



Intro to Cybersecurity

2.2.2 - OSINT

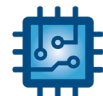


GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

OSINT – Open-Source Intelligence Tools

- To create an effective phishing email, you need to gather information about the target
 - i.e., perform reconnaissance about their life, their interests, their work, family, hobbies, schools, etc.
- Once you have gathered this info you can craft a scam email that will appeal to them personally.
- OSINT tools provide a simple, powerful way to gather publicly available information about people or companies.



GALANTECH —with—
GARDEN STATE CYBER

OSINT Definition

- Any information that can be gathered from free, public sources about an individual or organization
- This information must be legally accessible by a member of the public. Examples are an Etsy review, tweets from an open Twitter account, posting about a home on Zillow,
- OSINT also includes information that has been leaked to the public and are available on the Internet. Examples are information published by Wikileaks.org or posts by data breach hackers. *Essentially, this is accessing information that someone else stole and posted publicly. Does that seem ethical?*



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

What's Online About You?



GALANTECH —with—
GARDEN STATE CYBER

OSINT Tools

- **Google search** - instead of John Doe - use “John Doe”
Try a different search engine! DuckDuckGo, Bing, or Dogpile
- **Google Maps Streetview and Satellite** view
- **Google Reverse Image Search** - with 1 photo of target
- **Archive.org** (aka the Wayback Machine) – even if data is no longer online, it may be available here.
- **Social media sites** – Facebook, Twitter, Pinterest, YouTube, Classmates, Instagram, Reddit – the target’s public profile may have a lot of information.



OSINT Tools

- **Spokeo**: people search with addresses, phone numbers, family relationships
- **Real Estate** – Zillow: cost of home, pictures (in & out), home description
- **LinkedIn** – for info about career & awards & contacts
- **Political affiliation** – www.politicalmoneyline.com
- **Shopping** - Amazon wish lists, gift registries



Example OSINT

- The target is Tony Stark, a rich businessman. We want to gather info about his personal life so that we can spear phish him or find enough info to guess his password.
- The only thing we know to start with is his name and his town: Southfolk, VA.
- Let's begin our OSINT search with **Spokeo** . . .





Intro to Cybersecurity

Activity – OSINT Report on Tony Stark



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Possible phishing emails from this OSINT



Hi Tony,

I'm a realtor in your area and saw that your house was for sale a while ago. Does your family need more space? Are you looking to upscale? I have the perfect home!

Your kids will love the extra space with 7 bedrooms and the pool is ready for fun with a slide and cabana. Plus, you can keep the boat, it's on the water!

[Check out these pictures](#) and call me for a walkthrough. It's priced to sell!



Hi Tony,

I don't know if you'll remember me from when you lived in Malibu. Our kids were in pre-school together way back then! I saw you on Instagram with your adorable new puppy.

We recently moved to the Southfolk area to open a Wag, Wash'n Board franchise. I'd love to connect again and meet your new furry family member.

Come on by! Here's a [coupon](#) for a first grooming!



Spokeo Results

Tony Legene Stark, 74

RESIDES IN MADISON, AL

Lived In Athens AL, Milton FL, Pensacola FL, Riverview FL

Related To Stephen Stark, Karyn Stark, Matthew Stark, Jessica Stark, Daniel Stark

Also known as Denie R Stark, Stark L Tony, Stark Kathy

Includes ✓ Address(18) ✓ Phone(9) ✓ Email(11)

Tony Stark, 57

RESIDES IN HIAWATHA, KS

Lived In Mission KS, Junction City KS, Shawnee KS, Lakeland FL

Also known as Stark Tony

Includes ✓ Address(6) ✓ Phone(6) ✓ Email(4)

Tony Eugene Stark, 52

RESIDES IN SOUTHFOLK, VA

Lived In Malibu CA, Chattahoochee GA

Related To Miriam Bernhart-Stark, William Stark, Logan Stark, Eric Stark, Lindsey Stark, Hailey Stark

Also known as Tony Stark

Includes ✓ Address(13) ✓ Phone(2) ✓ Email(4)

[Spokeo.com](https://www.spokeo.com) - what info can we find here?

1. His age = 52
2. His middle name
3. Used to live in Malibu, CA and Chattahoochee, GA
4. Names of 5 family members, probably wife and children.



