
# Exploits in Wetware

**Defcon 25 – 2017: CTF @ SE Village Experience**

*Defending Against Social Engineering*

# Robert Sell
## Senior IT Manager | Aerospace Industry


@robertesell

robertsell@protonmail.com

www.linkedin.com/in/robertsell

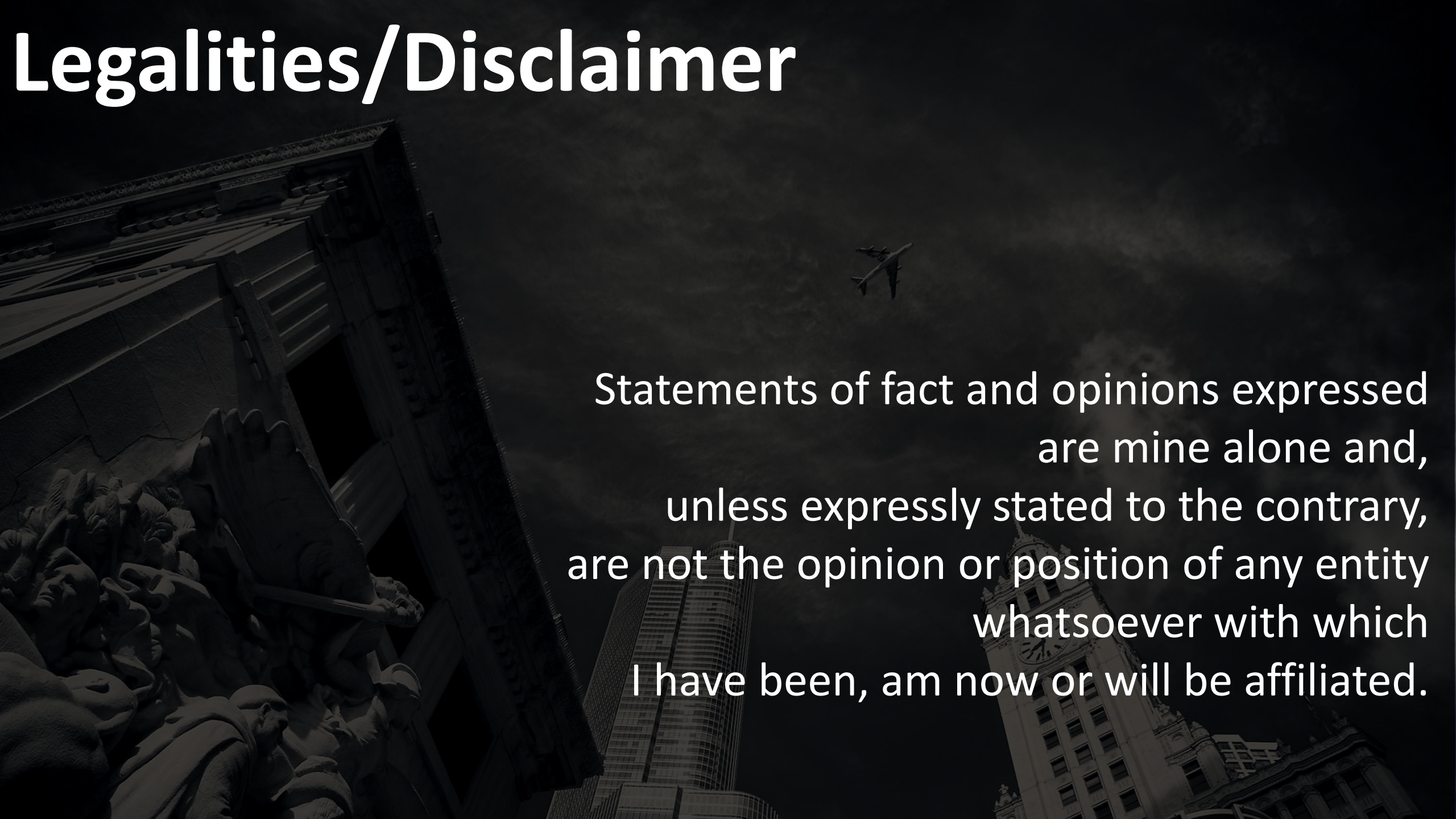
www.patreon.com/robertsell


# Value Proposition

- Social Engineering Insights
- Defcon SE CTF Understanding
- OSINT & Vishing Basics
- Social Engineering Tricks
- Pretexts That Work
- How to Defend against SE Attacks
- Tools

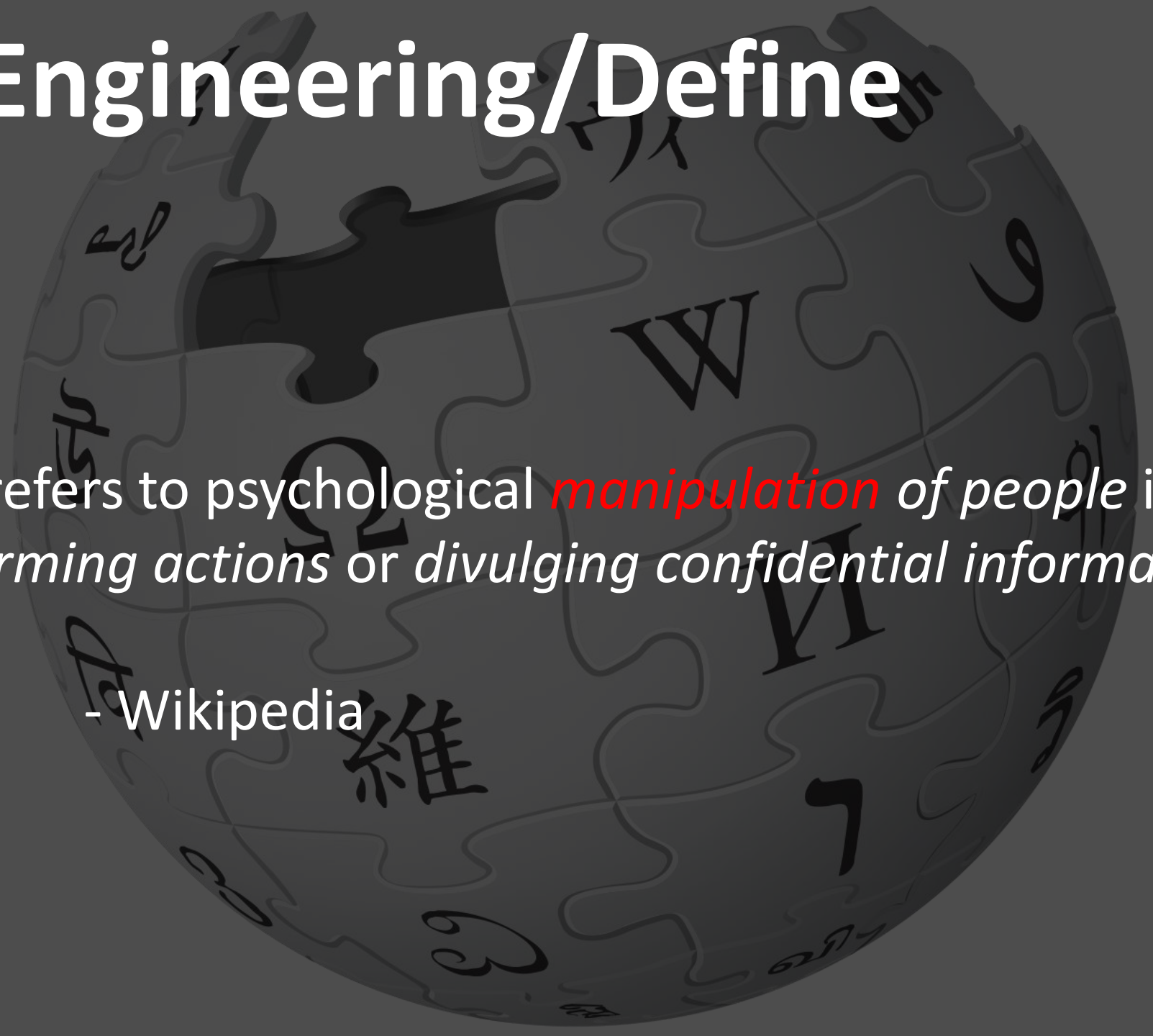
YOU BETTER HURRY UP AND START BEING AWESOME
BECAUSE I'M NOT WAITING FOR YOU

# Legalities/Disclaimer



Statements of fact and opinions expressed
are mine alone and,
unless expressly stated to the contrary,
are not the opinion or position of any entity
whatsoever with which
I have been, am now or will be affiliated.

