



# Exploiting Your Digital Footprint

**Addy Moran & Vidya Murthy**

Tuesday, March 3, 2020

Copyright © 2020 Raytheon Company. All rights reserved.

# 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

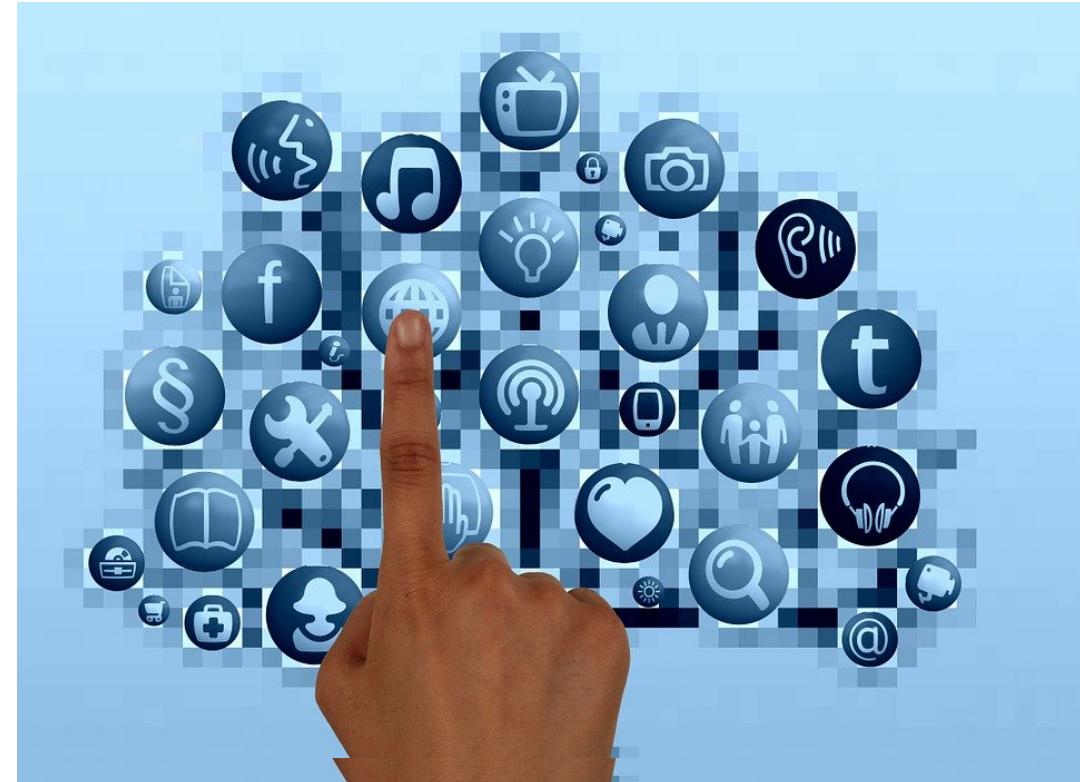
Certified Ethical Hacker

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."

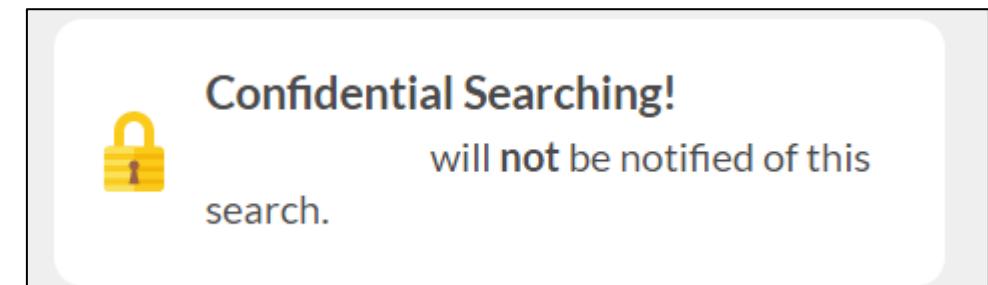
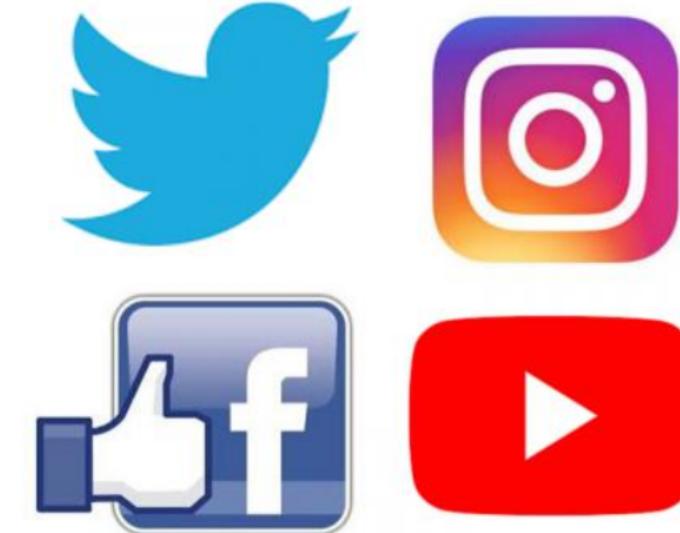
Source: [https://techterms.com/definition/digital\\_footprint](https://techterms.com/definition/digital_footprint)



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

**Goal:** Compromise target's accounts

**Motivation:** Personal, financial, reputational



Pixabay/TheDigitalArtist

Approved for Public Release

# Data Gathering

addy moran

All Images Videos News Maps More Settings Tools

About 1,700,000 results (0.52 seconds)

[www.linkedin.com](http://www.linkedin.com) › addy-moran-7b7875116

[Addy Moran - Cyber Threat Hunter - Raytheon | LinkedIn](#)

[Addy Moran - Cyber Threat Hunter - Raytheon | LinkedIn](#). Join nowSign in.

[addymoran.github.io](http://addymoran.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](http://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](http://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](http://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)



About Addy Moran

WORK

**Backcountry Perspective Photo & Video**  
CFO, Drone Pilot, Photographer · March 31, 2019 to present · Littleton, Colorado

**Raytheon**  
Software Engineer

**Colorado State University**  
Fort Collins, Colorado

EDUCATION

**Colorado State University**  
Class of 2018 · Computer Science · Mathematics · Fort Collins, Colorado

**Metropolitan State University of Denver**  
In 2014 · Denver, Colorado

**Addy Moran**  
6 Followers · 0 Following

Addy Moran's best boards

Drawing, Maybe Possibly?, Crafts, Christmas Ideas, Senior Pic Ideas

Approved for Public Release

People ▾ Addy Moran

**Addy Moran**  
Cyber Threat Hunter at Raytheon  
Colorado Springs, Colorado · 168 connections

Raytheon  
Colorado State University  
Personal Website

About

Software Engineer with more than 4 years of experience in research and development, focusing on cyber security and data analytics. Well-rounded engineer, seasoned in everything from program management to technical implementation.

