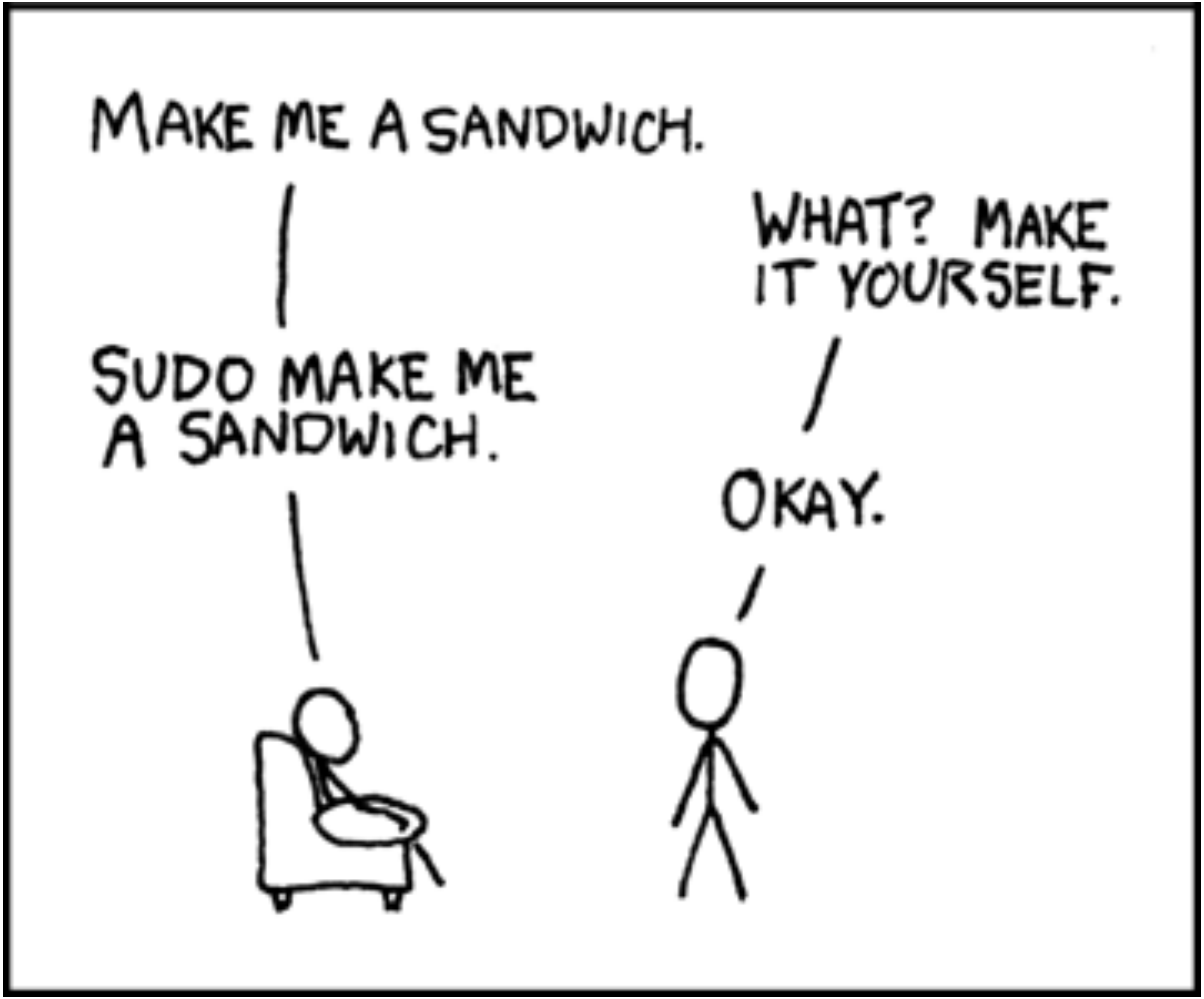
CS 55: Security and Privacy

OSINT and Social Engineering



https://xkcd.com/149/

Discussion

What is OSINT?

- Open-Source Intelligence
- Information available to the general public

What is social engineering?

- Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests

What is reverse social engineering?

- When the user approaches the social engineer

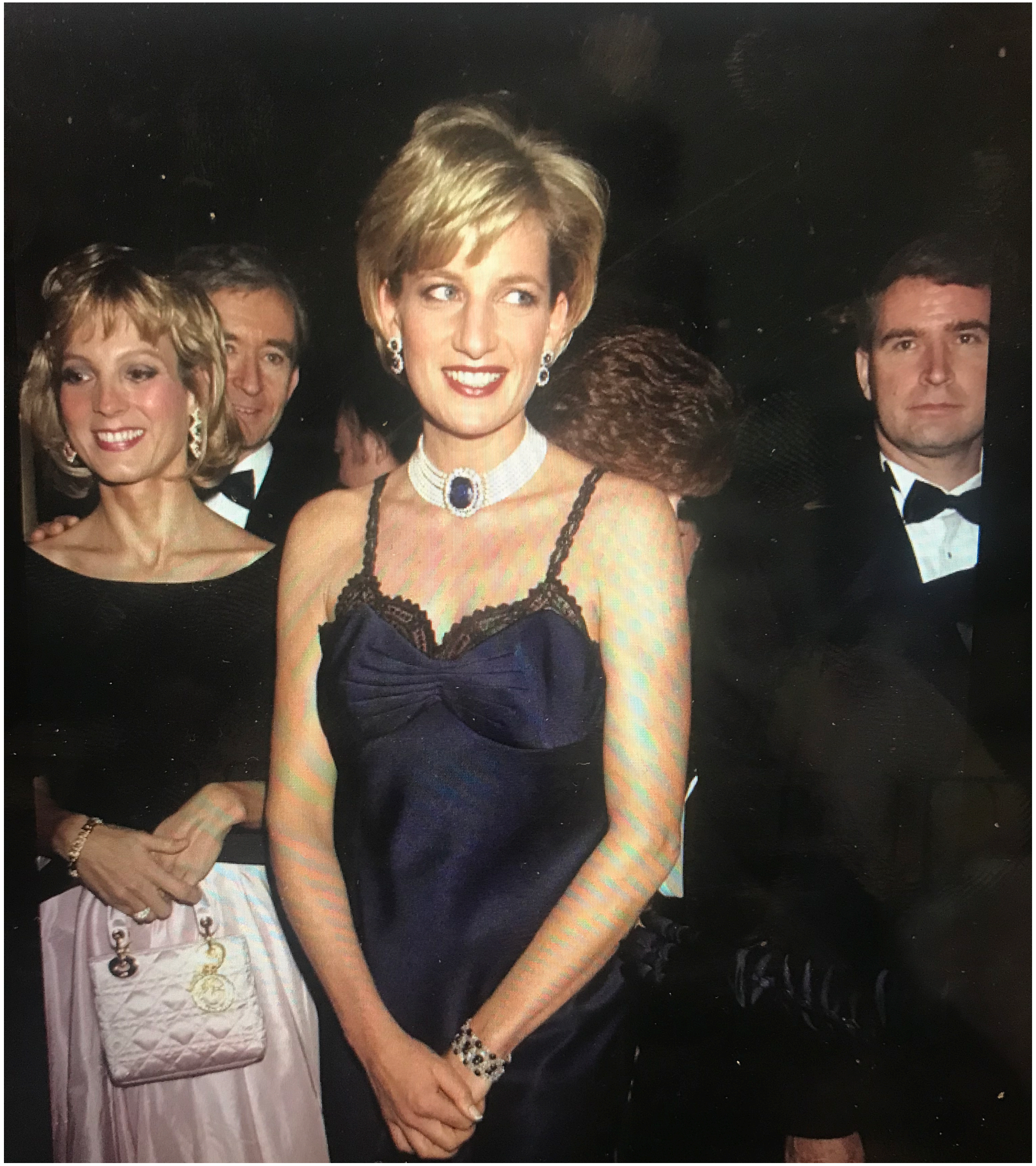
What are advantages of OSINT vs. technical attacks?