# Social Engineering/Define



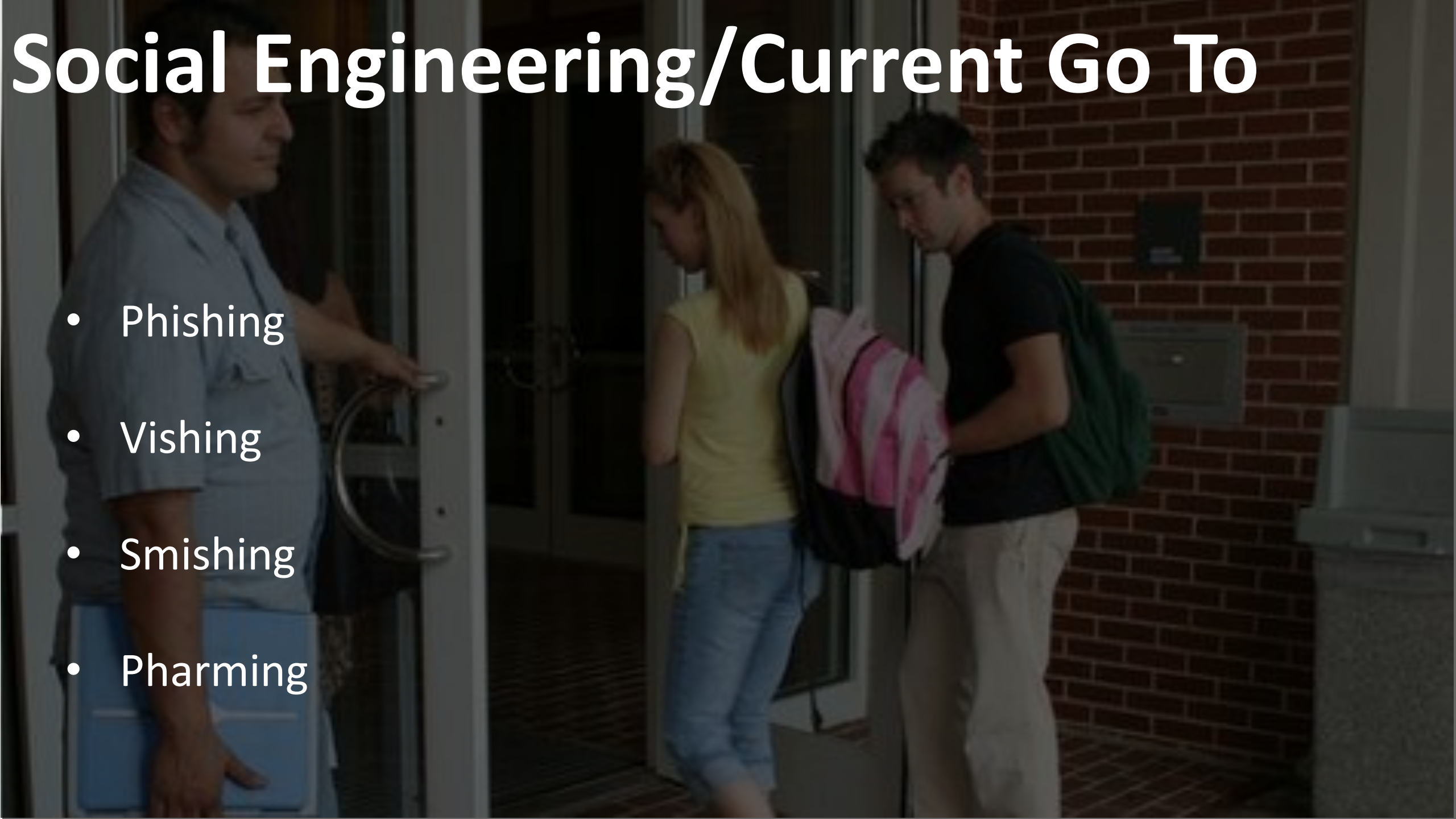
"…refers to psychological *manipulation* *of people* into *performing actions* or *divulging confidential information*."

- Wikipedia

# Social Engineering/Golden Oldies

- Impersonation
- Tailgating
- Shoulder surfing
- Dumpster diving

# Social Engineering/Current Go To



- Phishing
- Vishing
- Smishing
- Pharming

# Social Engineering/What's Next

- Social Media Impersonation
- Social Engineering as a Service (SEaS)
- Virtual Kidnaping
- Whaling (your executive)

# Social Engineering/Origin Story


## Sales (& Marketing)

Salesmen already made social engineering into a science.
Experts at changing human perception and ultimately behavior.

# Social Engineering/Trend

- 2017 Verizon Report: 90% of breaches involve social engineering.
- "Social" trend is *very* steep. Even vendors quote 20%.