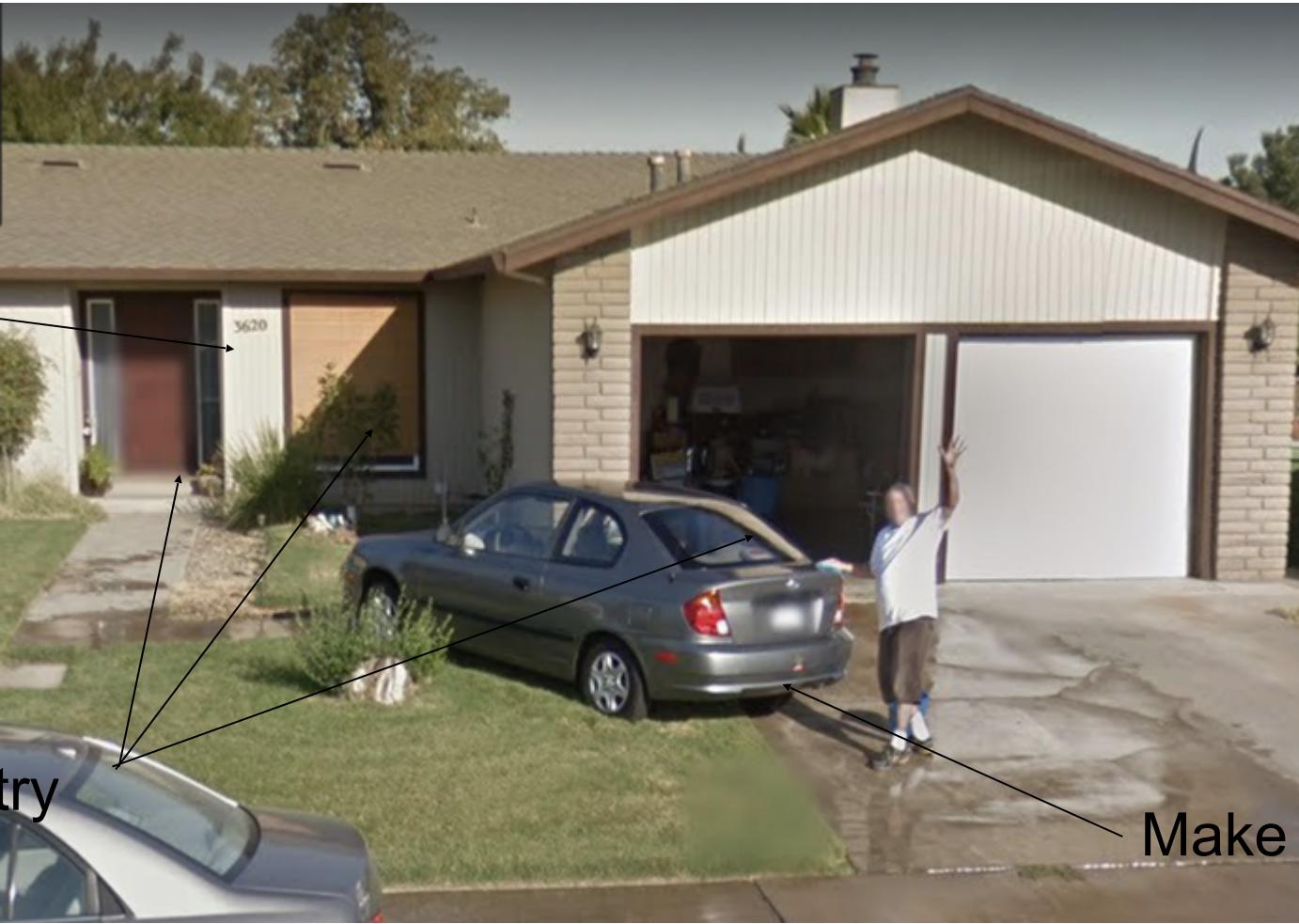
Instagram Search

**addymoran** Follow ...  
63 posts 63 followers 81 following  
Addy Moran

This Account is Private  
Follow to see their photos and videos.

# Data Gathering

Address



Points of Entry

Make & Model of Car

# Data Gathering



24 5' 10 Pittsburgh Yes

Associate Engineering Support at [REDACTED]

Triangle Tech

Virginia Polytechnic Institute and State University (Virginia Tech)

Christian

Mount Lebanon, Pennsylvania

Conservative

 X



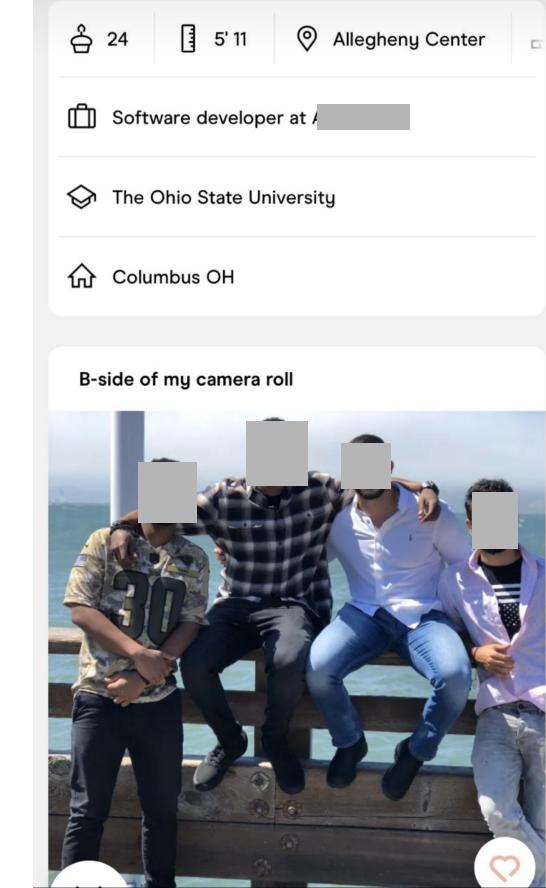
23 5' 11 Trafford Yes

Data Analyst at [REDACTED]

University of Pittsburgh

Oakland, Pennsylvania

 X



24 5' 11 Allegheny Center

Software developer at [REDACTED]