- Public, free, legal, low risk of getting caught (passive), possible huge result

NYT story yesterday on social engineering: Who is making all those scam calls?

https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html
https://www.youtube.com/watch?v=R1etkjUN6Ak&t=607&start=60

Another example of social engineering



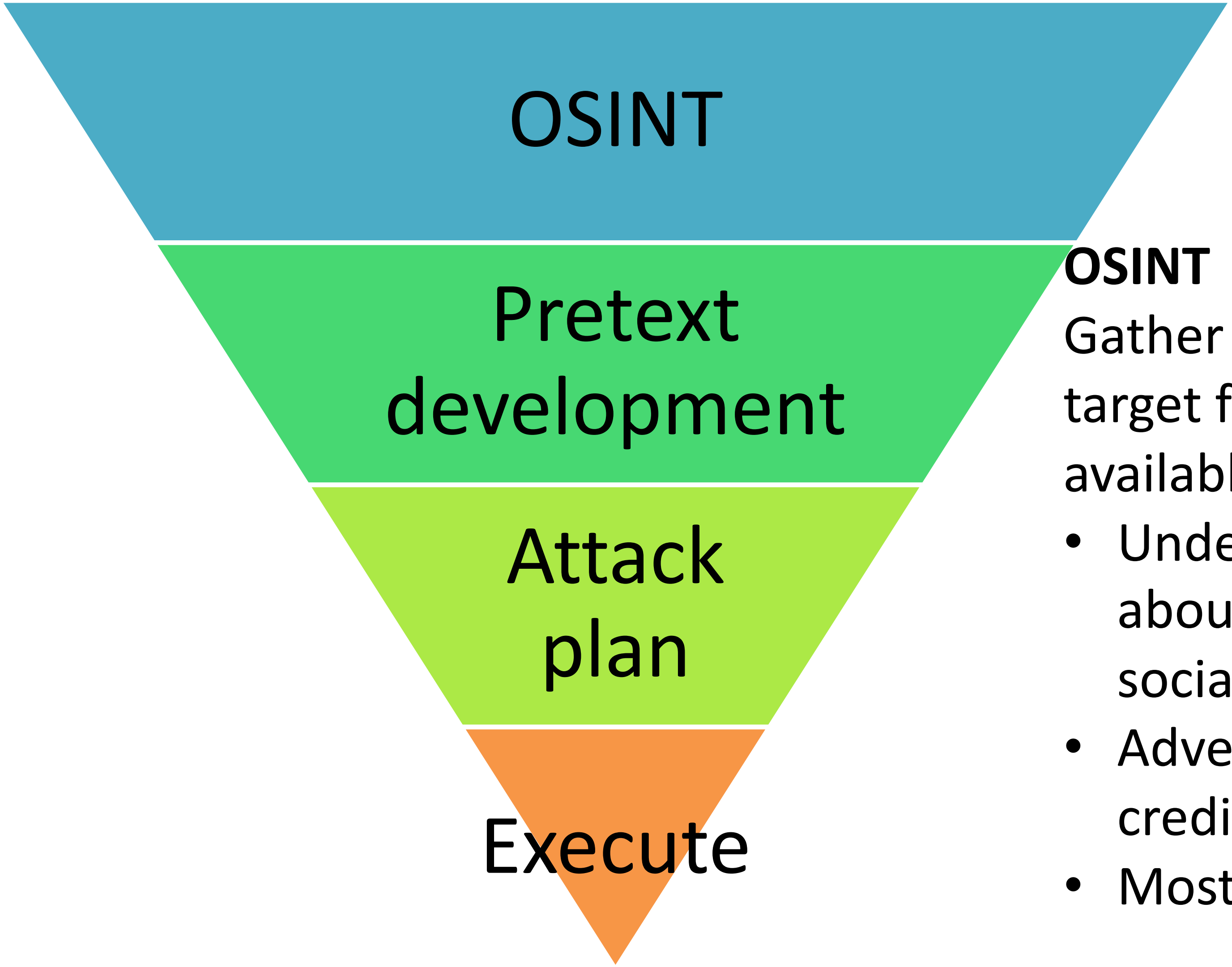
Agenda

1. Open-Source Intelligence (OSINT)

2. Social engineering

3. Defenses

Social engineering attacks typically begin with Open-Source Intelligence (OSINT)



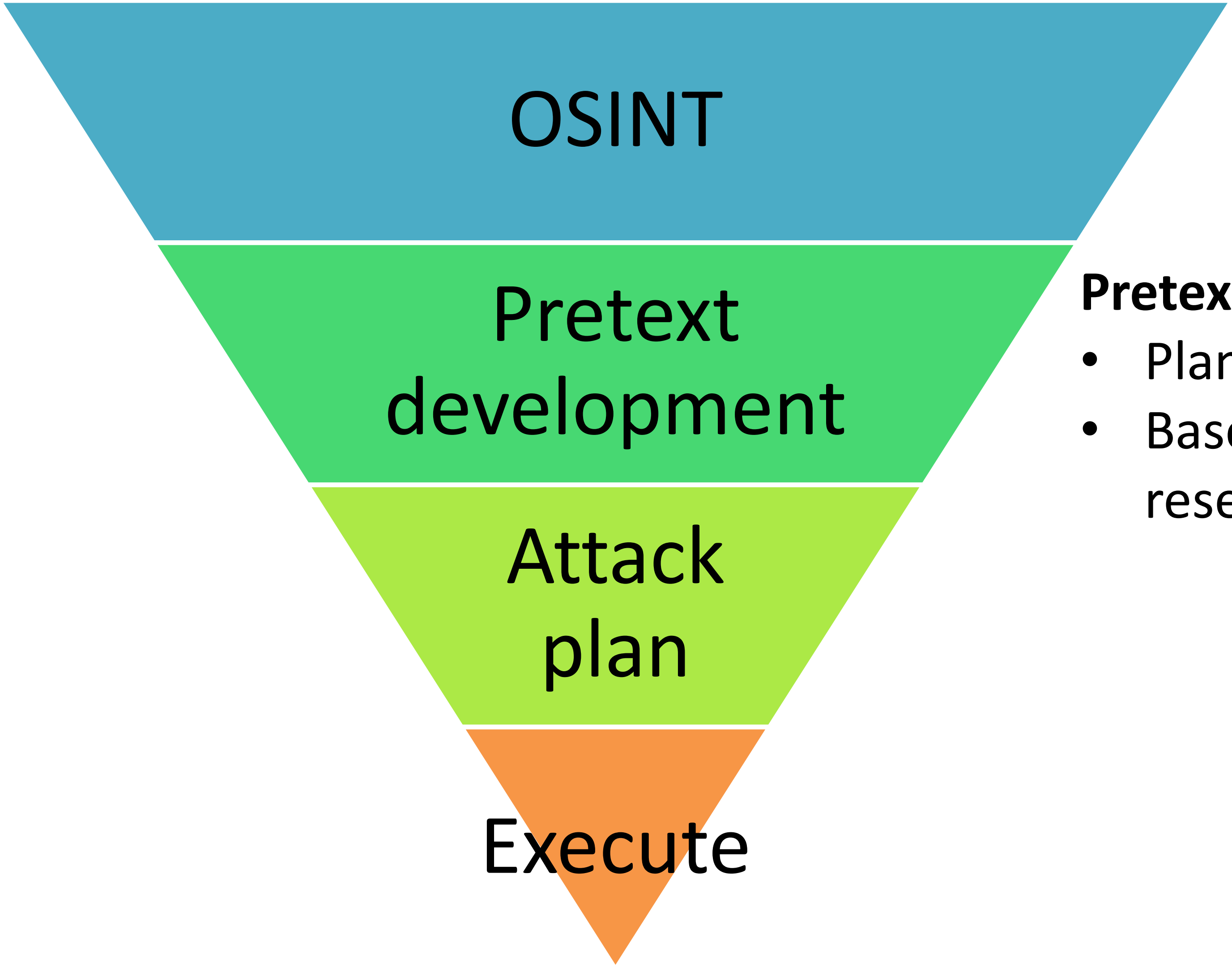
OSINT

Gather intelligence about target from openly available sources

- Understand details about target: personal, social, or professional
- Adversary can provide credible info later
- Most time spent here

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

After gathering OSINT information, social engineers develop a pretext for an attack