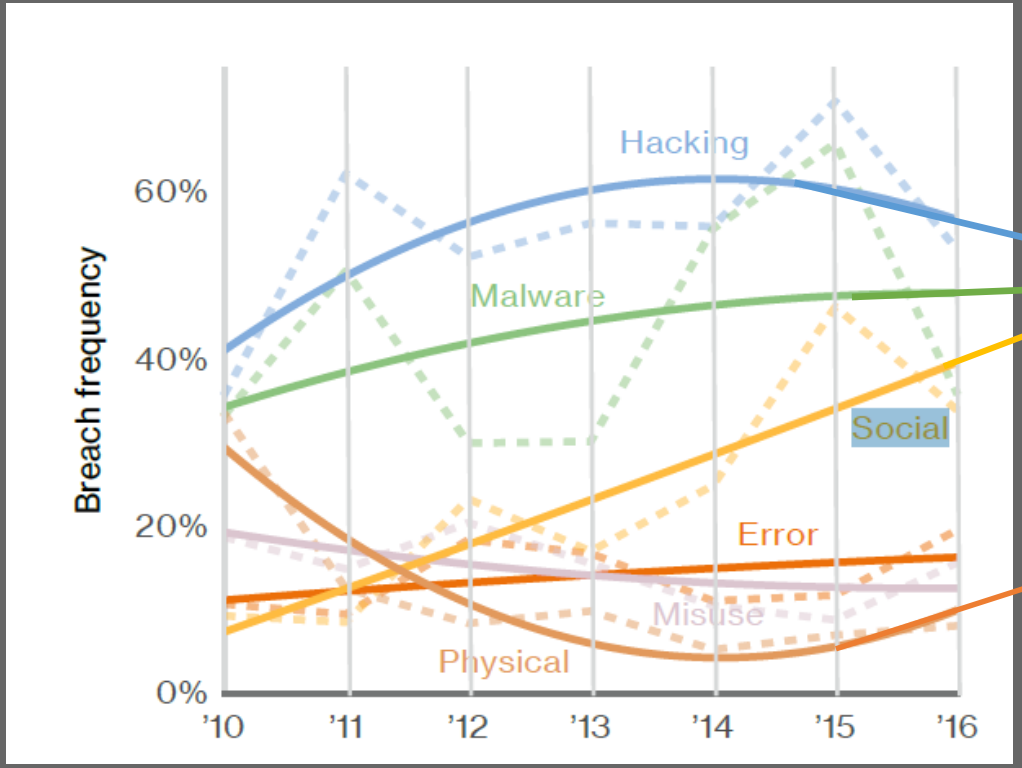


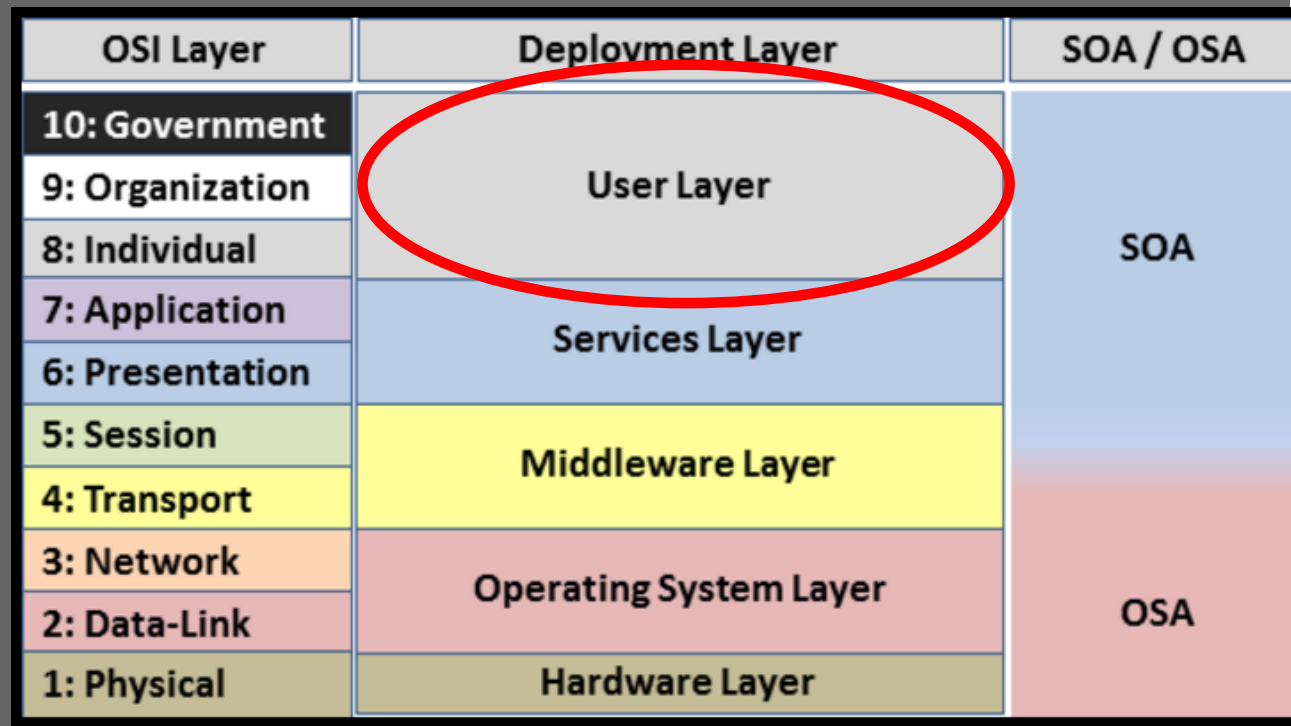




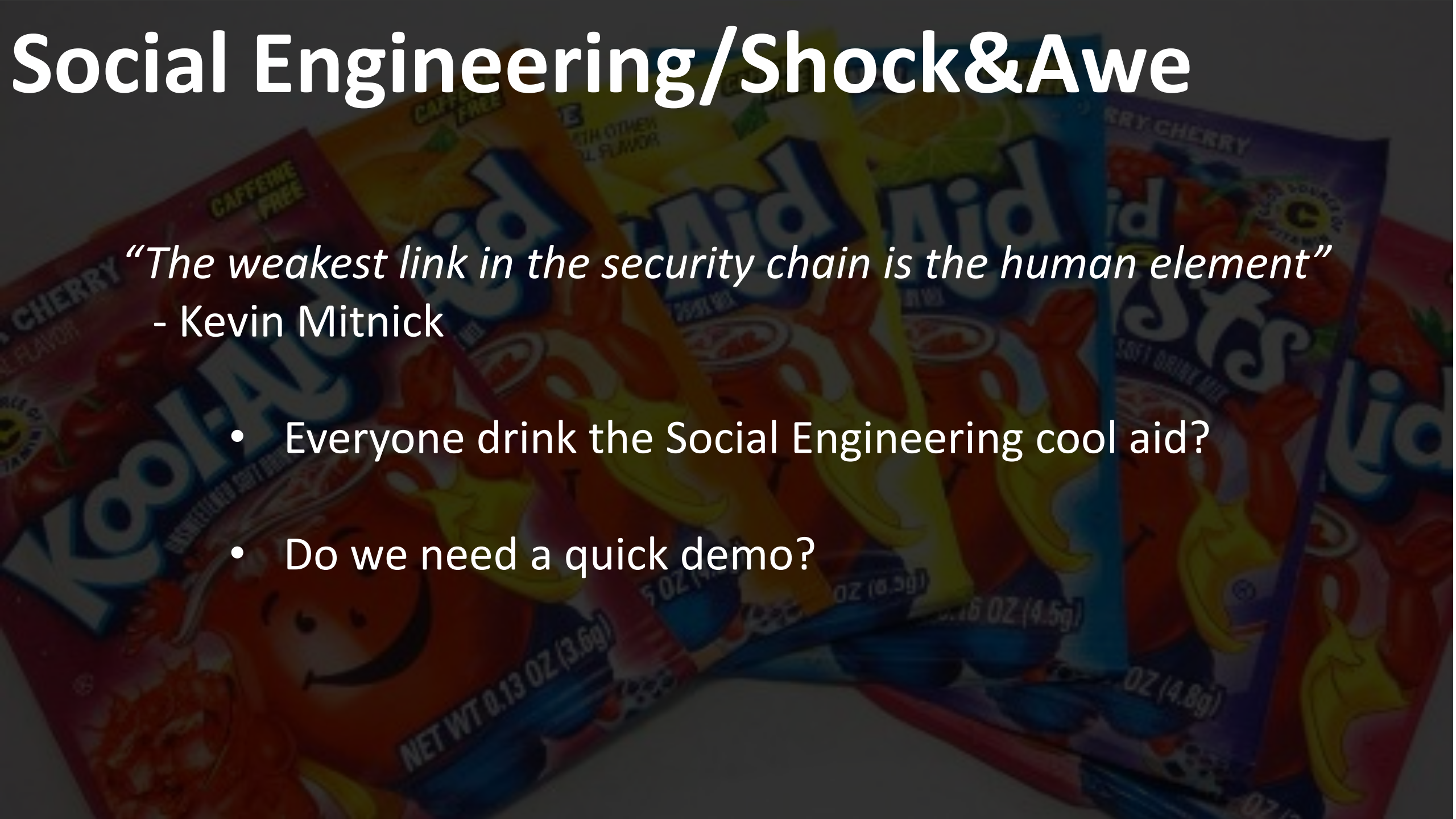
**Chart source: DBIR 2017 Verizon Report – Page 7**

# Social Engineering/Models

- The infamous OSI model: time to acknowledge the human.
- “User Layer” is a cost effective target.
- Just ask for the password (and they will give it to you).



# Social Engineering/Shock&Awe



*"The weakest link in the security chain is the human element"*
- Kevin Mitnick

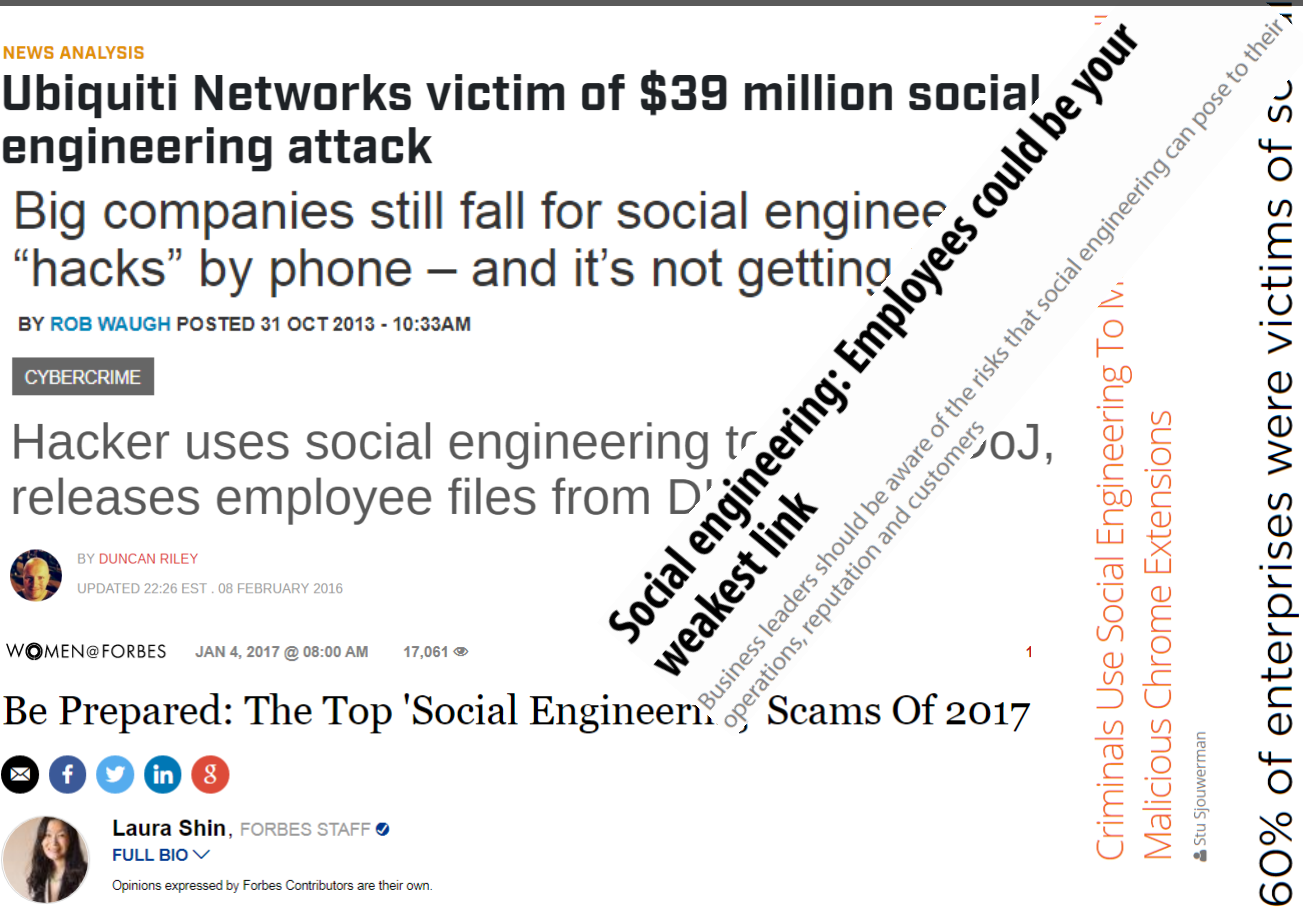
- Everyone drink the Social Engineering cool aid?
- Do we need a quick demo?