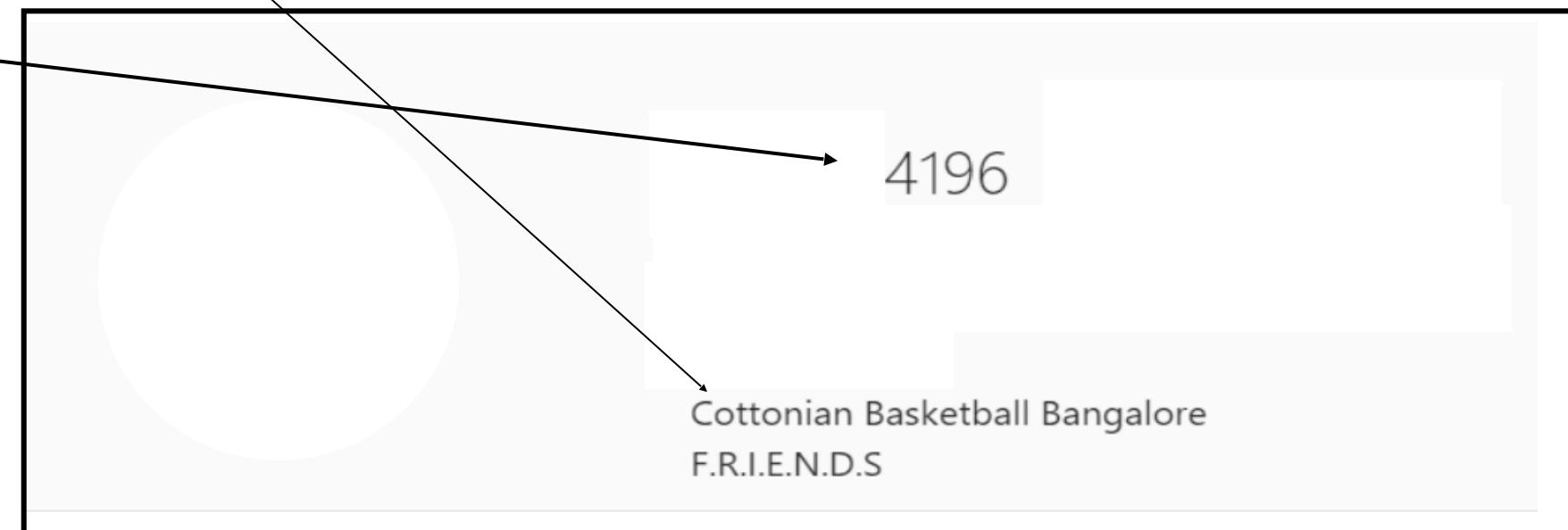
The Ohio State University

Columbus OH

B-side of my camera roll

# Data Gathering

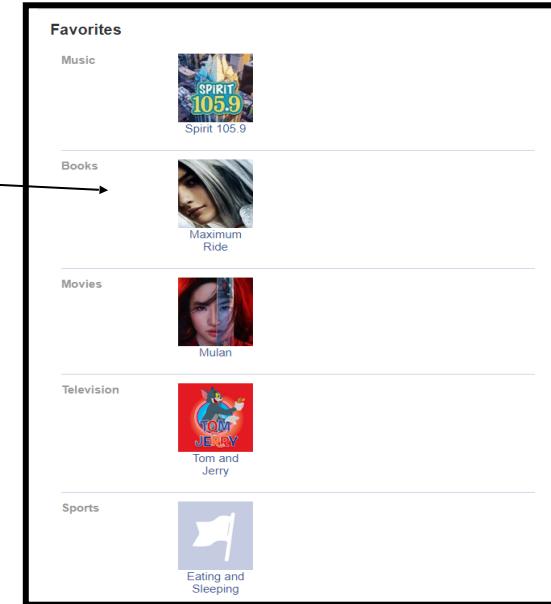
- Things of interest
- Place of residence
- Place of birth
- Birthdays



# Option 1: Reset Password Using Security Questions

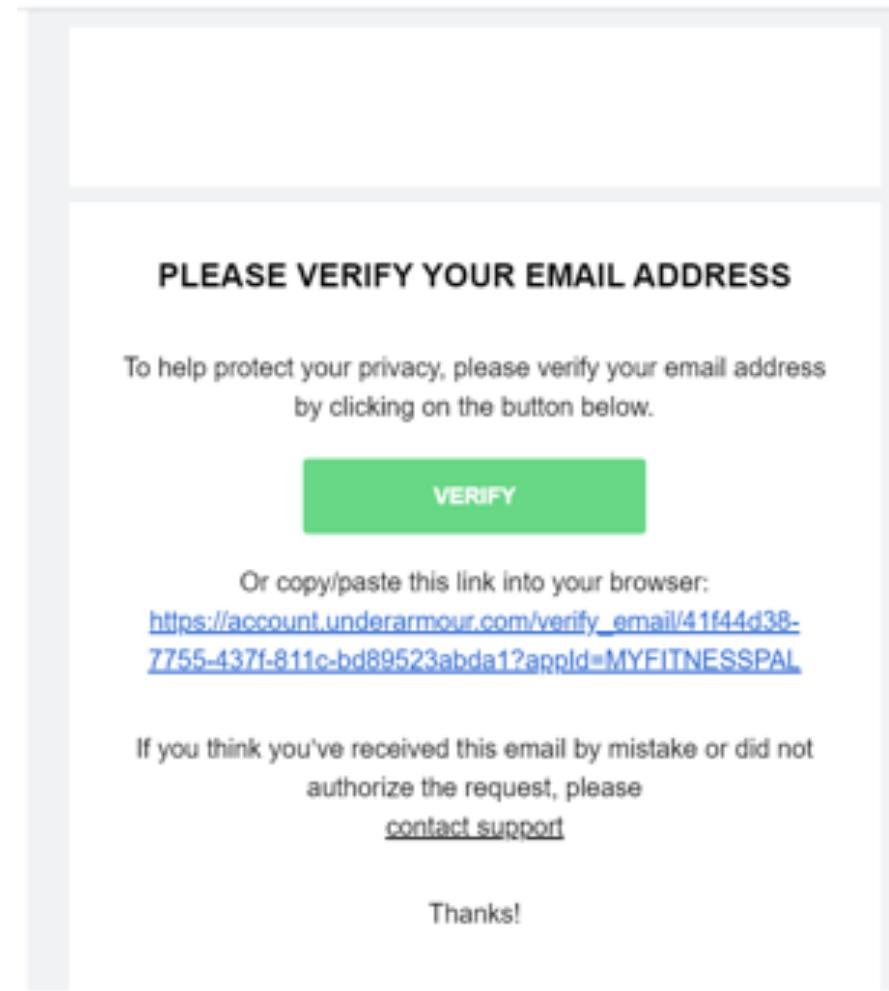
- What is your favorite book? \_\_\_\_\_
- What is the name of the road you grew up on? \_\_\_\_\_
- What is your mother's maiden name?
- What is your favorite food?
- What city were you born in?
- What was the first company that you worked for?
- Where did you go to college? \_\_\_\_\_
- What was the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

[From StumbleForward \(2012\)](#)