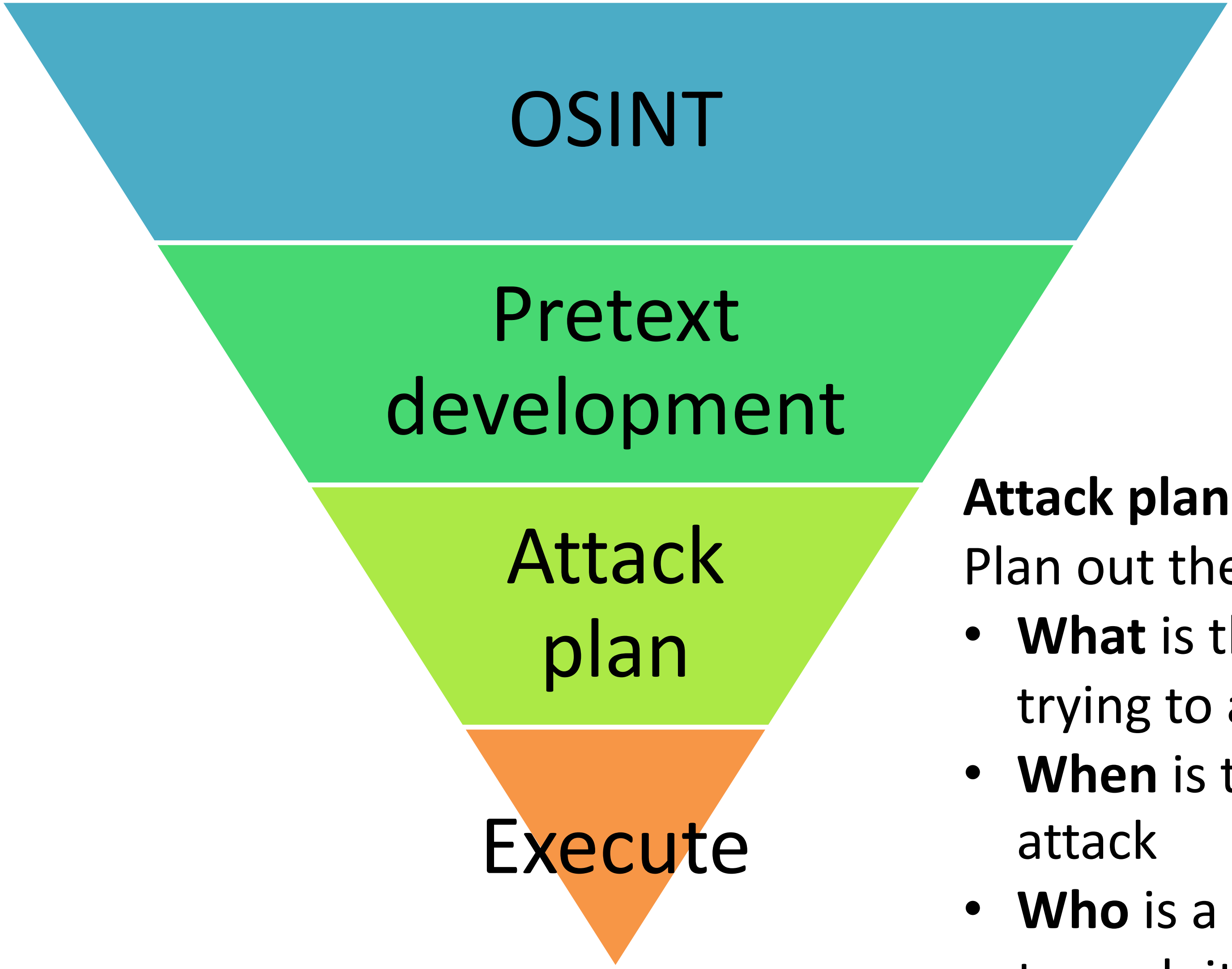


Pretext development

- Plan a cover story
- Based on OSINT research

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Next social engineers plan their attack, focusing on What, When and Who



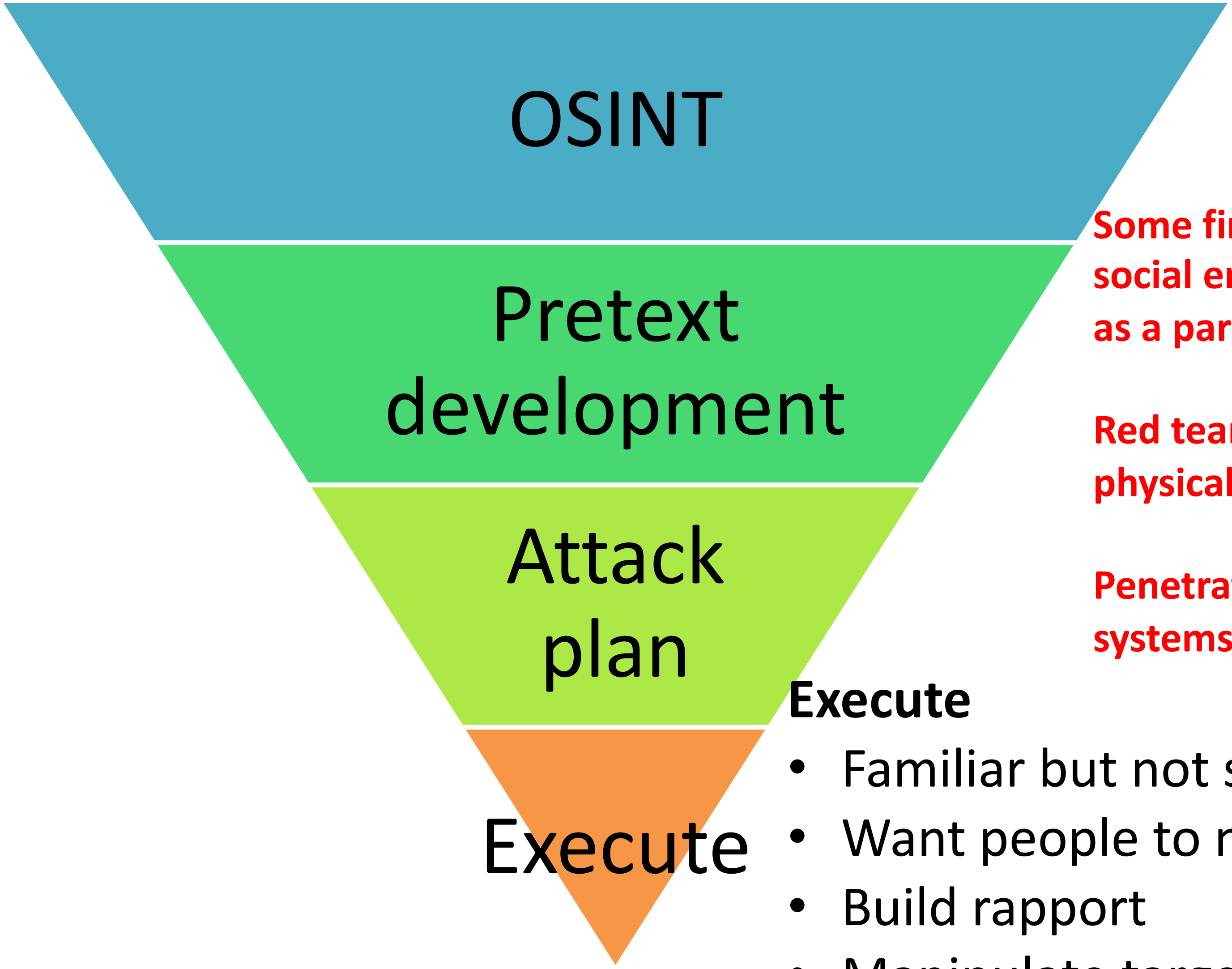
Attack plan

Plan out the 3 W’s

- **What** is the adversary trying to achieve
- **When** is the best time to attack
- **Who** is a good candidate to exploit

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Finally, social engineers execute an attack, exploiting humans



Some firms specialize in only social engineering, many use it as a part of a penetration test

Red teams come onsite to physically gain entry

Penetration tests attack systems

Execute

- Familiar but not scripted
- Want people to not think too much
- Build rapport
- Manipulate target

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Some questions to ask when doing OSINT about a corporation

OSINT on a corporation

- How does the corporation use the Internet?
- How does the corporation use social media?
- Does the corporation have policies in place for what its people can put on the Internet?
- How many vendors does the corporation have?
- What vendors does the corporation use?
- How does the corporation accept payments?
- How does the corporation issue payments?
- Does the corporation have call centers?
- Where are headquarters, call centers, or other branches located?
- Does the corporation allow BYOD (bring your own device)?
- Is the corporation in one location or many locations?
- Is there an org chart available?

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Some questions to ask when doing OSINT about an individual

OSINT on an individual

- What social media accounts does the person use?
- What hobbies does the person have?
- Where does the person vacation?
- What are the person's favorite restaurants?
- What is the person’s family history (sicknesses, businesses, …)?
- What is the person's level of education/areas of study?
- What is the person's job role, including whether people work from home, for themselves, and who they report to?
- Are there any other sites that mention the person (maybe they give speeches, post to forums, or are part of a club)?
- Does the person own a house? If yes, what are the property taxes, liens, and so on?
- What are the names of the person's family members (as well as any of the previously mentioned info on those people)?

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

An OSINT example: finding James Comey's social media accounts

Does Comey even have any social media accounts?
There were at least 60 different social media platforms
In a public appearance, Comey said he had Twitter and Instagram accounts

https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

An OSINT example: finding James Comey's social media accounts

Does Comey even have any social media accounts?

There were at least 60 different social media platforms

In a public appearance, Comey said he had Twitter and Instagram accounts

No twitter accounts with his name

But his son posted a congratulations for being named Director

https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

An OSINT example: finding James Comey’s social media accounts

Does Comey even have any social media accounts?
There were at least 60 different social media platforms
In a public appearance, Comey said he had Twitter and Instagram accounts

No twitter accounts with his name
But his son posted a congratulations for being named FBI Director

Son linked Twitter and Instagram accounts
Instagram locked!
Researcher followed son
Was able to see who son follows – found reinholdniebuhr

https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

An OSINT example: finding James Comey's social media accounts

Does Comey even have any social media accounts?
There were at least 60 different social media platforms
In a public appearance, Comey said he had Twitter and Instagram accounts

No twitter accounts with his name
But his son posted a congratulations for being named FBI Director

Son linked Twitter and Instagram accounts
Instagram locked!
Researcher followed son
Was able to see who son follows – found reinholdniebuhr

Reinhold Niebuhr was American theologian
Died in 1971 – Twitter account probably not him!
Comey wrote about him in his college thesis

https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

An OSINT example: finding James Comey's social media accounts

Does Comey even have any social media accounts?
There were at least 60 different social media platforms
In a public appearance, Comey said he had Twitter and Instagram accounts

No twitter accounts with his name
But his son posted a congratulations for being named FBI Director

Son linked Twitter and Instagram accounts
Instagram locked!
Researcher followed son
Was able to see who son follows – found reinholdniebuhr

Reinhold Niebuhr was American theologian
Died in 1971 – Twitter account probably not him!
Comey wrote about him in his college thesis

Seven Twitter accounts using Reinhold's name
One was @ProjectExile7

https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

An OSINT example: finding James Comey's social media accounts

Does Comey even have any social media accounts?
There were at least 60 different social media platforms
In a public appearance, Comey said he had Twitter and Instagram accounts

Project Exile was the name of a program Comey started when he was a U.S. attorney in Richmond

This is probably his account!