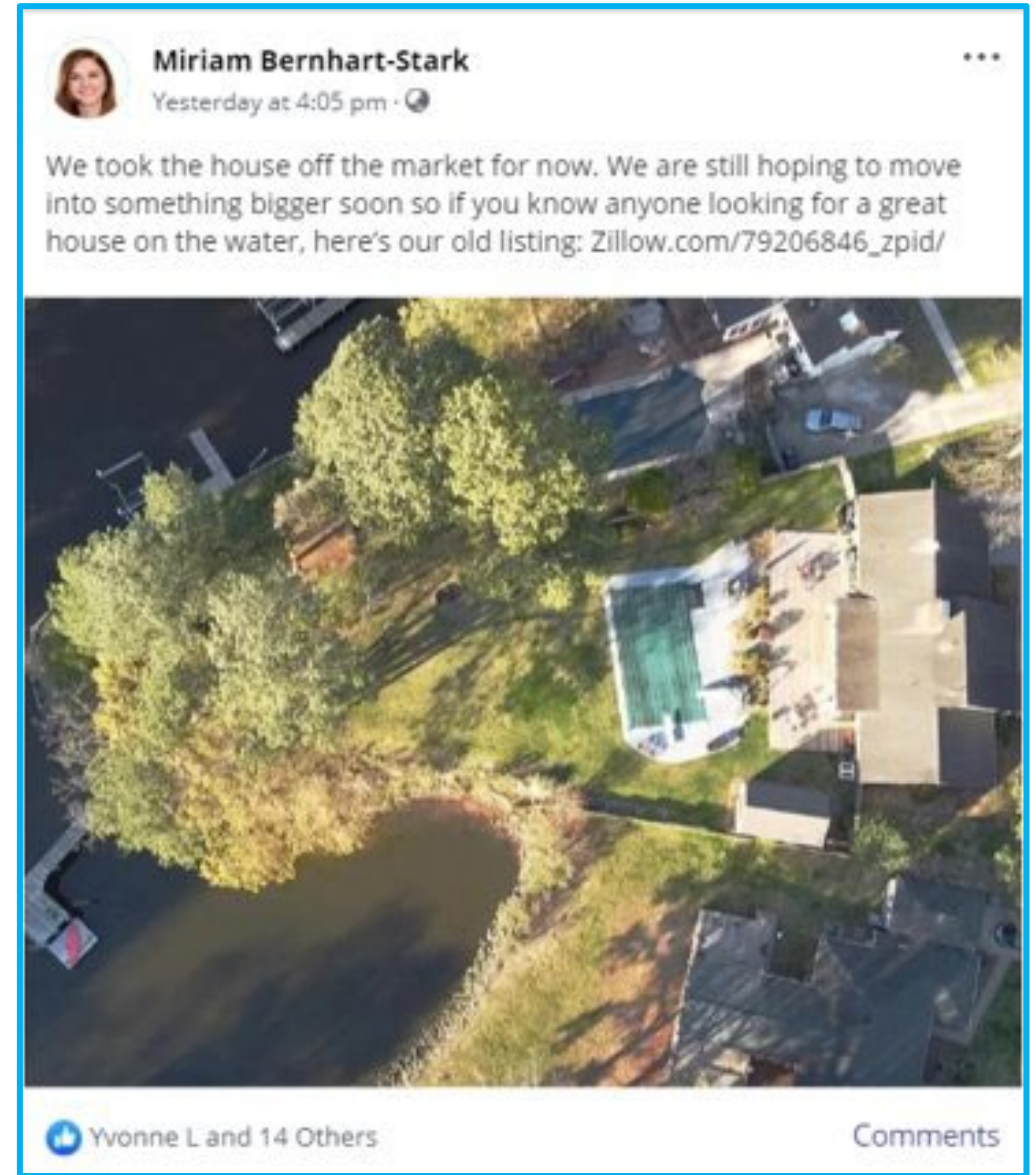
GALANTECH —with—
GARDEN STATE CYBER

Facebook Results

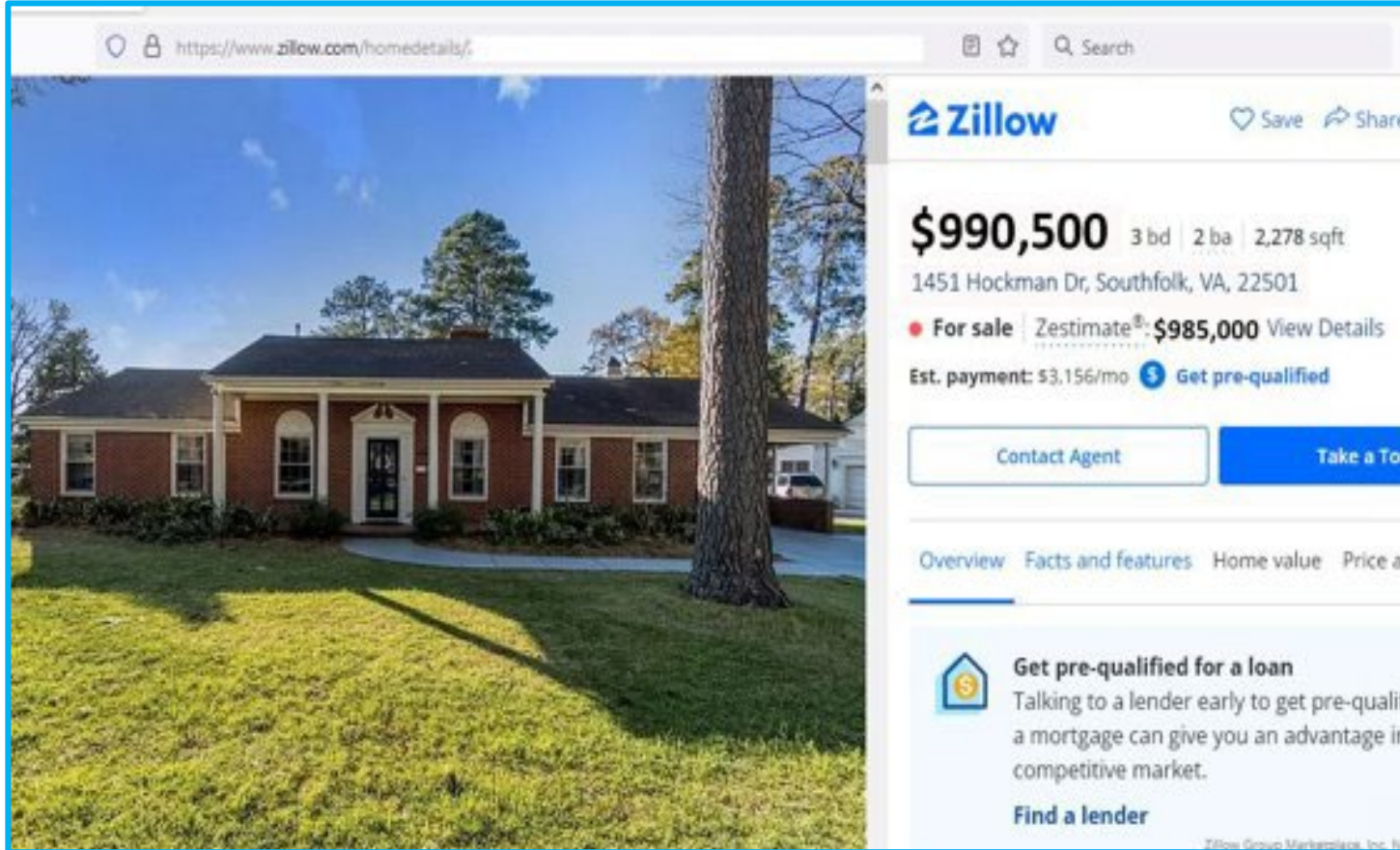
Do a Google search of the first family member name and find her **Facebook** - this is one of her postings that is public.

Info:

1. Now know wife's name
2. They have a pool and live on the water.
3. Family is looking to move to a bigger house.
4. Recent Zillow listing of their home!



Zillow Results



https://www.zillow.com/homedetails/

Zillow Save Share

\$990,500 3 bd | 2 ba | 2,278 sqft
1451 Hockman Dr, Southfolk, VA, 22501

• For sale Zestimate®: **\$985,000** View Details
Est. payment: \$3,156/mo Get pre-qualified

Contact Agent Take a Tour

Overview Facts and features Home value Price a

Get pre-qualified for a loan
Talking to a lender early to get pre-qualified for a mortgage can give you an advantage in a competitive market.
Find a lender

Zillow info:

1. Full Address
2. Price of home
3. Click through pictures
 - all children names on wall
 - there is a baby room



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Twitter Results

Find Tony's **Twitter** account
Info:

1. They have a new pet, a dog
2. It is a Chocolate Lab (breed)
3. Dog's name is "Kona"



Instagram Results

Find Tony's **Instagram** account Info:

1. He has a son (probably middle-school)
2. He likes baseball
3. Favorite team is Yankees



Blog Results

Find Tony's Blog
Info:

1. His birthdate
2. Picture was taken on the family vacation.



IRON MAN ADVENTURES

Burning up the road on my birthday!

4/2/2022