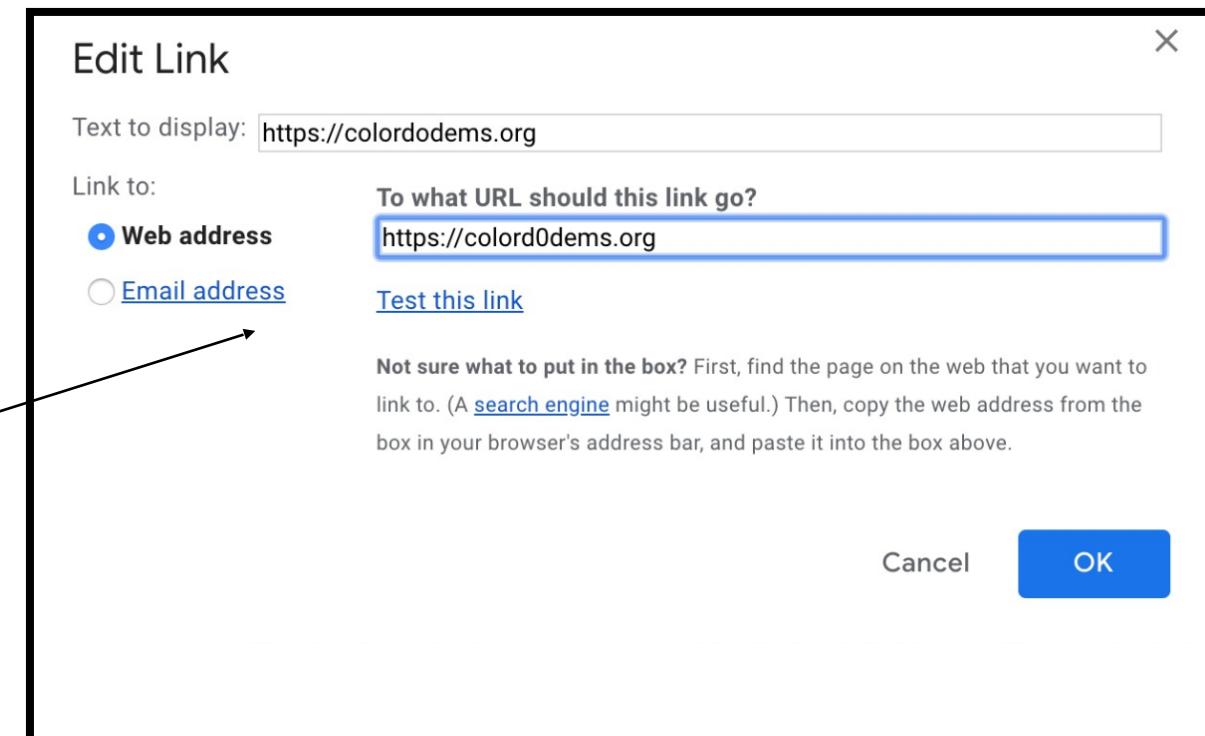
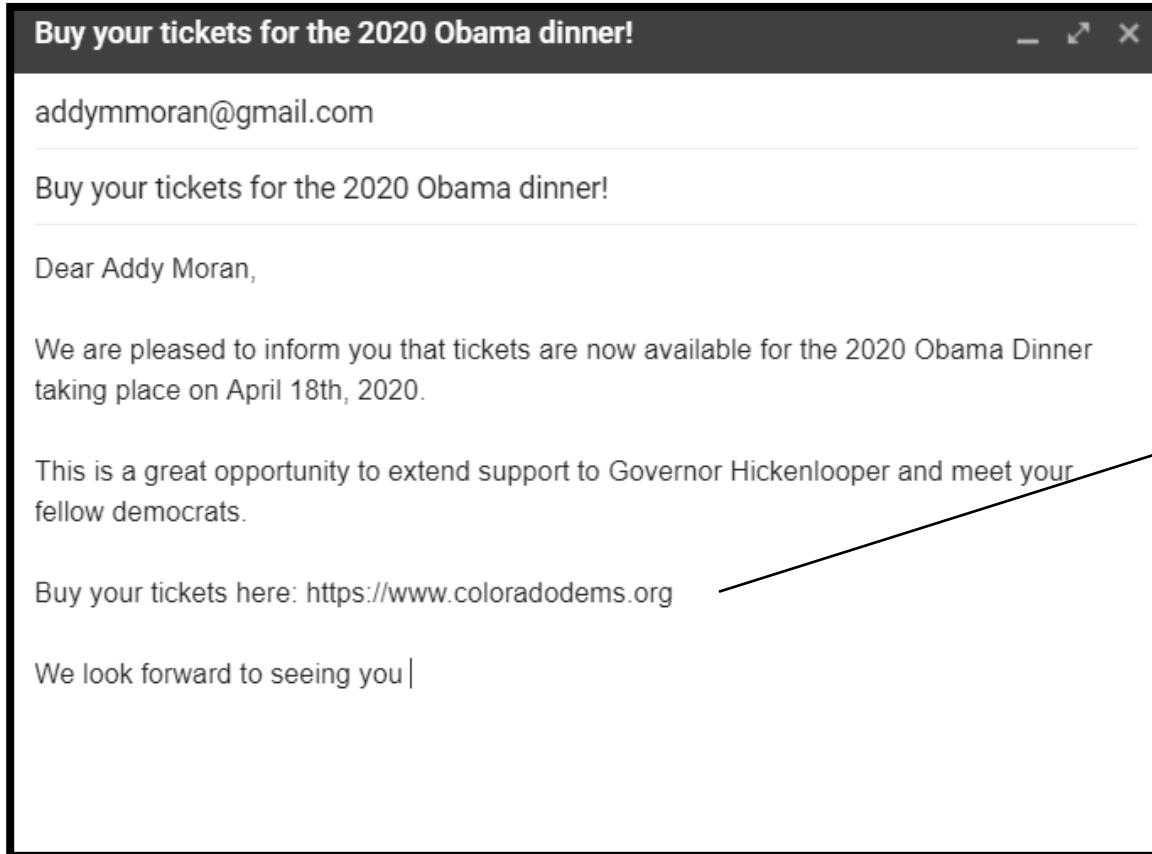


The image consists of two parts. The top part is a photograph of a man and a woman standing on a bridge overlooking a body of water. The bottom part is a screenshot of a LinkedIn profile for a user named "Addy Moran". The profile includes a profile picture, a cover photo of the same couple from the top image, and sections for "About Addy Moran", "WORK", "Raytheon Software Engineer", "Colorado State University Fort Collins, Colorado", and "EDUCATION" (with entries for "Colorado State University Class of 2018 - Computer Science - Mathematics - Fort Collins, Colorado" and "Metropolitan State University of Denver In 2014 - Denver, Colorado").