# I am sorry!

Can we move on?

# Social Engineering/News

If you still doubt the power of social engineering, just Google it.







# Defcon/Define

- Defcon 24 – 2016 was my first Defcon.

- Not actually a conference. More like attending Burning Man.
  - Villages, CTFs, workshops, talks, parties, BBQs, gun shooting, line ups and spontaneous events….
  - Very little support structure (ie. no formalized lunches).
  - Read the 10 Principles of Burning Man to understand Defcon

- Defcon is whatever you make of it.

# Defcon SE CTF/Application

- Amazed by the SE Village. Promised myself I would apply.
- Hundreds of people apply. Make an “interesting” video.


DefCon 25 2017 Social Engineering Village CTF - Audition Video

https://youtu.be/dCC7k4C0YMg

# Defcon SE CTF/Application

**Holy Crap! I'm in!**

Now 3 Weeks to do OSINT. Goodbye weekends and evenings....

**SECTF Team** <sectf@social-engineer.org> May 29

to Chris

Contestants,

You have been chosen to participate in the SECTF at DEF CON 25. We are really excited but we need your help.

1. Please confirm you accept this invitation
2. To solidly confirm your spot you need to pay us a $20 FULLY REFUNDED payment. How do you get it refunded? When you show up at DEF CON to get in the booth we will give you a crisp $20 bill + some schwag. (Crispness not guaranteed)
3. We need this done in the next 48 hours of we will choose someone else please
4. You will receive your packets and notice right after.

Thank you

You can:

1. Paypal $20 marked as SECTF Reg to logan@social-engineer.org
2. Or by CC here: https://www.social-engineer.com/store/#!/DEF-CON-25-SECTF-Registration-Fee/p/24671879/category=0

Thank you and we can't wait to see you at DEF CON 25.

# Defcon SE CTF/Stages

**Stage 1: OSINT - 3 Weeks – At home (6,000 minutes)**

- Comprised of 16 competitors
- Everyone has own target but part of a common industry
- 29 flags to capture. Points for quality of report
- NO ENGAGEMENT

RECON

**Stage 2: Vishing – Live at Defcon – (20 minutes)**

- Takes place over 2 days at the SE Village at Defcon
- Same flags but can get points for each person
- Winner captures the most “flags” hence CTF

ATTACK

# OSINT/Flags

Capturing “the Flags”

- Logistics: Cafeteria
- Tech: VPN
- Onsite: Janitorial service
- Company Tech: OS
- Employee Info: Tenure

| Logistics | Rpt Pts | Call Pts |
|---|---|---|
| Is IT Support handled in house or outsourced? | 3 | 6 |
| Who do they use for delivering packages? | 3 | 6 |
| Do you have a cafeteria? | 4 | 8 |
| Who does the food service? | 4 | 8 |
| | | |
| **Other Tech** | | |
| What is the name of the company VPN? | 4 | 8 |
| Do you block websites? | 2 | 4 |
| If website block = yes, which ones? (Facebook, Ebay, etc) | 3 | 6 |
| Is wireless in use on site? (yes/no) | 2 | 4 |
| If yes, ESSID Name? | 4 | 8 |
| What make and model of computer do they use? | 3 | 6 |
| What anti-virus system is used? | 5 | 10 |
| | | |
| **Can Be Used for Onsite Pretext** | | |
| What is the name of the cleaning/janitorial service? | 4 | 8 |
| Who does your bug/pest extermination? | 4 | 8 |
| What is the name of the company responsible for the vending machines onsite? | 4 | 8 |
| Who handles their trash/dumpster disposal? | 4 | 8 |
| Name of their 3rd party or in house security guard company? | 5 | 10 |
| What types of badges do you use for company access? (RFID, HID, None) | 8 | 16 |
| | | |
| **Company Wide Tech** | | |
| What operating system is in use? | 5 | 10 |
| What service pack/Version? | 8 | 16 |
| What program do they use to open PDF documents and what version? | 5 | 10 |
| What browser and version do they use? | 6 | 12 |
| What mail client is used? | 5 | 10 |
| Do you use disk encyption, if so what type? | 5 | 10 |
| Fake URL(getting the target to go to a URL) www.seorg.org | NA | 26 |
| | | |
| **Employee Specific Info** | | |
| How long have they worked for the company? | 3 | 6 |
| What days of the month do they get paid? | 3 | 6 |
| Employees schedule information (start/end times, breaks, lunches) | 3 | 6 |
| What is the name of the phone/PBX system? | 4 | 8 |
| When was the last time they had awareness training? | 5 | 10 |
| | | |
| **Report Scoring** | | |
| Half points for any flag found from information gathering | ** | ** |
| 10 points each for each realistic attack vector detailed in the report to a maximum of 50 points. Supporting evidence must be provided for each attack vector as to why it is realistic. | 10-50 | |
| Format, structure, grammer, layout, general quality of the report a maximum of 50 points. | 0-50 | |

# OSINT/Aquire Target

- Physical (building, locations)
- Technical (websites, IP address, dns, etc)
- Corporate (registration, legal, property)
- Staff (personal information)

