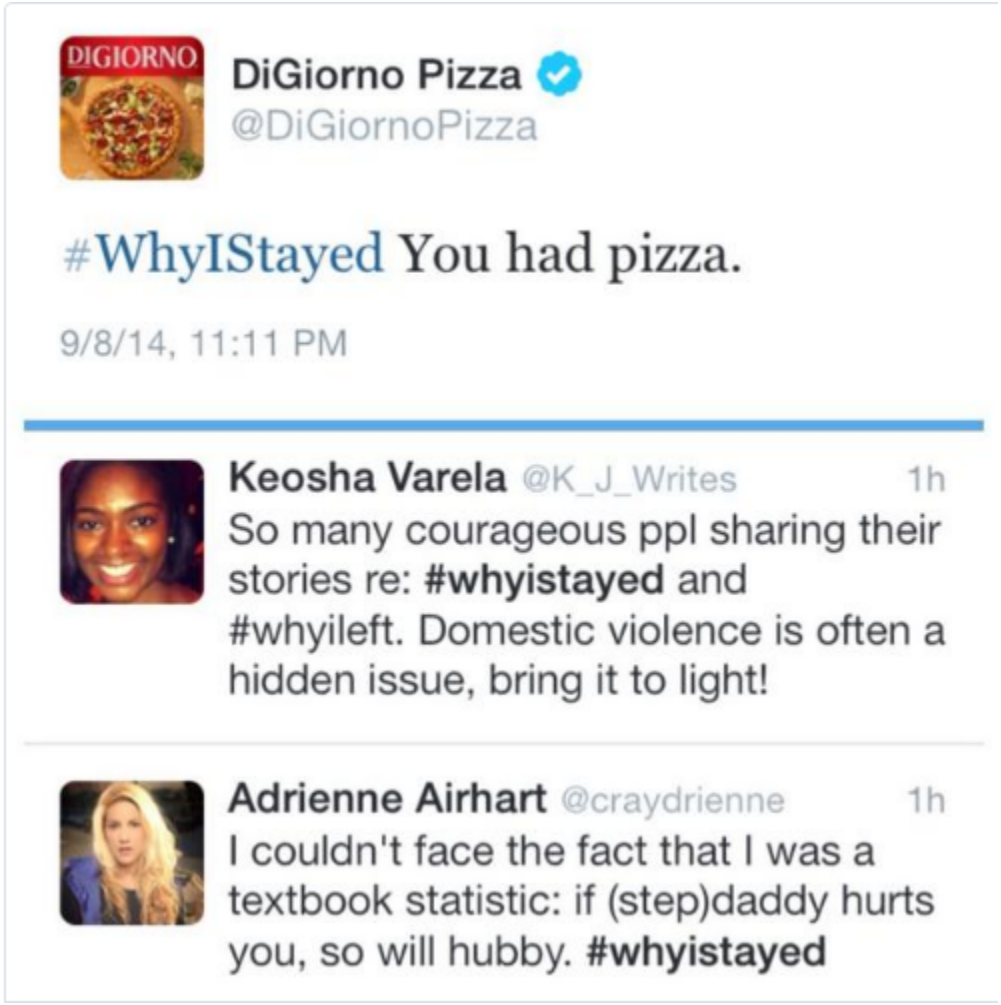
- Hashtag hijacking: “when a hashtag that a brand sets up to generate positive PR, is hijacked by detractors. Instead of being used for positive sentiment, it is used for attacks on the business, or in a sarcastic or snarky way.” (Campbell, 2019)

and 100's more...

https://www.felberpr.com/blog/the-danger-of-hashtag-hijacking-and-how-to-prevent-it/