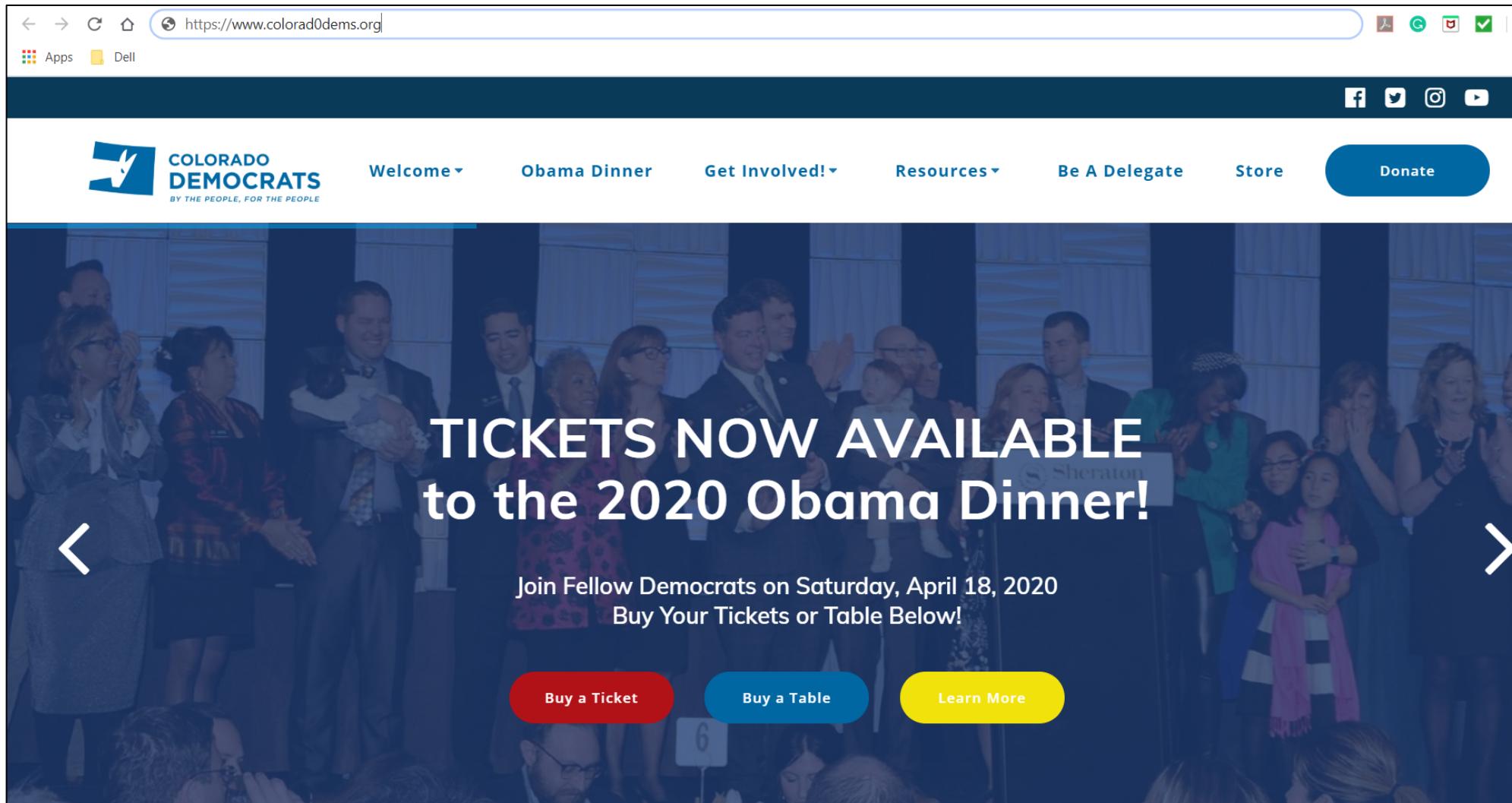
## Option 2: Spear Phishing for Account Information



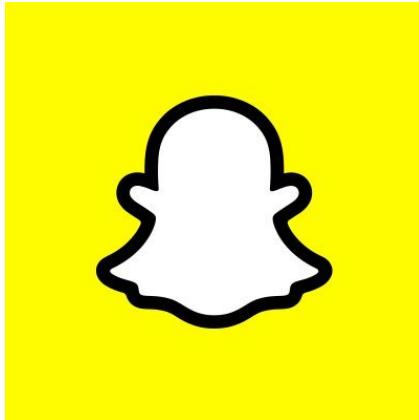
# Option 3: Spear Phishing for Monetary Gains



# Option 3: Spear Phishing for Monetary Gains



# Ammunition for an Insider Threat



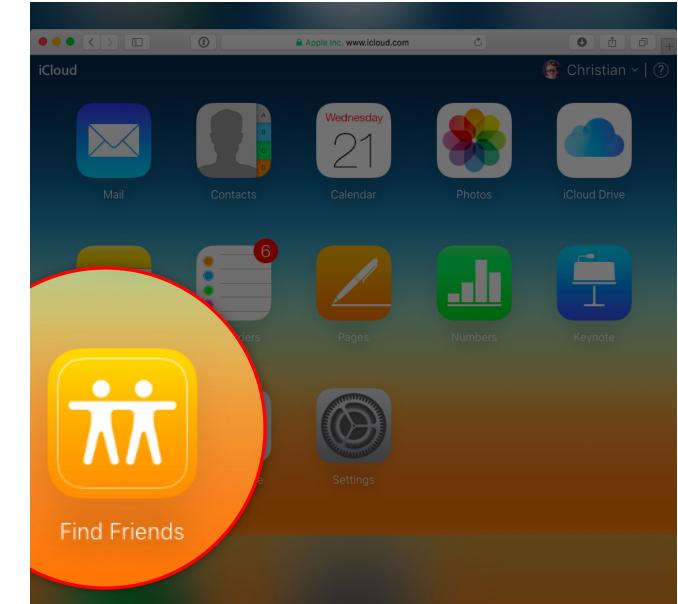
**venmo**



**LinkedIn**



**myspace®**  
a place for friends

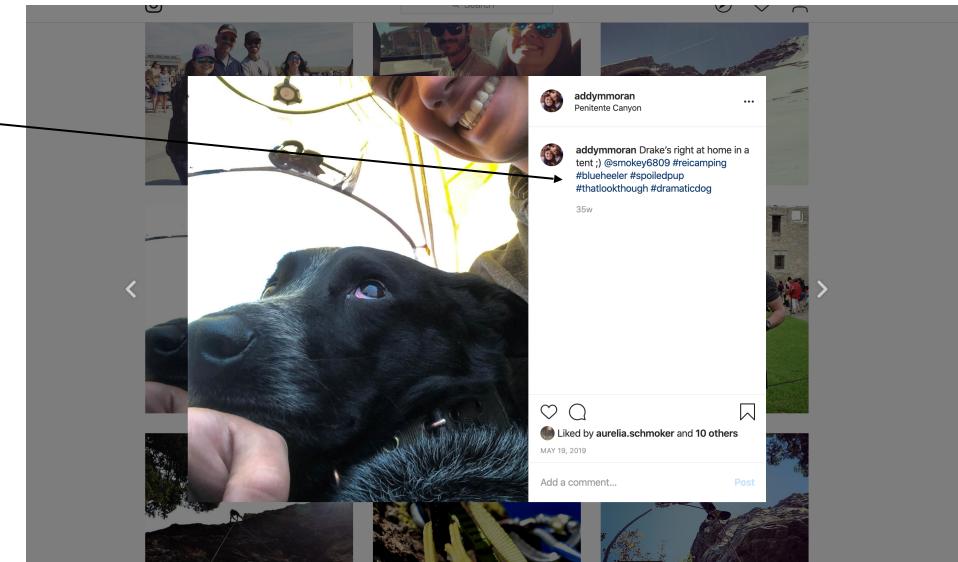


# Exploiting “Being Friends” on Social Media

## Top 10 Security Questions:

- What is your favorite book? → goodreads
- 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 \(2012\)](#)