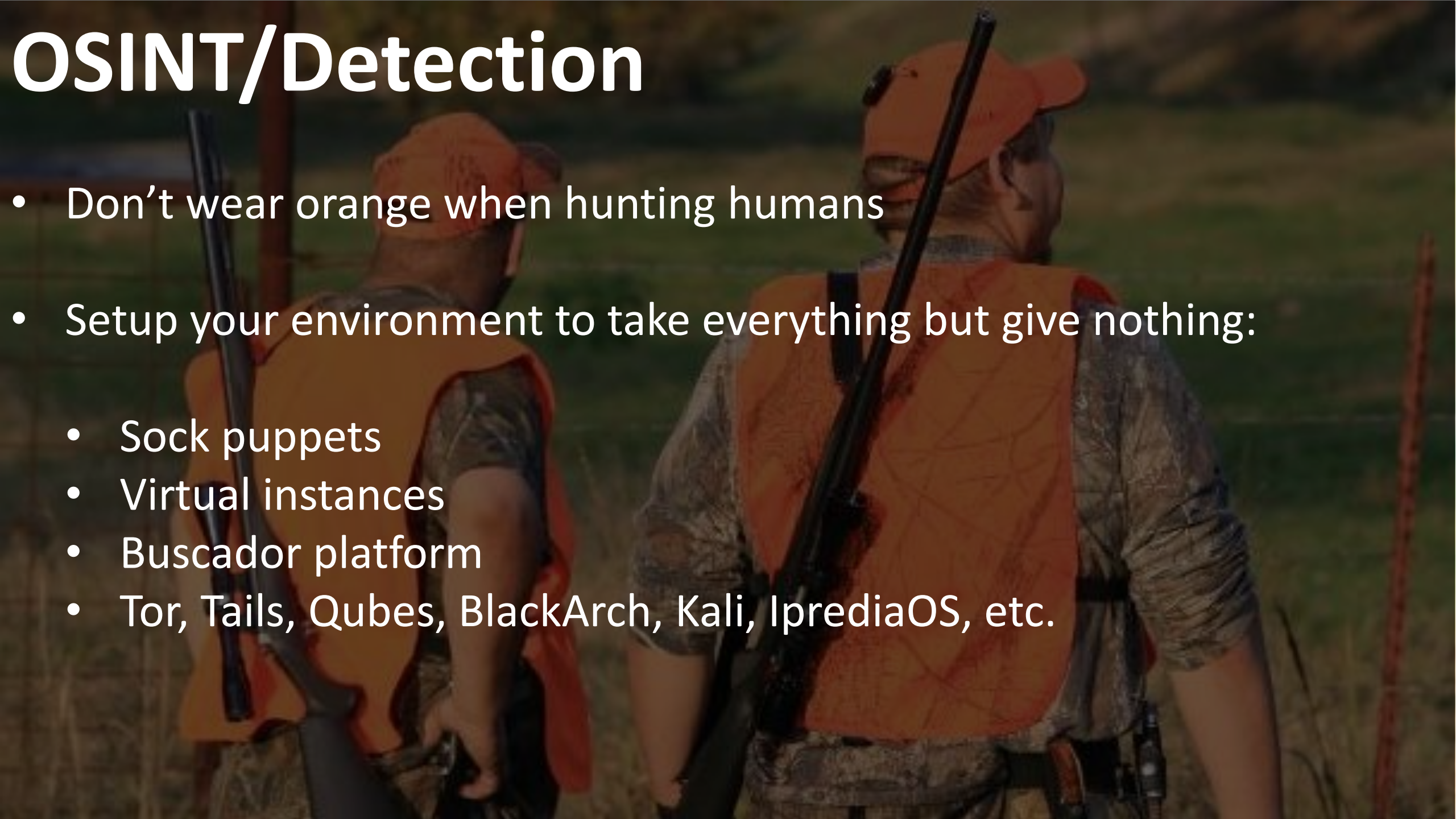
# OSINT/LinkedIn

- Corporate: Start with LinkedIn
- Search by company to get all staff
  Target rich environment
- The more connections you have
  the more you people you can see
- Get around the “free” limitations with LinkedIn XRay.
  http://recruitmentgeek.com/tools/linkedin/

# OSINT/Focus


- 80/20 rule: 20% of the people will give you 80% of the content.
- Look for the social butterflies and spend time on them.
  - Social media, friends, personal websites, etc.

# OSINT/Detection



- Don’t wear orange when hunting humans
- Setup your environment to take everything but give nothing:
  - Sock puppets
  - Virtual instances
  - Buscador platform
  - Tor, Tails, Qubes, BlackArch, Kali, IprediaOS, etc.

# OSINT/Pretext Development

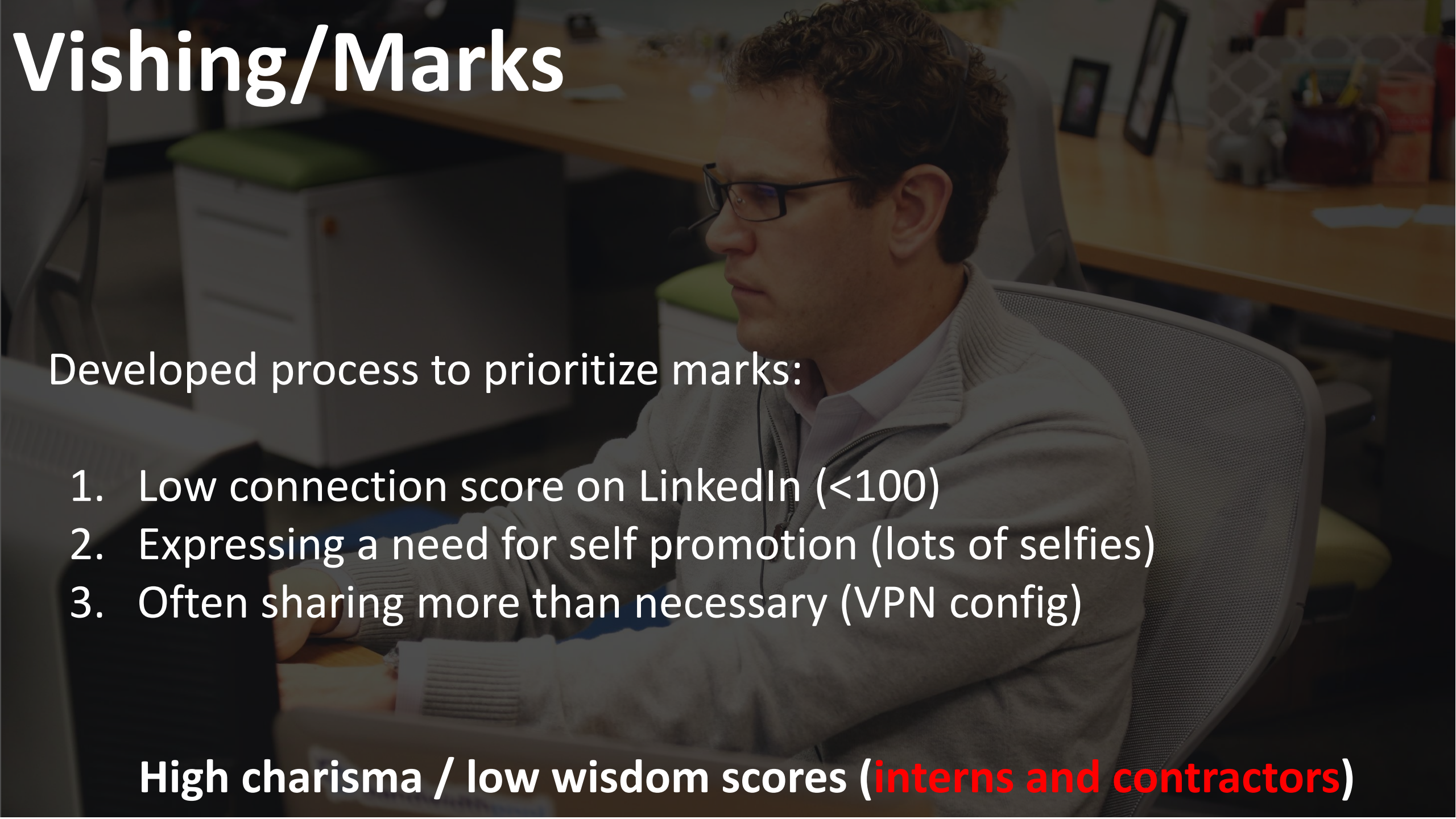
- Test out pretexts on real people. Receptionists are the best
  - Receptionists are SE defense experts
  - Always professional (even when hanging up on you)
  - Likely have kids (can say no)
  - Deal with cold calls from sales all day

# Vishing/Vegas Prep

## Going to Vegas!

- Stay outside of main Defcon hotel (Caesars).
- Comfortable shoes – You go through the casinos to get anywhere.
- Famous Defcon 3,2,1 Rule:
  - 3 hours of sleep: as a minimum so you can function.
  - 2 meals a day: plus snacks and hydration.
  - 1 shower: “con funk” is frowned upon. Bring/use deodorant.

# Vishing/Marks



Developed process to prioritize marks:

1. Low connection score on LinkedIn (<100)
2. Expressing a need for self promotion (lots of selfies)
3. Often sharing more than necessary (VPN config)