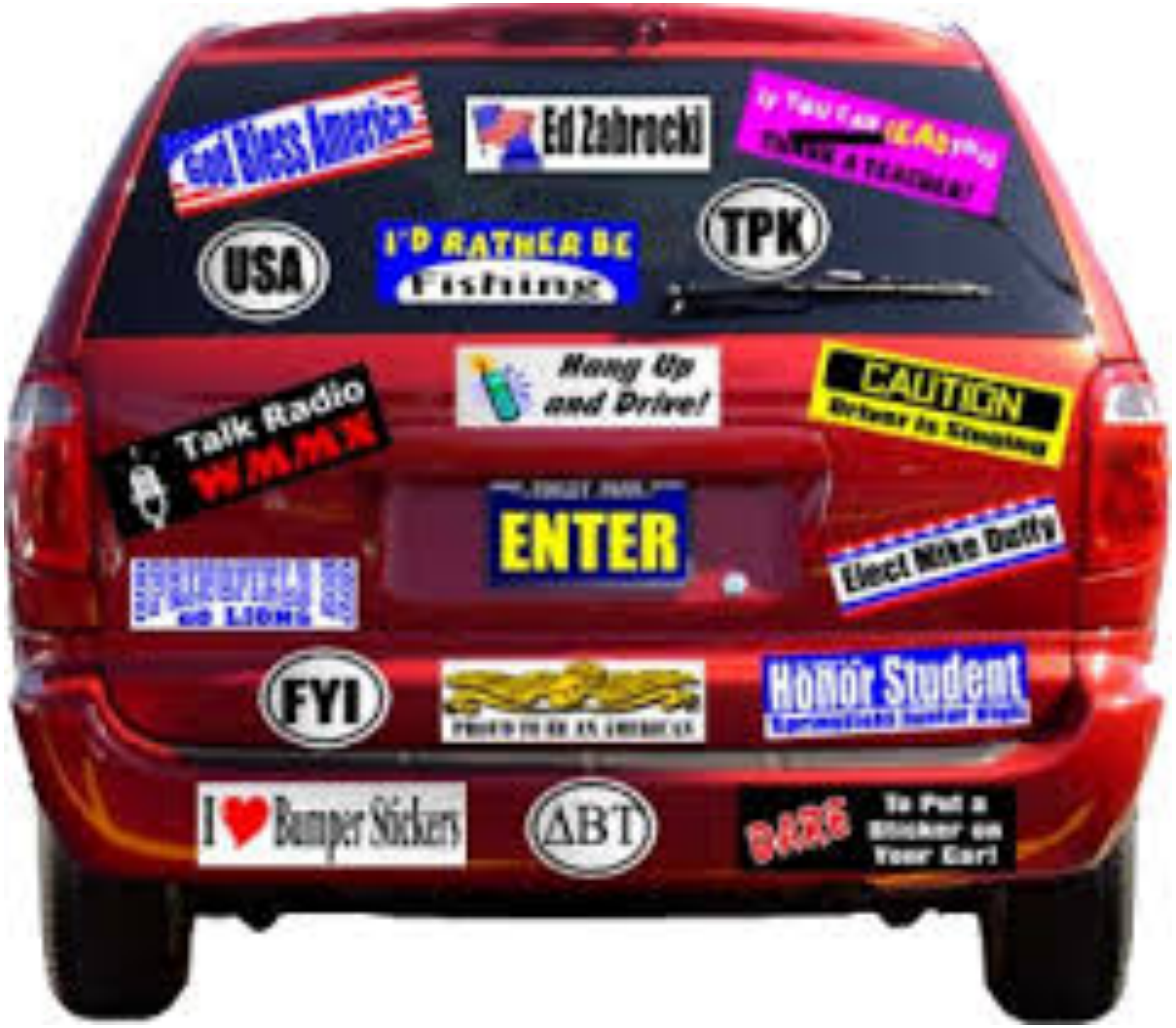
hr

Reinhold Niebuhr was American theologian
Died in 1971 – Twitter account probably not him!
Comey wrote about him in his college thesis

Seven Twitter accounts using Reinhold's name
One was @ProjectExile7

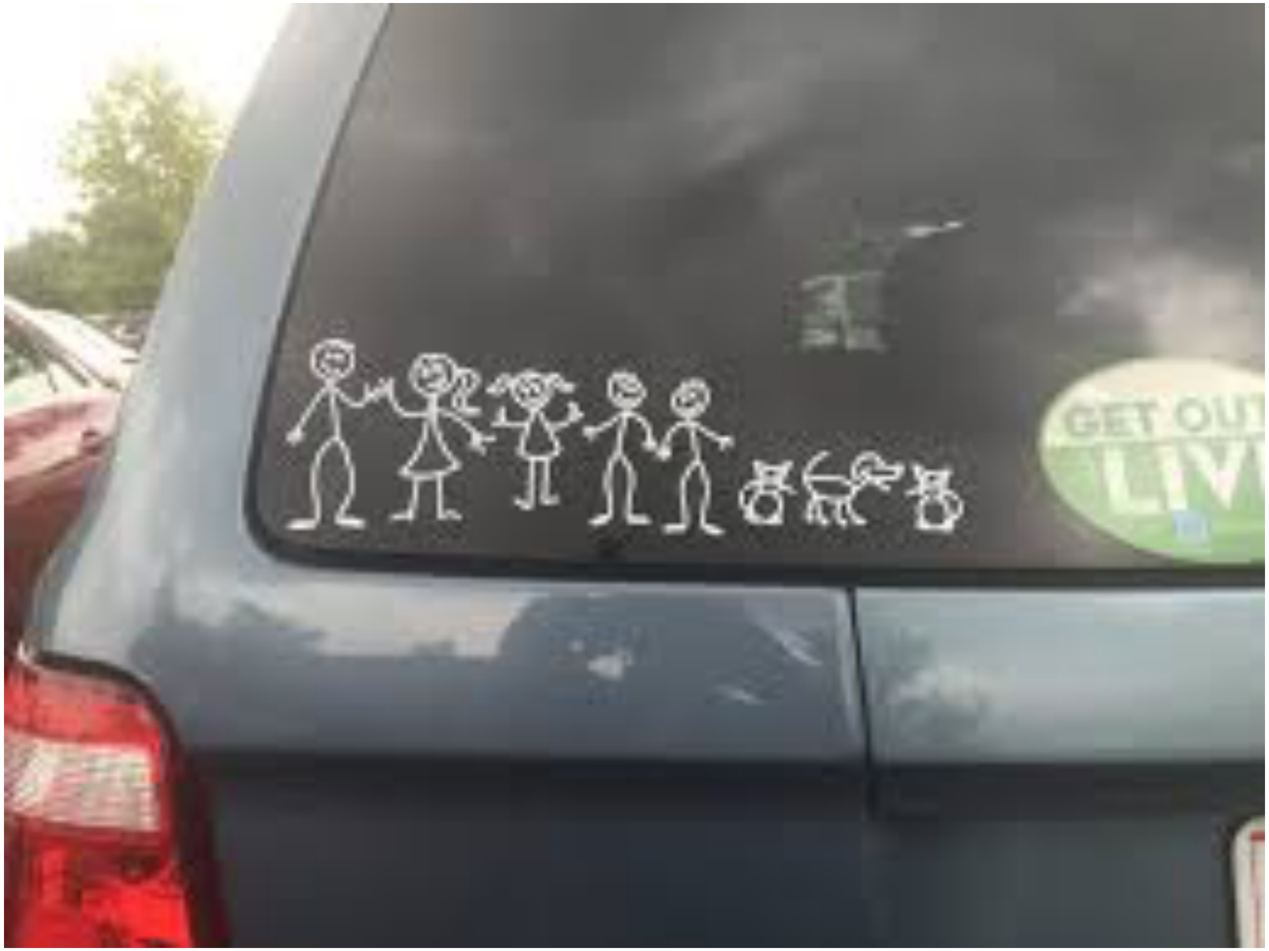
https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