# Exploiting “Being Friends” on Social Media

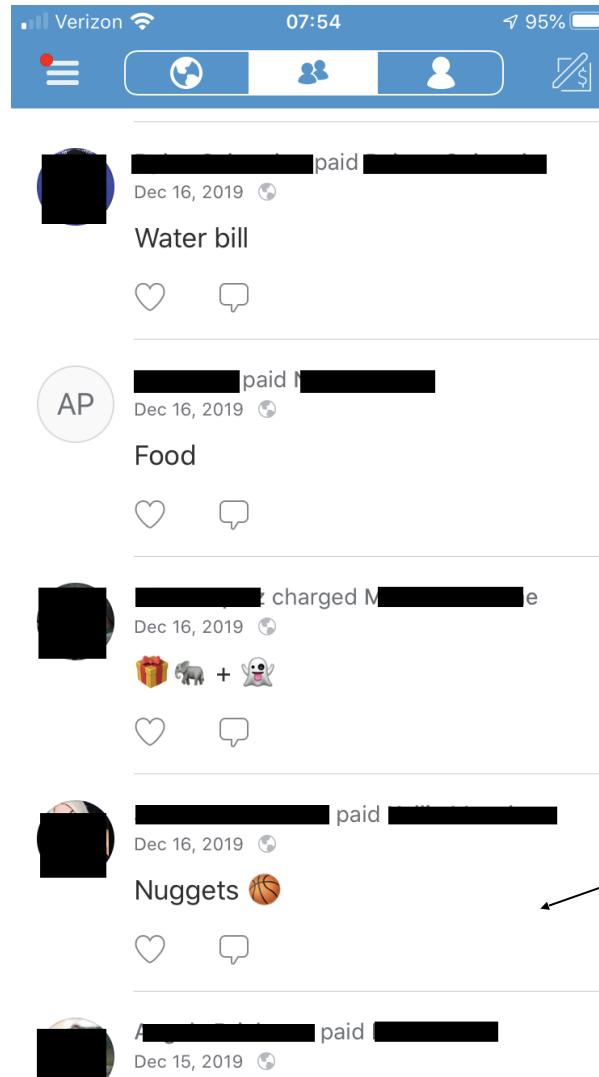
## Top 10 Security Questions:

- 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 \(2012\)](#)

The image shows a LinkedIn profile for Addy Moran. At the top, there's a search bar and navigation links for Home, My Network, Jobs, and More. Below that is a profile picture of Addy Moran, with the title "Cyber Threat Hunter at Raytheon". A section for "Colorado" follows. Under "Work Experience", there's a listing for "Research & Teaching Assistant" at "Colorado State University Online · Part-time" from "Jan 2016 – Jan 2018 · 2 yrs 1 mo" in "Fort Collins, Colorado Area". It notes she completed offensive cyber research on various Internet of Things (IoT) devices and automated the parsing and testing of transferred medical data. Under "Education", it lists "Colorado State University" with a "Bachelor's Degree, Computer Science" from "2013 – 2018". Activities listed include "Activities and Societies: HashDump Security Club" and "IoT Research, HashDump Security Club". In the "Licenses & Certifications" section, two credentials are shown: "Part 107 Commercial Drone Pilot" from "FAA" issued "Feb 2019 · No Expiration Date" with a link to "See credential", and "Certified Ethical Hacker (CEH)" from "EC-Council" issued "Nov 2018 · No Expiration Da" with a link to "See credential".