Hashtags

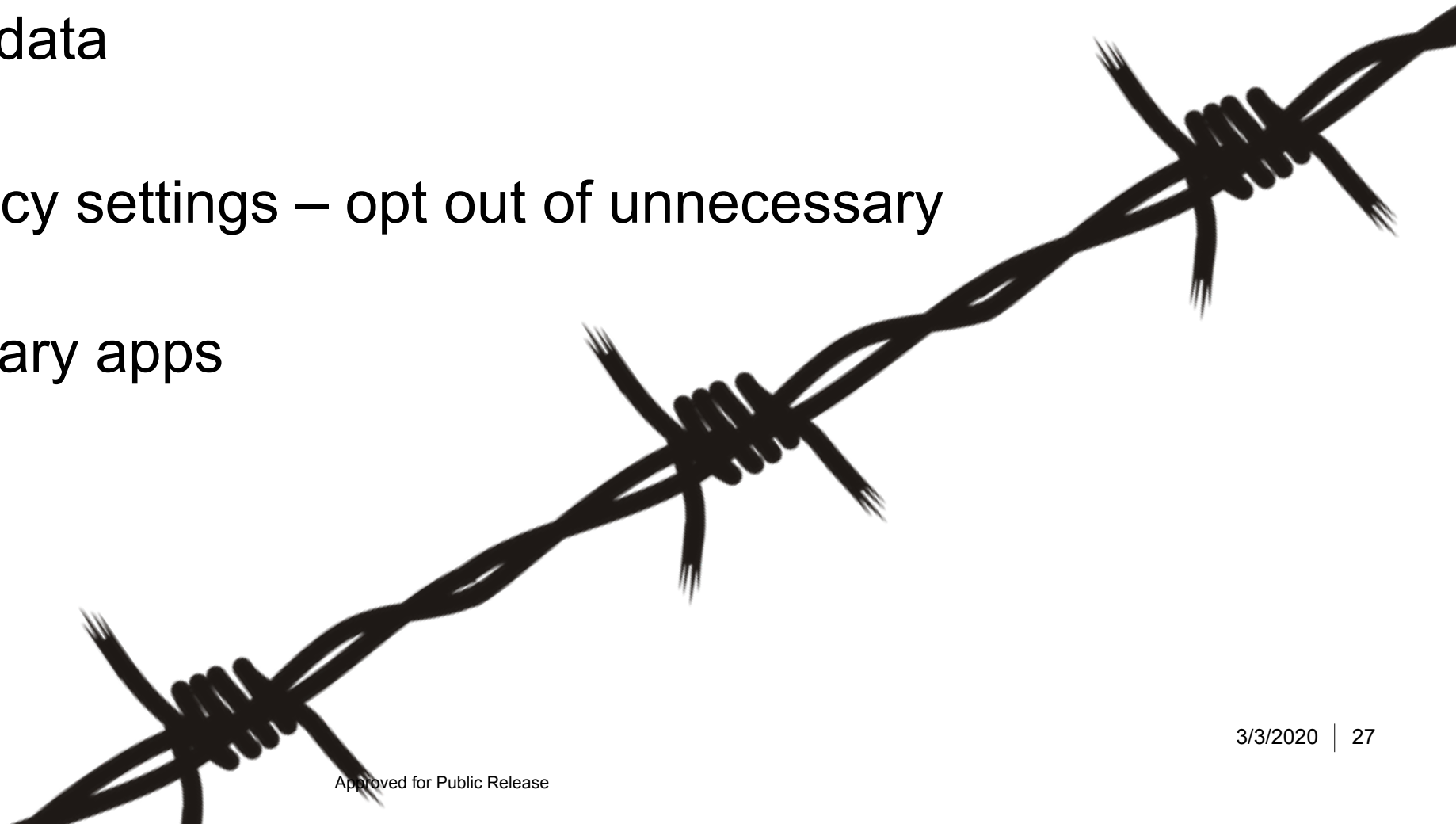
- Hashtag hijacking: “when a hashtag that a brand sets up to generate positive PR, is hijacked by detractors. Instead of being used for positive sentiment, it is used for attacks on the business, or in a sarcastic or snarky way.” (Campbell, 2019)