Sometimes you can learn a lot just by passively observing



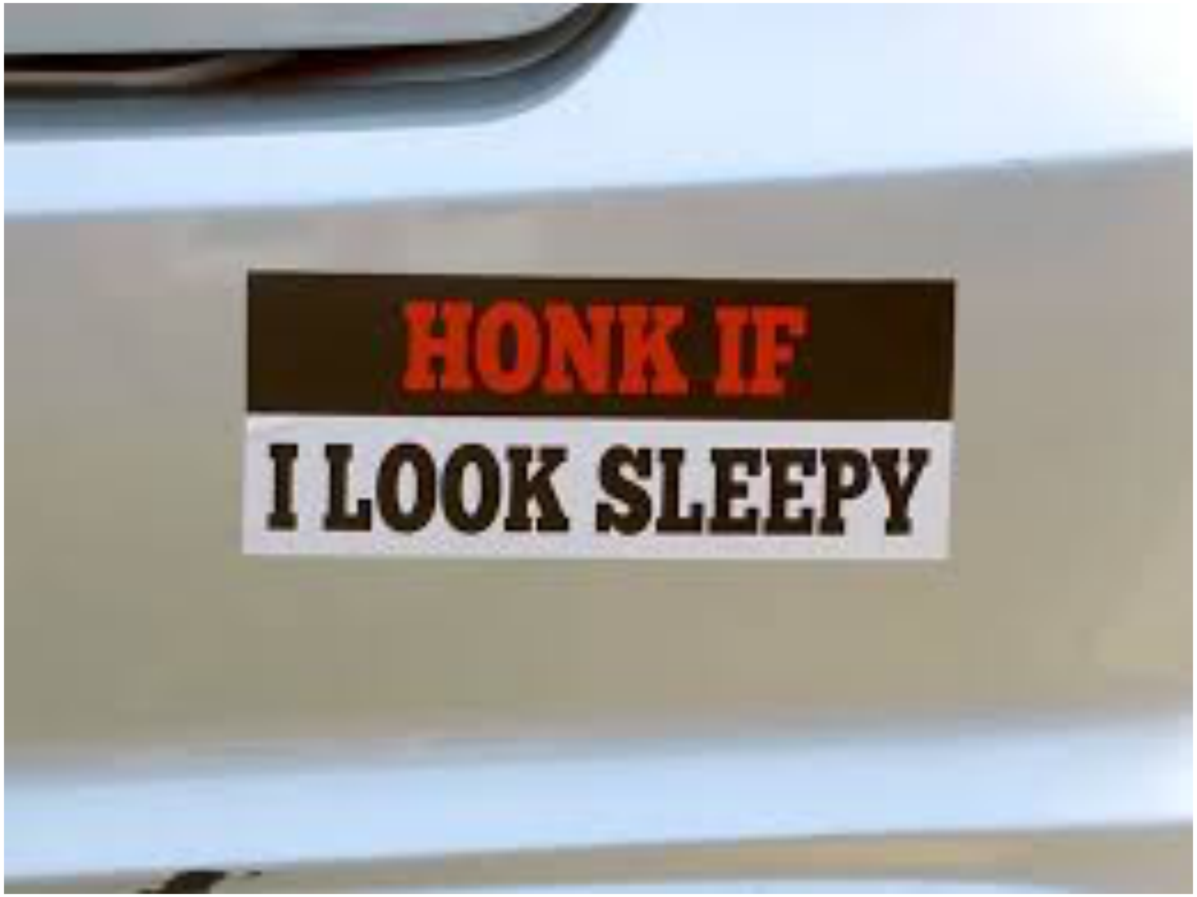
What can we learn by looking at this person's car?

Sometimes you can learn a lot just by passively observing



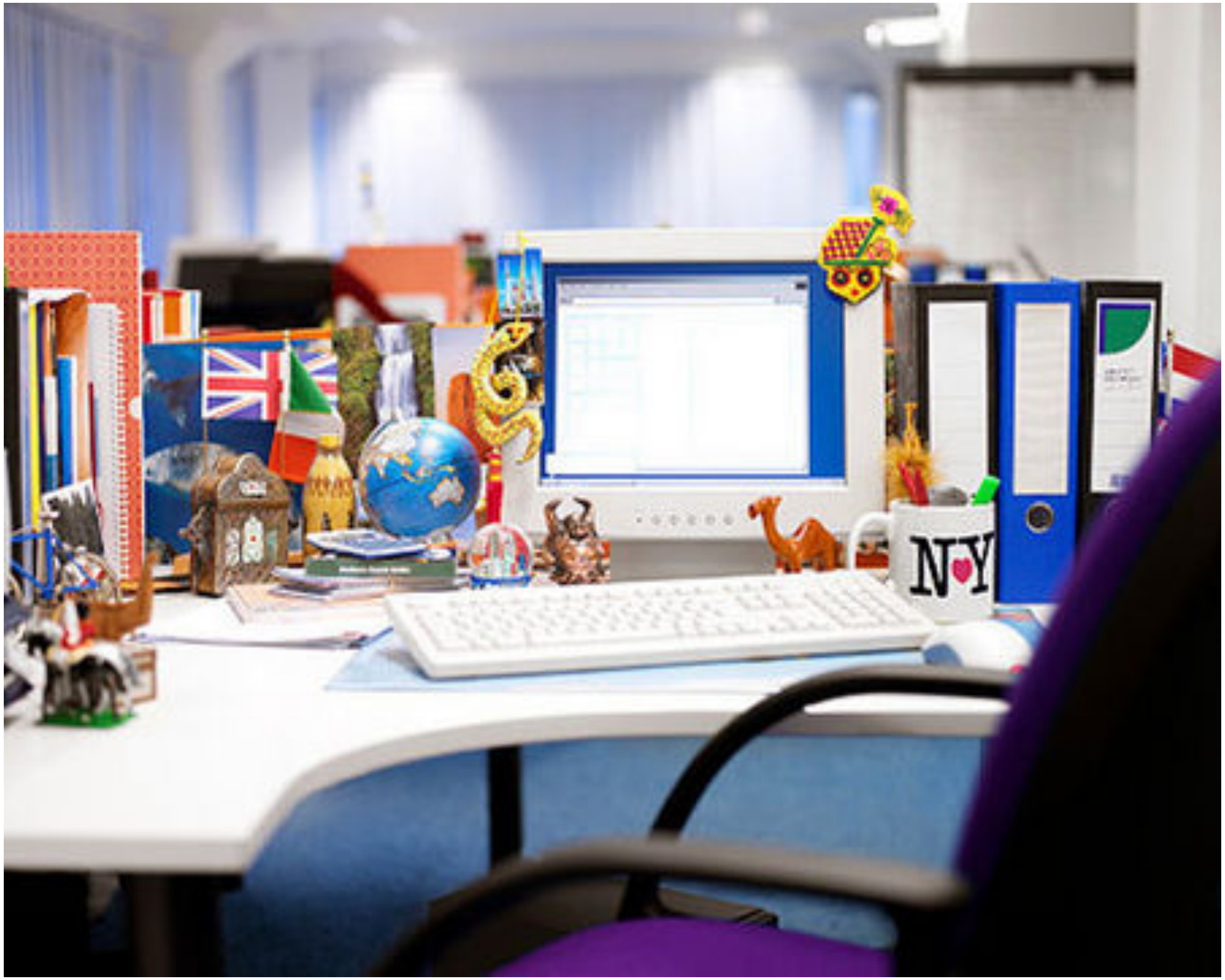
What can we learn by looking at this person’s car?

Sometimes you can learn a lot just by passively observing



My favorite

Sometimes you can learn a lot just by passively observing



What can we learn by looking at this person's desk?

Also observe

- Clothing
- Entries/Exits
- Entry requirements
- Perimeter security
- Security staff
- Lobby setup

Being a little more active can sometimes reveal more information

Eavesdropping

Shoulder surfing

Dumpster diving

Baiting

Tailgating

Social media can give away a lot of useful information to a social engineer

Linked In

- Job history
- Education
- Clubs/achievements
- People who endorse you or you endorse

Facebook

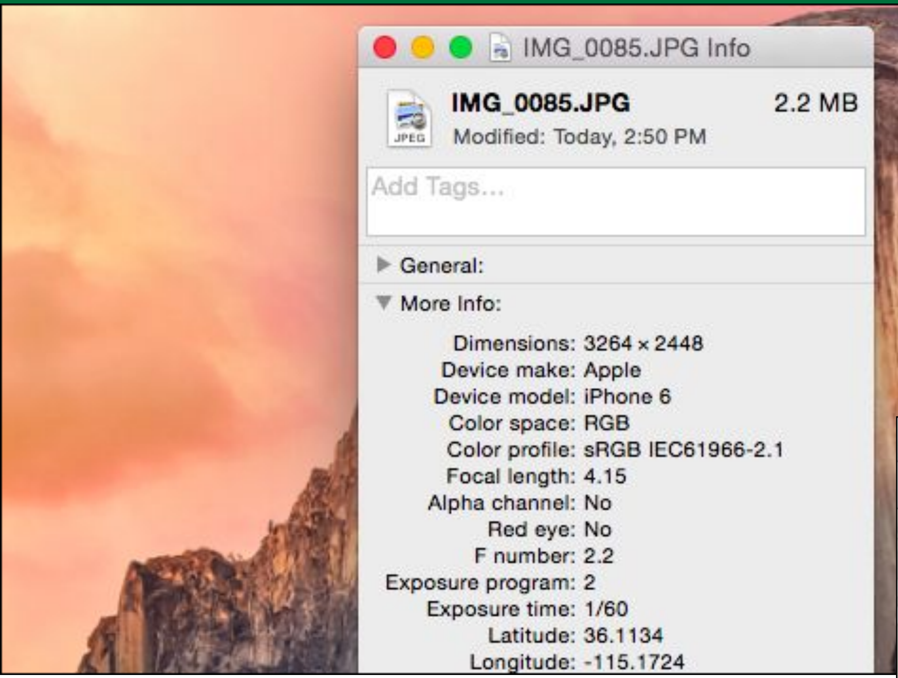
- Friends/family
- Music/movies
- Vacations
- Clubs
- Lots more