**High charisma / low wisdom scores (interns and contractors)**

# Vishing/The Room

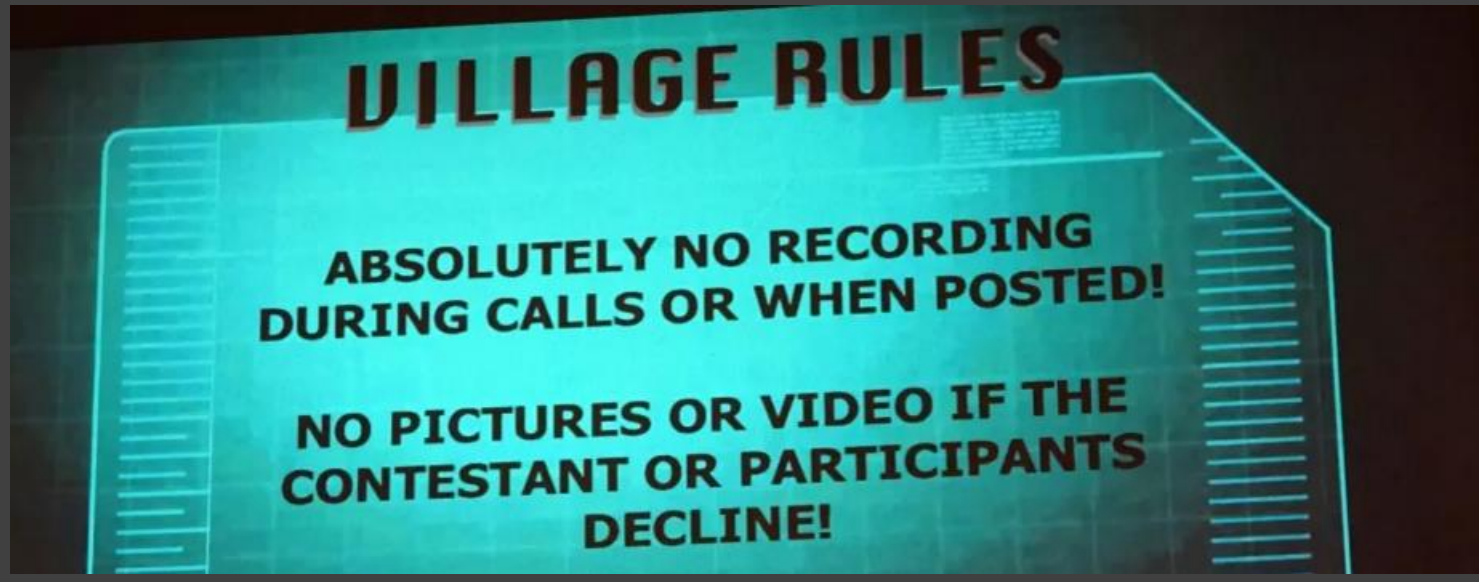

*"We don't rise* to the level of *our expectations, we fall to the level of our training."*
- Archilochus (Greek Poet)

# Vishing/The Booth

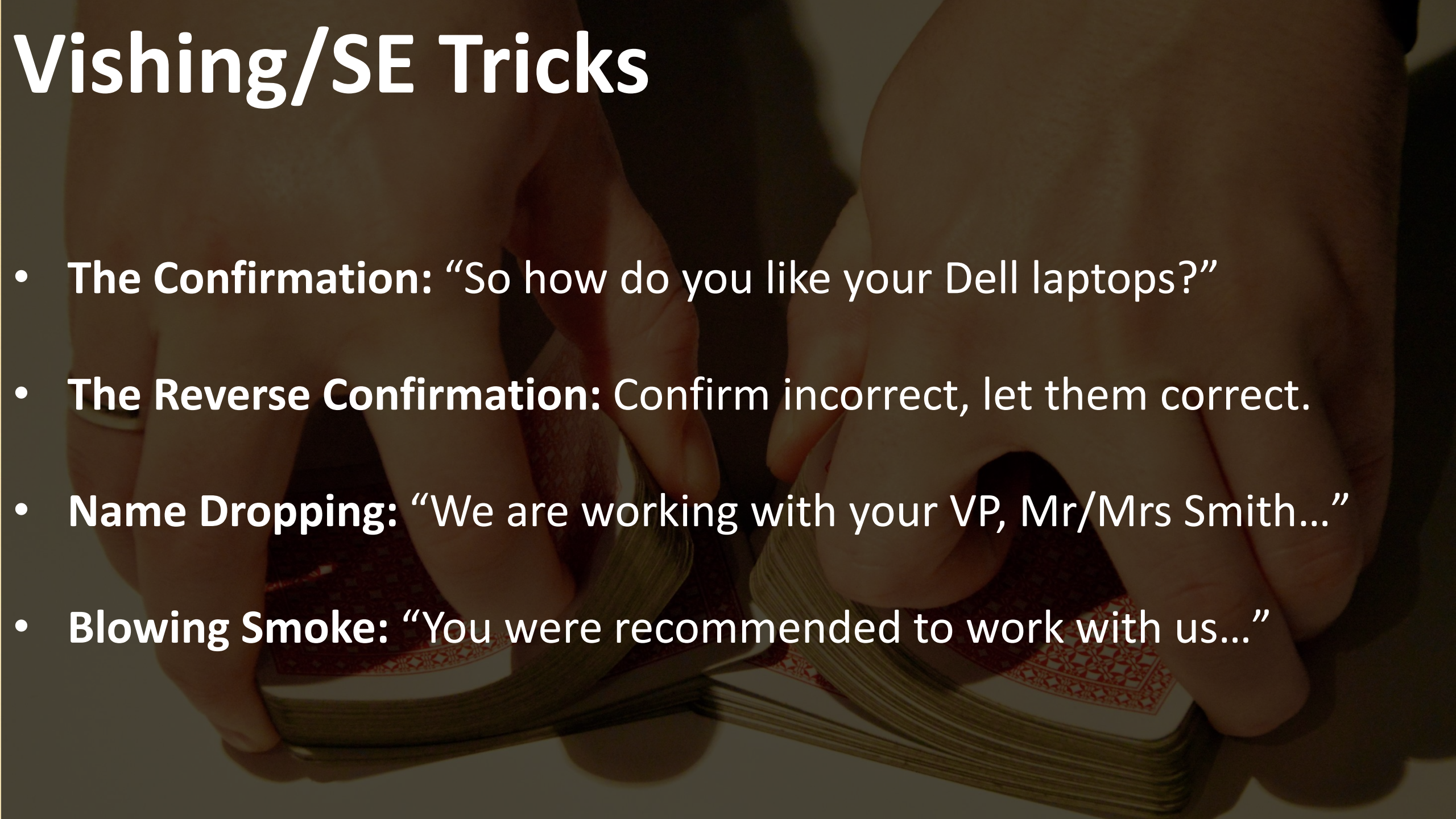
- The clock is the enemy: dialing, ringing and voicemail takes time
- Lots of “no answers” took lots of time
- Fall to sure bets: reception always answers
- Fast pretext/intro when you get someone

# Vishing/Audience Rules

- Pictures are okay if contestant approves
- No video as per State of Nevada Law
- No clapping or shouting till call ends