I'm obsessed with racing in all forms but lately Ironman competitions have become my one true hobby. Here's a picture showing off the new biking outfit on my birthday, a couple of days before the latest race. I'll admit that I chose this specific race for the location, not the date - we were able to double up my race with a great family adventure. Anyone want to guess where this was?



GALANTECH —with—
GARDEN STATE CYBER

CYBER.ORG

Exif Results

Use **Exif** tool on the photo
Info:
GPS coordinates - put into
Google Maps to find he
vacationed in *Bearwallow*.



```
File Edit Format View Help
---- ExifTool ----
File Name           : Bike1.jpg
Directory           : .
File Size           : 2.1 MB
File Creation Date/Time : 2022:06:05 15:55:06-04:00
File Type           : JPEG
MIME Type           : image/jpeg
Image Width         : 2448
Image Height        : 3264
---- EXIF ----
Make                : Apple
Camera Model Name   : iPhone 8
Orientation         : Horizontal (normal)
Exposure Time       : 1/3968
F Number            : 2.2
Exposure Program    : Program AE
ISO                 : 32
Shutter Speed Value : 1/3968
Aperture Value      : 2.2
Brightness Value    : 11.1354209
Exposure Compensation : 0
Metering Mode       : Multi-segment
Flash               : Auto, Did not fire
Focal Length        : 4.2 mm
Scene Type          : Directly photographed
Exposure Mode       : Auto
White Balance       : Auto
Focal Length In 35mm Format : 29 mm
Scene Capture Type  : Standard
GPS Latitude        : 37.48429°
GPS Longitude       : -79.66861°
GPS Time Stamp      : 15:22:55.06
GPS Speed Ref       : km/h
GPS Speed           : 0
```