Twitter

- What you are doing now
- Geolocation
- Emotional state
- Eating habits

Other sites such as pipl aggregate information from many sources

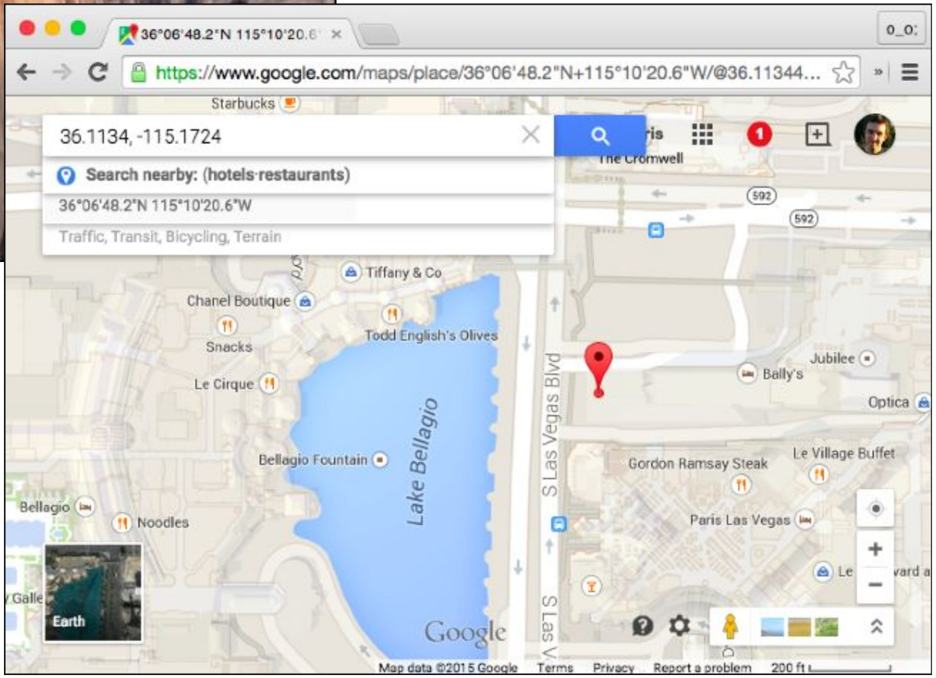
Photos posted often include latitude and longitude of where the photo was taken



IMG_0085.JPG 2.2 MB
Modified: Today, 2:50 PM

Dimensions: 3264 × 2448
Device make: Apple
Device model: iPhone 6
Color space: RGB
Color profile: sRGB IEC61966-2.1
Focal length: 4.15
Alpha channel: No
Red eye: No
F number: 2.2
Exposure program: 2
Exposure time: 1/60
Latitude: 36.1134
Longitude: -115.1724

EXIF data



https://www.google.com/maps/place/36°06'48.2"N+115°10'20.6"W/@36.11344…

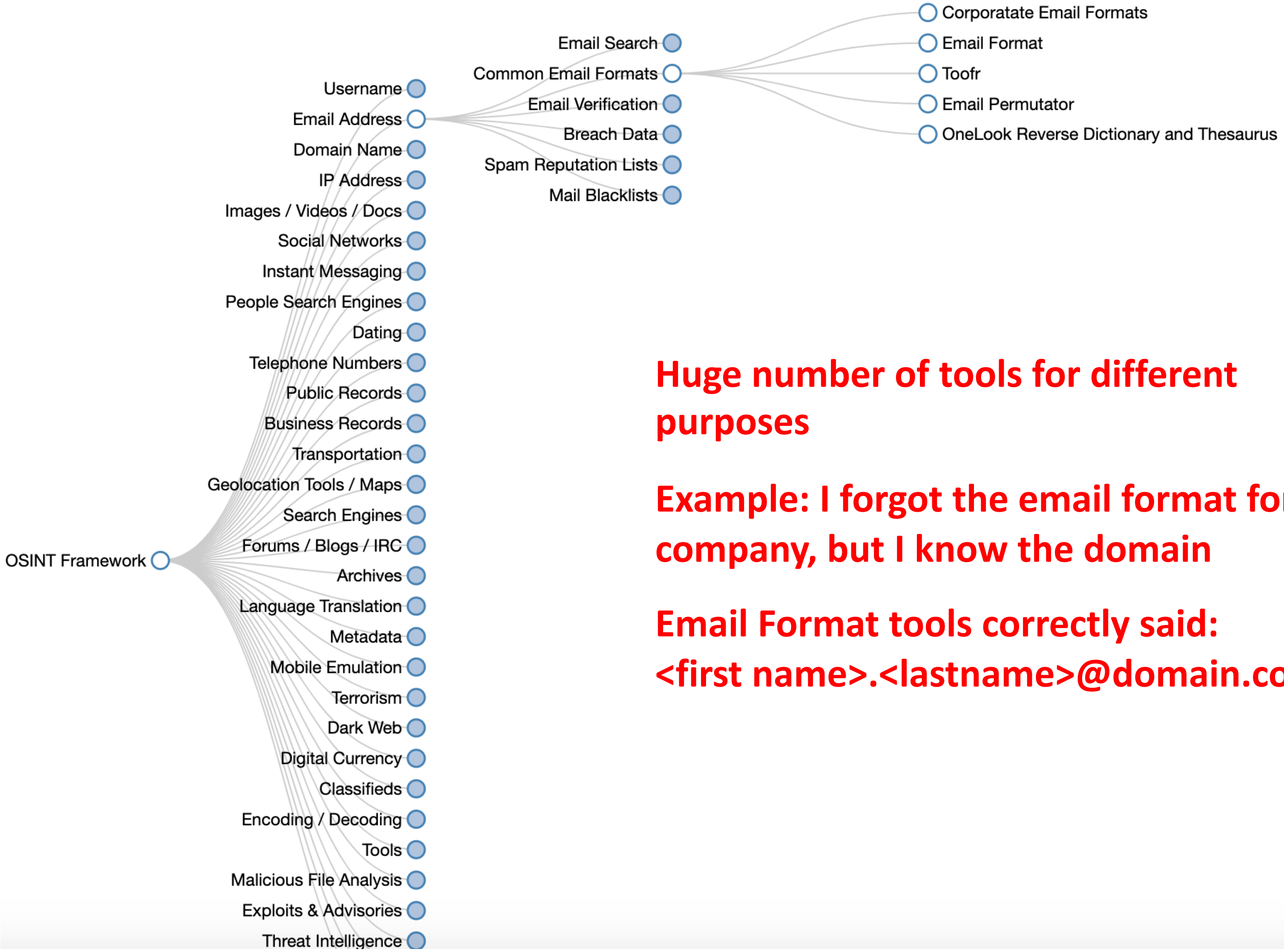
36.1134, -115.1724

36°06'48.2"N 115°10'20.6"W

Facebook strips EXIF out (but saves it for its own purposes)

https://www.howtogeek.com/211427/how-to-see-exactly-where-a-photo-was-taken-and-keep-your-location-private/

The OSINT Framework provides links to large number of tools



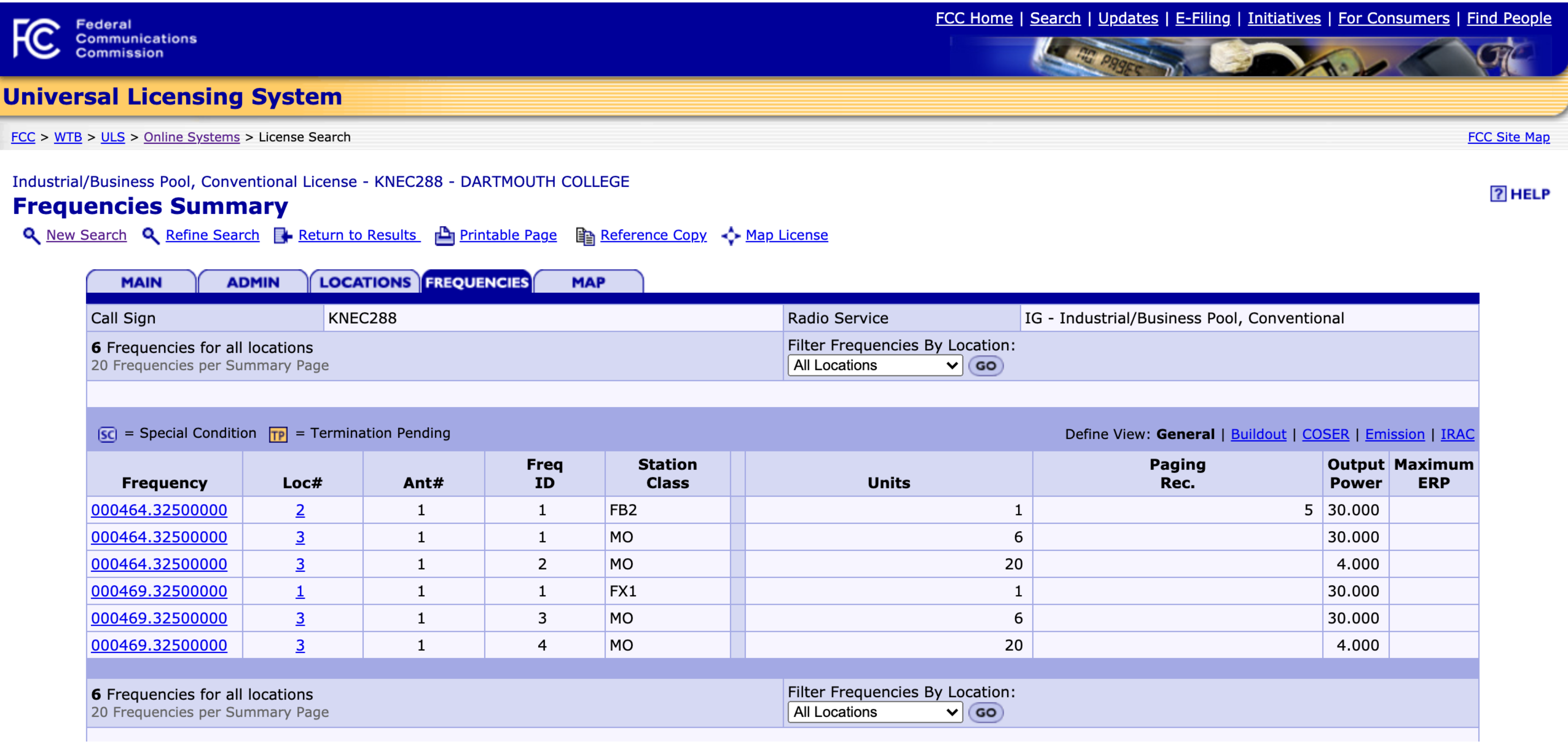
Huge number of tools for different purposes