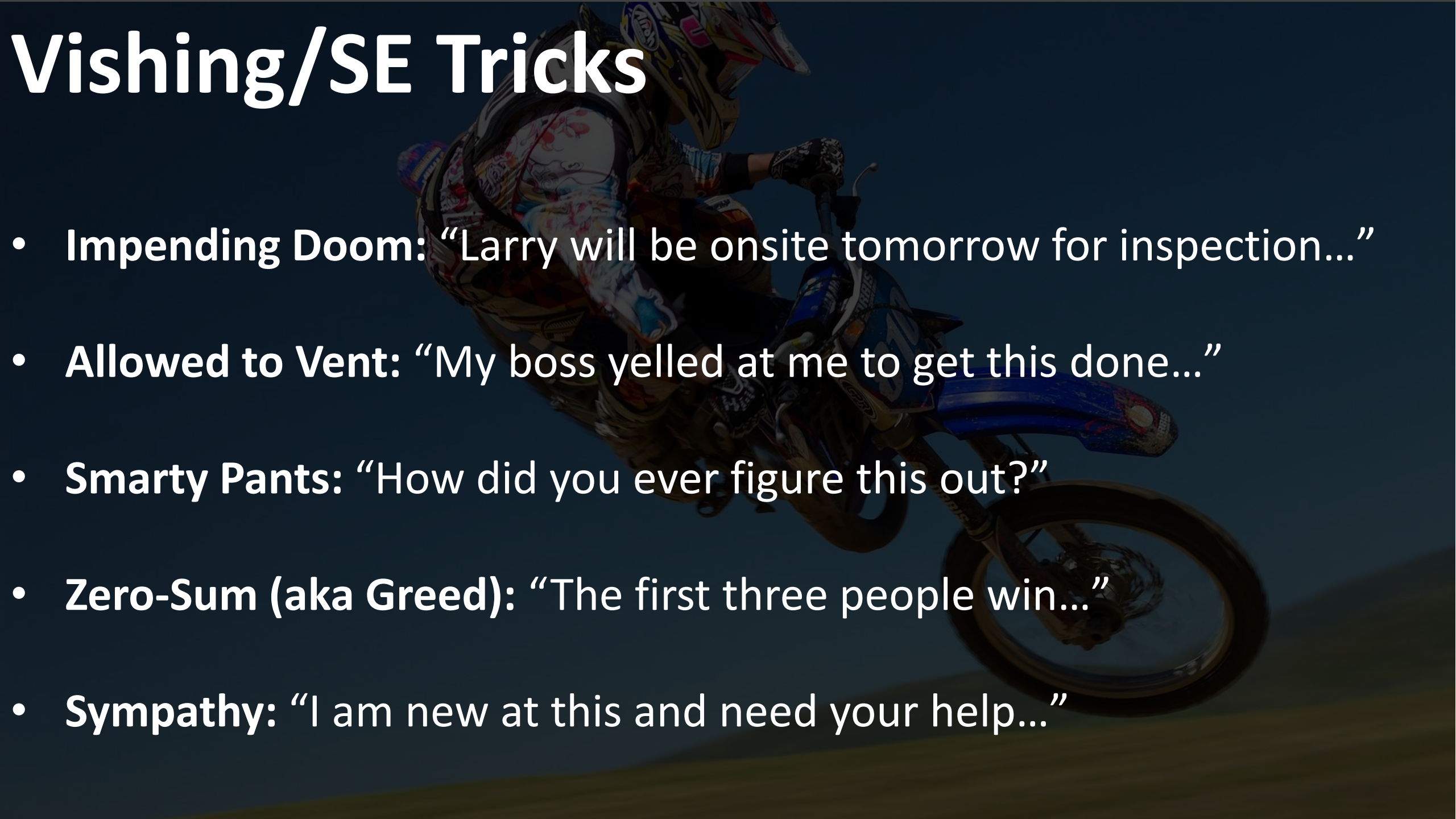


# Vishing/SE Tricks



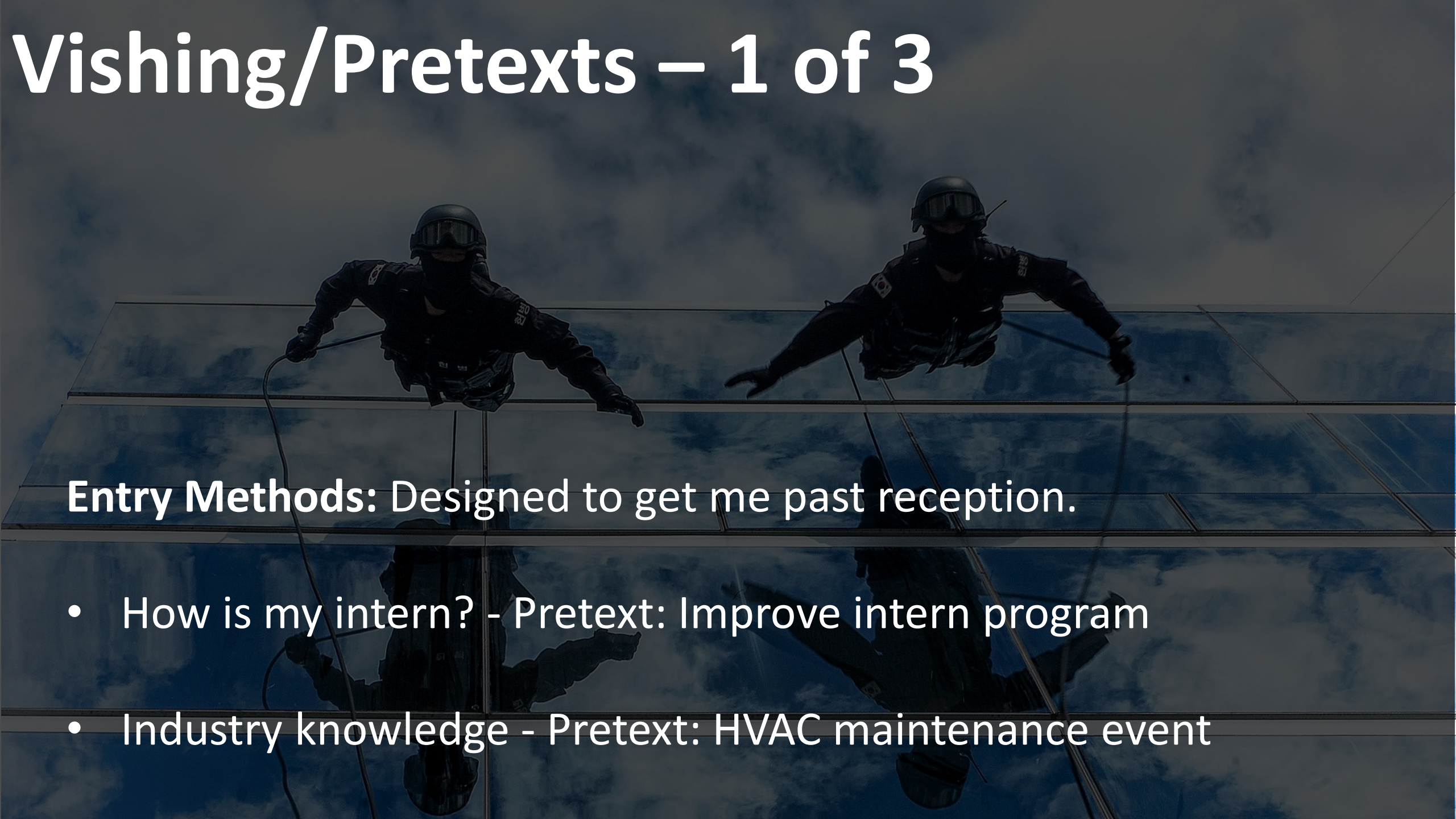
- **The Confirmation:** “So how do you like your Dell laptops?”
- **The Reverse Confirmation:** Confirm incorrect, let them correct.
- **Name Dropping:** “We are working with your VP, Mr/Mrs Smith…”
- **Blowing Smoke:** “You were recommended to work with us…”

# Vishing/SE Tricks



- **Impending Doom:** “Larry will be onsite tomorrow for inspection…”
- **Allowed to Vent:** “My boss yelled at me to get this done…”
- **Smarty Pants:** “How did you ever figure this out?”
- **Zero-Sum (aka Greed):** “The first three people win…”
- **Sympathy:** “I am new at this and need your help…”

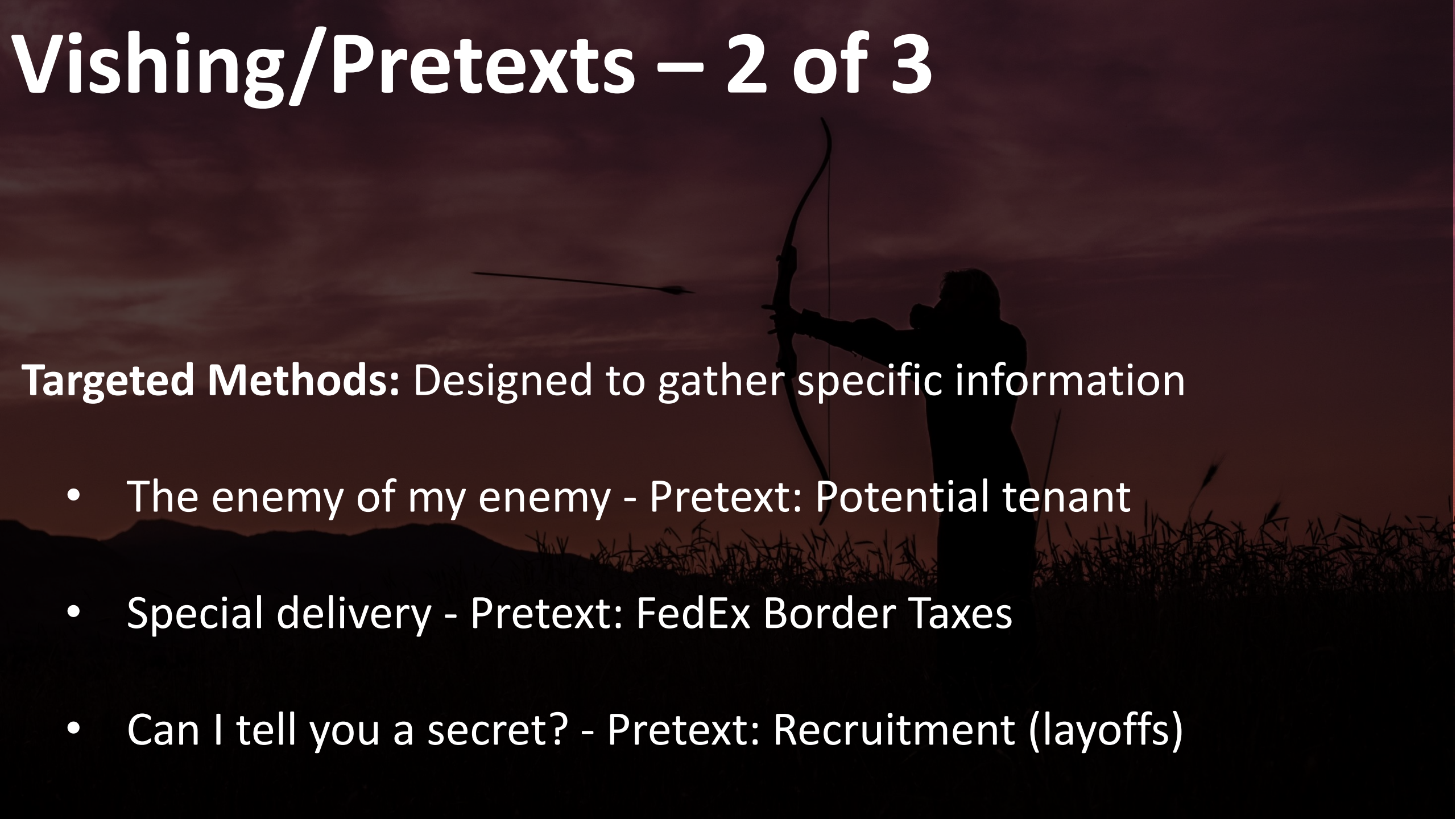
# Vishing/Pretexts – 1 of 3



**Entry Methods:** Designed to get me past reception.

- How is my intern? - Pretext: Improve intern program
- Industry knowledge - Pretext: HVAC maintenance event