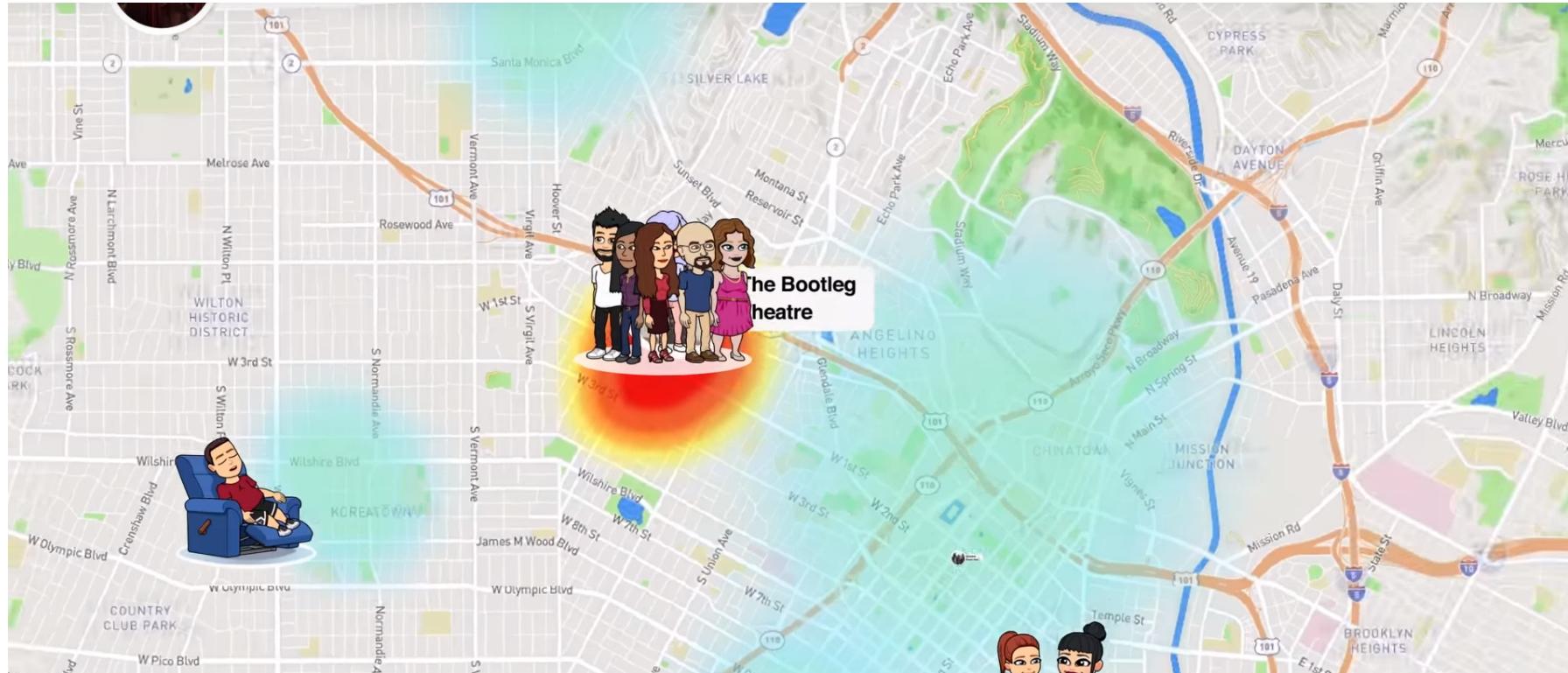
# Unconventional Sources of Information



Roommates

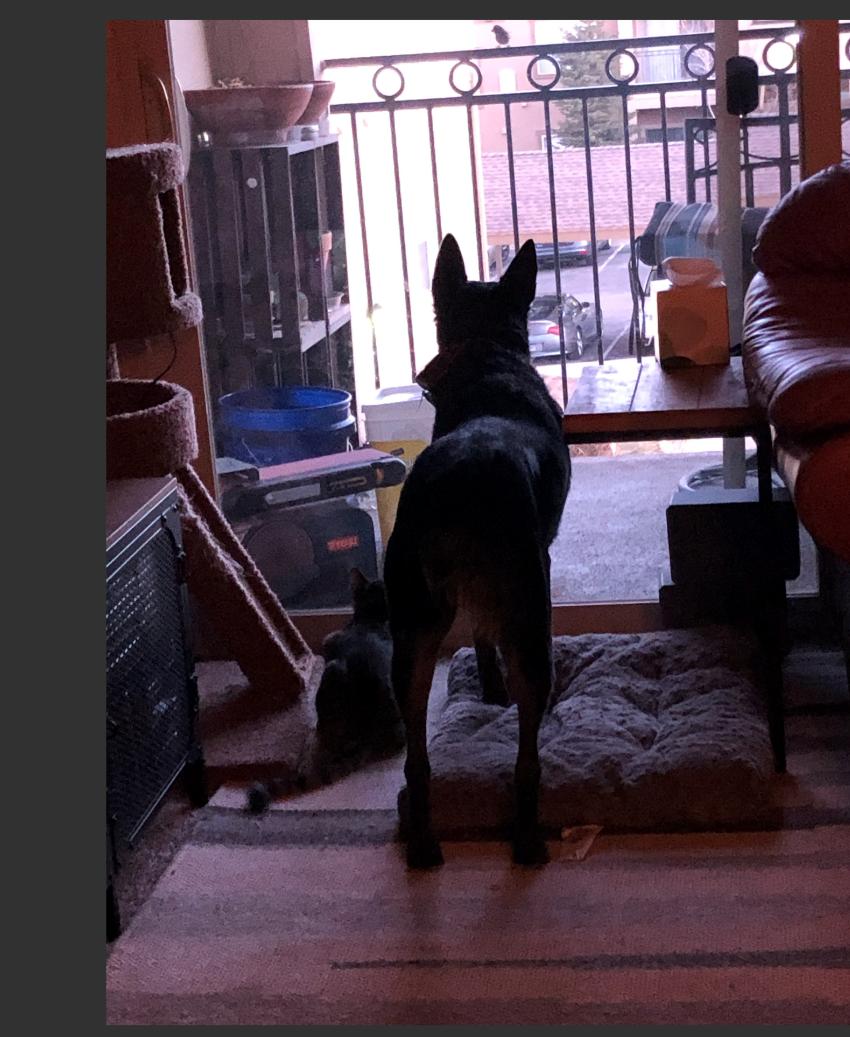
Favorite Sports Teams

# Unconventional Sources of Information



Snapchat Maps

# Unconventional Sources of Information



The image shows a black dog standing on a textured rug, looking out through a glass door or window. Outside, a street with parked cars and buildings is visible. The dog is positioned in front of a dark-colored chair.

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 : calab9582257f104d389913d5d1ea1582  
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 0.78487  
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  
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 : 1/18  
Create Date : 2020:01:28 07:11:44.965-07:00  
Date/Time Original : 2020:01:28 07:11:44.965-07:00  
Modify Date : 2020:01:28 07:11:44-07:00  
GPS Altitude : 0 m Above Sea Level  
GPS Latitude : 1 deg 0' 3" N  
GPS Longitude : 0 deg 48' 1" 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 : 1° 0' 3" N, 0° 48' 1" W  
Hyperfocal Distance : 5.61 m  
Light Value : 5.0  
+ tools ▾

## EXIF Data

# Exploiting the Access of an Insider Threat

Addy Moran  
October 19, 2012 · Denver · •

This is what you get for leaving your facebook open!!!! 😊  
love your gorgeous [REDACTED]

1 Like 1 Comment

Like Comment Share

[REDACTED] Hacked! 😊

Like · Reply · 7y

Write a comment... Smiley face icons

Close

# Exploiting the Access of an Insider Threat

 Addy Moran is with [REDACTED] and [REDACTED] ...  
[REDACTED].

January 29, 2017 · 

When the hacker gets hacked...  
Love you ;)

 You, [REDACTED] and 4 others      1 Comment

---

 Like     Comment     Share

# Company/Organization Perspective

- 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

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)

McDonald's @McDonalds

Meet some of the hard-working people dedicated to providing McDs with quality food every day #McDStories  
mcd.to/zEckNn

18 Jan 12   

@Cate\_Storm

CATE STORM

#McDStories I just read that McDonalds chicken nuggets have a foaming agent in them, similar to products used for building materials

@vegan

Vegan

My memories of walking into a McDonald's: the sensory experience of inhaling deeply from a freshly-opened can of dog food. #McDStories

**and 100's more...**

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

3/3/2020 | 25

# 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)

DIGIORNO  
DiGiorno Pizza   
@DiGiornoPizza

#WhyIStayed You had pizza.

9/8/14, 11:11 PM

---

Keosha Varela @K\_J\_Writes 1h  
So many courageous ppl sharing their stories re: #whyistayed and #whyileft. Domestic violence is often a hidden issue, bring it to light!