Example: I forgot the email format for a company, but I know the domain

Email Format tools correctly said: <first name>.<lastname>@domain.com

https://osintframework.com/

OSINT example: what frequencies does a company use for its wireless comms?



Federal Communications Commission
FCC Home | Search | Updates | E-Filing | Initiatives | For Consumers | Find People

Universal Licensing System

FCC > WTB > ULS > Online Systems > License Search

FCC Site Map

Industrial/Business Pool, Conventional License - KNEC288 - DARTMOUTH COLLEGE

Frequencies Summary

? HELP

New Search | Refine Search | Return to Results | Printable Page | Reference Copy | Map License

MAIN | ADMIN | LOCATIONS | FREQUENCIES | MAP

Call Sign	KNEC288	Radio Service	IG - Industrial/Business Pool, Conventional
6 Frequencies for all locations 20 Frequencies per Summary Page		Filter Frequencies By Location: All Locations GO	

SC = Special Condition TP = Termination Pending

Define View: **General** | Buildout | COSER | Emission | IRAC

Frequency	Loc#	Ant#	Freq ID	Station Class		Units	Paging Rec.	Output Power	Maximum ERP
000464.32500000	2	1	1	FB2		1	5	30.000	
000464.32500000	3	1	1	MO		6		30.000	
000464.32500000	3	1	2	MO		20		4.000	
000469.32500000	1	1	1	FX1		1		30.000	
000469.32500000	3	1	3	MO		6		30.000	
000469.32500000	3	1	4	MO		20		4.000	

6 Frequencies for all locations
20 Frequencies per Summary Page

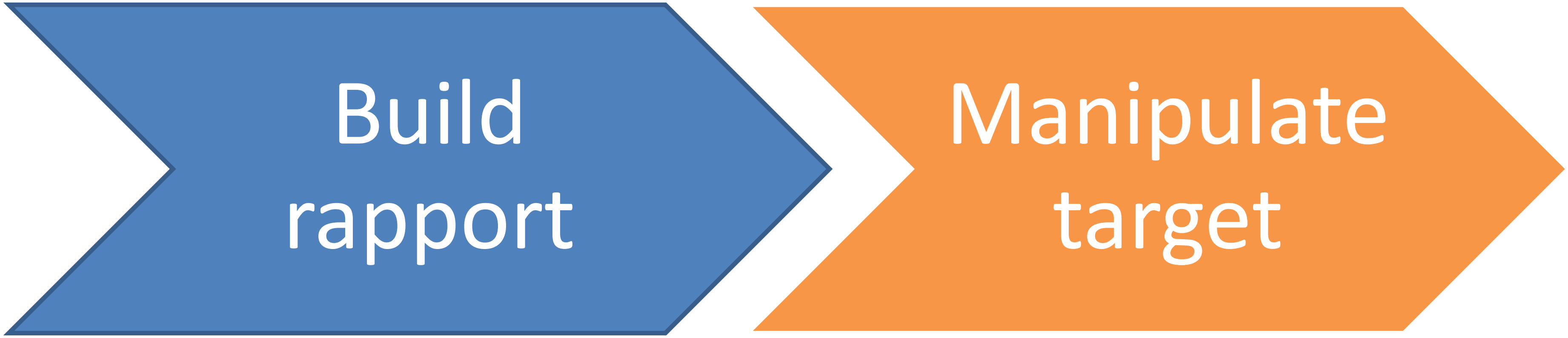
Filter Frequencies By Location:
All Locations GO

https://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp; search By Name

Agenda

1. Open-Source Intelligence (OSINT)
2. Social engineering
3. Defenses

During execution, social engineers first build rapport, then manipulate target


Build rapport

Manipulate target

Sometimes social engineers make contact indirectly

Indirect approaches

- Phishing
- Spear phishing
- Vishing
- SMiShing

Rely on OSINT gathered information to make convincing presentation

Do not make the mistake of thinking people who fall for this are dumb!

Whether direct or indirect contact, building rapport with the user is important

User's questions

- Who is this person?
- What does this person want?
- Is this person a threat?
- How long will this take?

Good social engineers pre-plan answers to these questions

Try to develop rapport

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Discussion: what is rapport?

What is rapport and how do you build it?

- Building a bridge for communications based on trust and common interests

10 principles for building rapport

10 principles for building rapport

1. Artificial time constraints
2. Accommodating nonverbals
3. Using a slower rate of speech
4. Employing sympathy or assistance
5. Suspending your ego
6. Validating others
7. Asking how, why, and when questions
8. Quid pro quo
9. Employing reciprocal altruism
10. Managing expectations

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

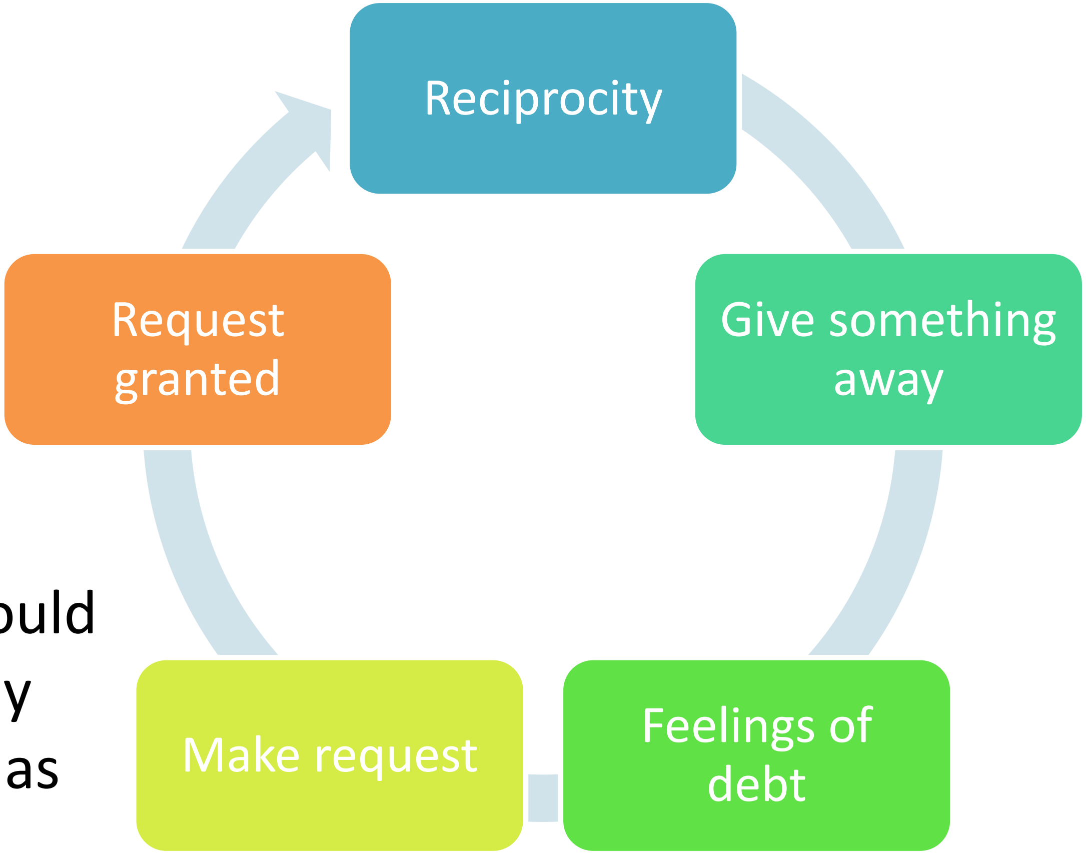
Once rapport is built, social engineers move on to manipulation

Principles for manipulation

1. Reciprocity
2. Obligation
3. Concession
4. Scarcity
5. Authority
6. Consistency and commitment
7. Liking
8. Social proof

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

1) Reciprocity: if given a favor, people often feel the need to pay it



Thing given away can be as simple as a compliment

Request should have roughly same value as the gift

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

2) Obligation: like reciprocity but based on social norms

Let someone go in front of you in traffic merge

What must they do?