# Vishing/Pretexts – 2 of 3



**Targeted Methods:** Designed to gather specific information

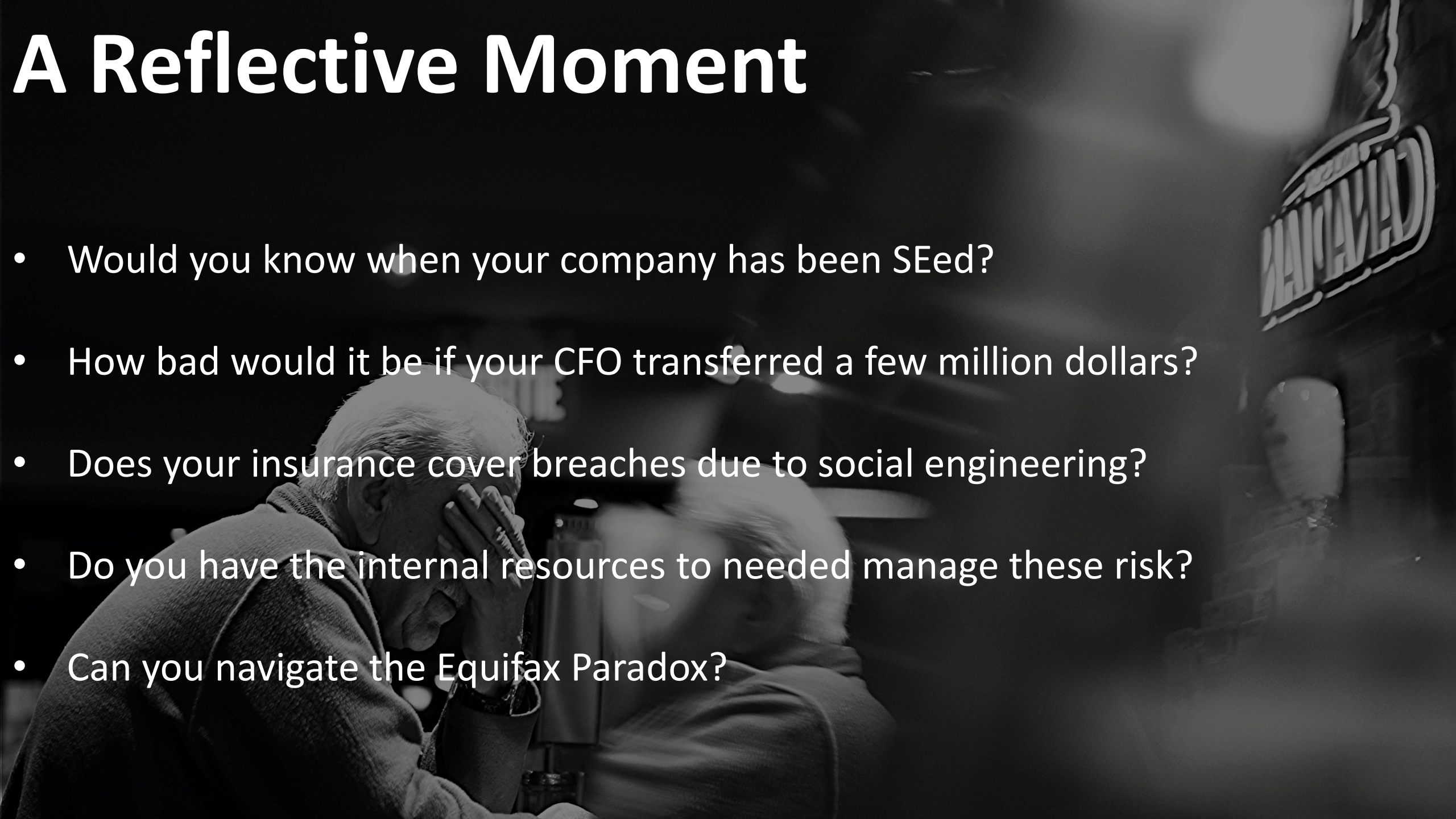
- The enemy of my enemy - Pretext: Potential tenant
- Special delivery - Pretext: FedEx Border Taxes
- Can I tell you a secret? - Pretext: Recruitment (layoffs)

# Vishing/Pretexts – 3 of 3

**Full Dump Methods:** Designed to get a lot of info.

- You’re a lucky winner - Pretext: Radio station contest
- The upgrade opportunity - Pretext: New Dell account rep
- You are special – Pretext: Employee engagement survey
- Ok you caught me - Pretext: Hired security company

# A Reflective Moment



- Would you know when your company has been SEed?
- How bad would it be if your CFO transferred a few million dollars?
- Does your insurance cover breaches due to social engineering?
- Do you have the internal resources to needed manage these risk?
- Can you navigate the Equifax Paradox?

# Recommendations

**Understand your Exposure:**

1. OSINT yourself
2. OSINT your company
3. Find the butterflies
4. Understand what’s at risk

# Recommendations

**Build up Defenses against Phishing:**

1. Phishing program:  measure clicks *and reporting*
2. Create an “EXT” tag on incoming email to stop spoofing
3. Stop allowing active links in email
4. Provide safer communications channels (Slack, Twitter, blog, etc)

# Recommendations


**Build up Defenses against Vishing:**

1. Vish your executive (with their permission)
2. Create choke points – Invest in your receptionist
3. PBX: Remove the dial by name
4. Give DIDs only to external facing (ie Sales)
5. Stop answering the phone (*unless it's your boss of course*)

# Recommendations

**Get on the Offensive:**

- No one reads your policy or cares about the annual training
- Instead create continual challenges with goals
- Communicate and advertise “program/goal of the month”
- Celebrate wins with the business – prizes!

# Recommendations

**Cultural Change:**

- Recognize we can’t win if we can’t scale
- Celebrate success far more than you punish failure
- Allow scalability through the heroes (mentors)
- Create a culture of proud protective awareness
  (Make security every employees performance metric? Silly talk!)

# Tools/Physical

- Start with physical address (all offices):
  - www.youtube.com (tour of the office?)
  - www.loopnet.com (find commercial properties)
  - www.google.ca/maps (street view, ingress/egress points)

- Ownership of property and assets, associated records (city, tax, legal).
- IoT on their cameras and other Internet facing devices (shodan)
  - Sensors, fences/gates, HVAC, ID cards

# Tools/Technical

- who.is (IP blocks, email addresses, DNS, owners, names)
- dnshistory.org
- whoisology.com
- viewdns.info/iphistory
- moz.com/researchtools/ose
- alexa.com/siteinfo
- bgp.he.net (hurricane electric: good routing info)
- www.robtex.net (graphical info)
- scans.io (Internet Scan Data Repository)
- wigle.net (wifi SSID)

# Tools/Corporate

- www.indeed.com
- www.glassdoor.com
- pastebin.com
- www.geosearchtool.com

Focus on: Their website, their receptionist(s), security guards (company), parking, CCTV, card access

# Tools/Staff

- www.linkedin.com
  - recruitmentgeek.com/tools/linkedin
- www.facebook.com
- www.twitter.com
- www.instragram.com (geolocate pictures)
- www.slideshare.com (reference letters)
- sync.me
- justice.gov.bc.ca/cso/index.do (criminal records)
- Their personal websites

# Resources

- US OSINT Resource: https://inteltechniques.com
  - Training, tools, articles, podcast, book
- Canada - OSINT Resource: https://www.toddington.com
  - Training, tools, articles
- Social Engineer: https://www.social-engineer.org
  - Training, podcast, books, SE Village organizer
- Online Training:
  - Cybrary (free), Pluralsight (paid)

# The End/Thank You

## Q&A

Twitter: @robertesell
Email: robertsell@protonmail.com
Support: https://www.patreon.com/robertsell

My next project:
www.tracelabs.org