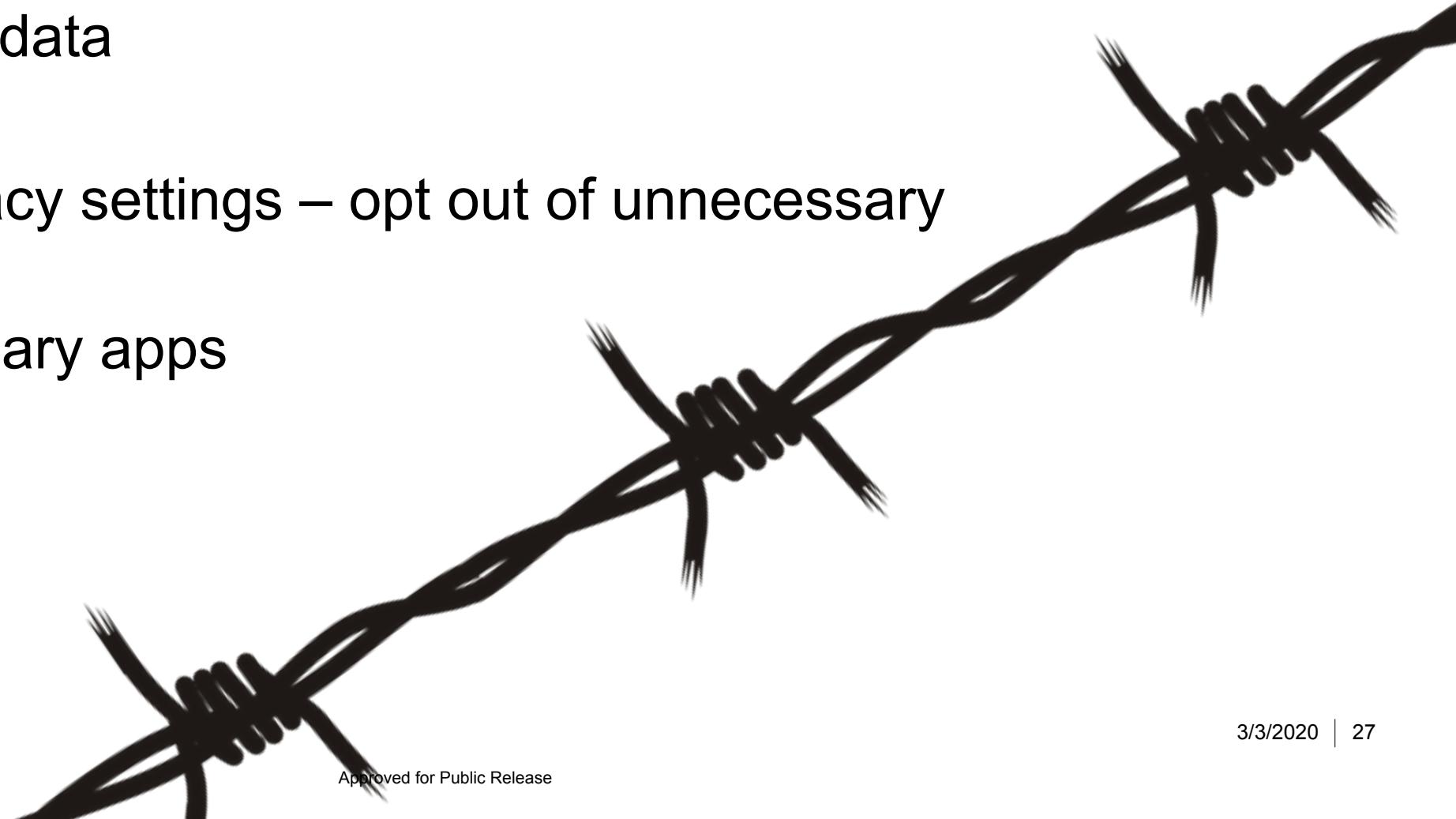
---

Adrienne Airhart @craydrienne 1h  
I couldn't face the fact that I was a textbook statistic: if (step)daddy hurts you, so will hubby. #whyistayed

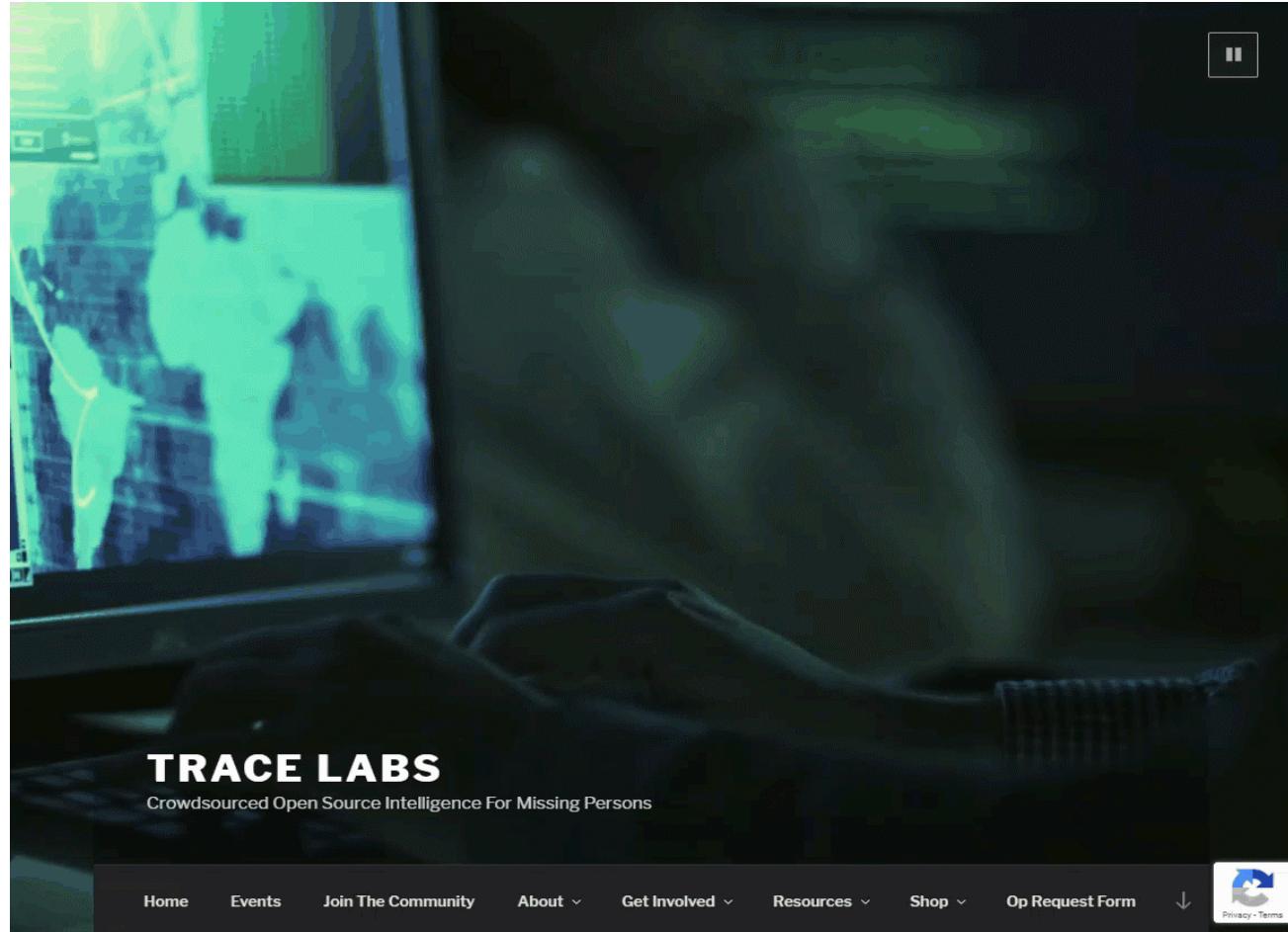
<https://setup.us/blog/hashtag-hijacking>

# 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](http://tracelabs.org)
- Operation Safe Escape: [goaskrose.com](http://goaskrose.com)
- The BADASS-Army: [badassarmy.org](http://badassarmy.org)
- The Innocent Lives Foundation: [innocentlivesfoundation.org](http://innocentlivesfoundation.org)

## ■ Tools

- OSINT Tool Breakdown: [osintframework.com](http://osintframework.com)
- ExifTool: [github.com/exiftool/exiftool](https://github.com/exiftool/exiftool)