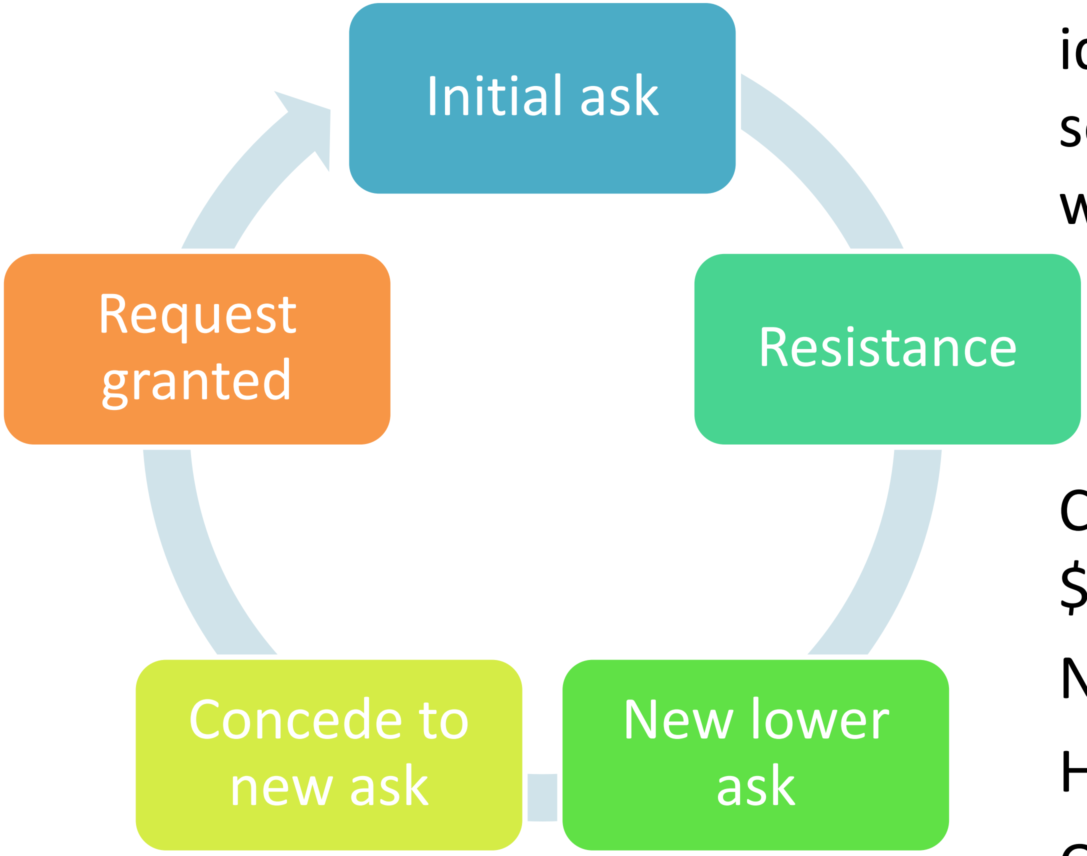
What if they don’t?

Social engineering attempting to get through a door

Carry a box!

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

3) Concession: ask for something large, but settle for what you really want



Makes people feel like it was their idea to take action social engineer wants

Can you donate $250 to our cause?

No way!

How about $25?

Ok

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

4) Scarcity: the value of something increases if it is scarce

Know CEO is out

- I have to fix his computer before he gets back
- I can’t get access to it? I’m busy and it’ll be four days until I can get back
- Sign here to acknowledge that I came to fix it, but you wouldn’t let me in

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

5) Authority: people tend to follow those who (appear to be) in charge

Looks the part

- Appearance provides a level of trust without proof
- Doctors have specialized knowledge, so we tend to do what they ask
- Wearing a suit signals importance in some places

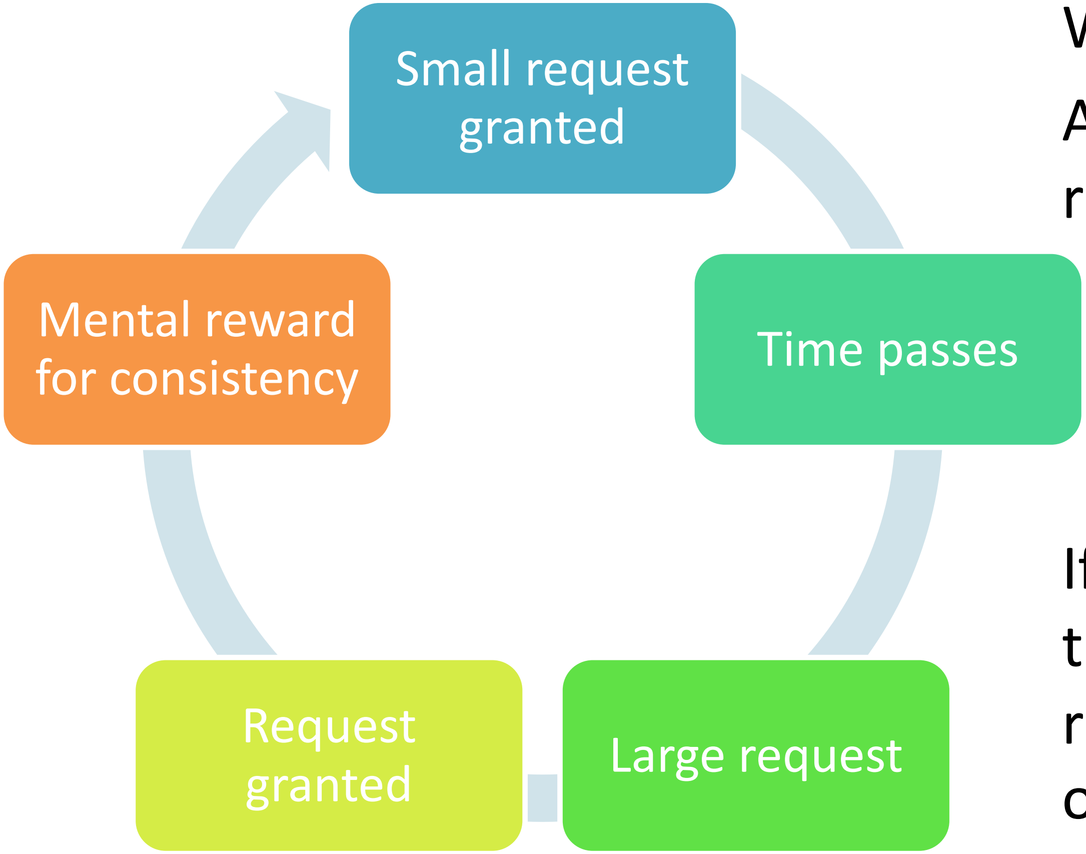
Milgram experiment

- Subjects told to shock people if they gave incorrect answers
- If subject objected, someone in lab coat said, “The experiment must go on, please continue”
- 65% of subjects increased voltage

Many people want to be helpful

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

6) Consistency and commitment: start small, ask for more, then more, then …



Get a small request granted

Wait

Ask for a larger related request

If pushback, remind them that the smaller, related request was granted, this one should be also

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

7) Liking: people tend to like people who like them (and are like them)

Liking must be genuine

Compliments are not the same as liking

Nonverbal signals play a huge role

Be genuinely interested

Don’t abruptly stop when you get what you want

Honeypot: extreme example

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

8) Social proof: people tend to do what others are doing

Every in an elevator looking at back of the elevator

New people (not in the joke) will look at the back also

Call two people, give same info

Later say you can check with (opposite person), they'll confirm this

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Social engineers in the real world are sometimes aggressive

3B's

Burglary

- Not exactly social engineering
- Defenses tested by "red teams"
- We will cover physical security soon

Bribery

- Get someone to take action for you or provide information
- Doesn't have to have an explicit change of cash

Blackmail

- Learn something about a person
- Threaten to expose the person unless they do as asked
- Extortion

Agenda

1. Open-Source Intelligence (OSINT)

2. Social engineering

➡ 3. Defenses

Discussion

What can be done to mitigate social engineering success?

Develop a Mitigation and Prevention Plan

Step 1: Learn to identify social engineering attacks

Step 2: Develop actionable and realistic policies

Step 3: Perform regular real-world check ups

Step 4: Implement applicable security awareness programs

Hadnagy, Christopher. *Social engineering: The science of human hacking*. Second edition. John Wiley & Sons, 2018.

Social engineering attacks often have common signs

Common signs of social engineering

- A tremendous sense of urgency or crisis
- Pressure to bypass or ignore security policies or procedures you are expected to follow
- Requests for sensitive information they should not have access to or should already know, such as your account numbers
- An email or message from a friend or coworker that you know, but the message does not sound like them
- An email that appears to be from a coworker or legitimate company, but the email is sent using a personal email address such as @gmail.com
- Playing on your curiosity or something too good to be true

If you suspect social engineering, stop communicating with the person

Report contact/ warn others

Remember, common sense is your best defense

https://www.sans.org/security-awareness-training/resources/social-engineering-attacks