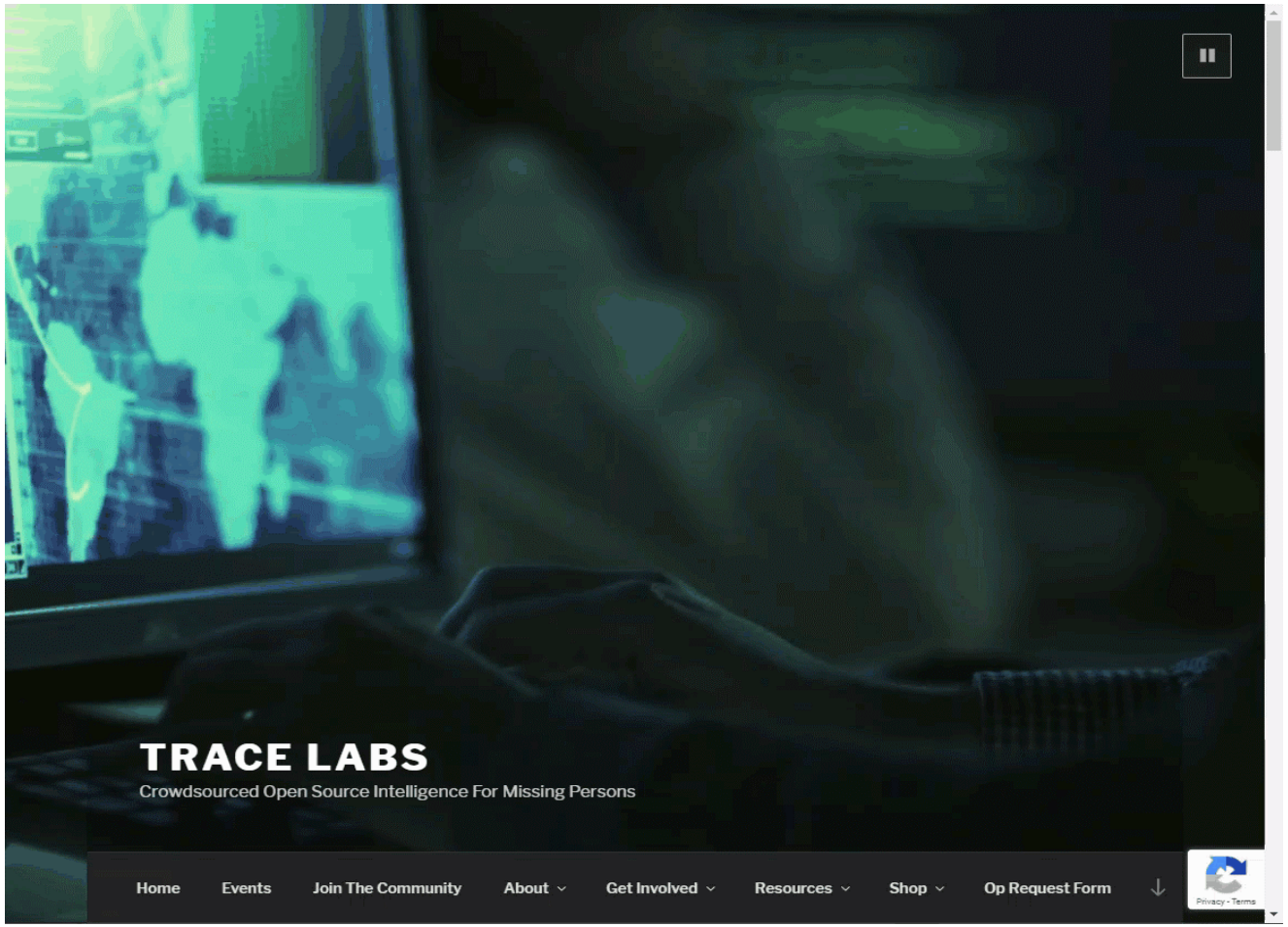
https://setup.us/blog/hashtag-hijacking

Defensive Measures

- When answering security questions don't actually answer the question but use something close enough to remember
- Turn off location data
- Privacy screens
- Check your privacy settings – opt out of unnecessary permissions
- Delete unnecessary apps



White Hat OSINT



OSINT methodologies is used to gain valuable information, not only for malicious purposes but to find and fight criminal activity

Resources

- Opportunities & Real Life Examples
  - Trace Labs CTF: tracelabs.org
  - Operation Safe Escape: goaskrose.com
  - The BADASS-Army: badassarmy.org
  - The Innocent Lives Foundation: innocentlivesfoundation.org
- Tools
  - OSINT Tool Breakdown: osintframework.com
  - ExifTool: github.com/exiftool/exiftool