# Exploits in Wetware

**Attack and Defense with Social Engineering**

BruCon 2018 – Robert Sell

*** V2: NEW CONTENT ***
Even More Evil Attacker Info!

# Explo Wetware

**Attack ense with Social Engineering**

BruCon 2 8 – Robert Sell

# Robert Sell - BCOM, MCP, CBCI, ITIL, CISSP [aka creep]

**Profession:** Senior IT Manager, Aerospace Industry
www.linkedin.com/in/robertsell

**Volunteer:** Coquitlam Search & Rescue: *Tracker*
www.coquitlam-sar.bc.ca

**Creator:** Nonprofit Crowdsourced OSINT for missing persons
www.tracelabs.org

**Twitter:** @robertesell

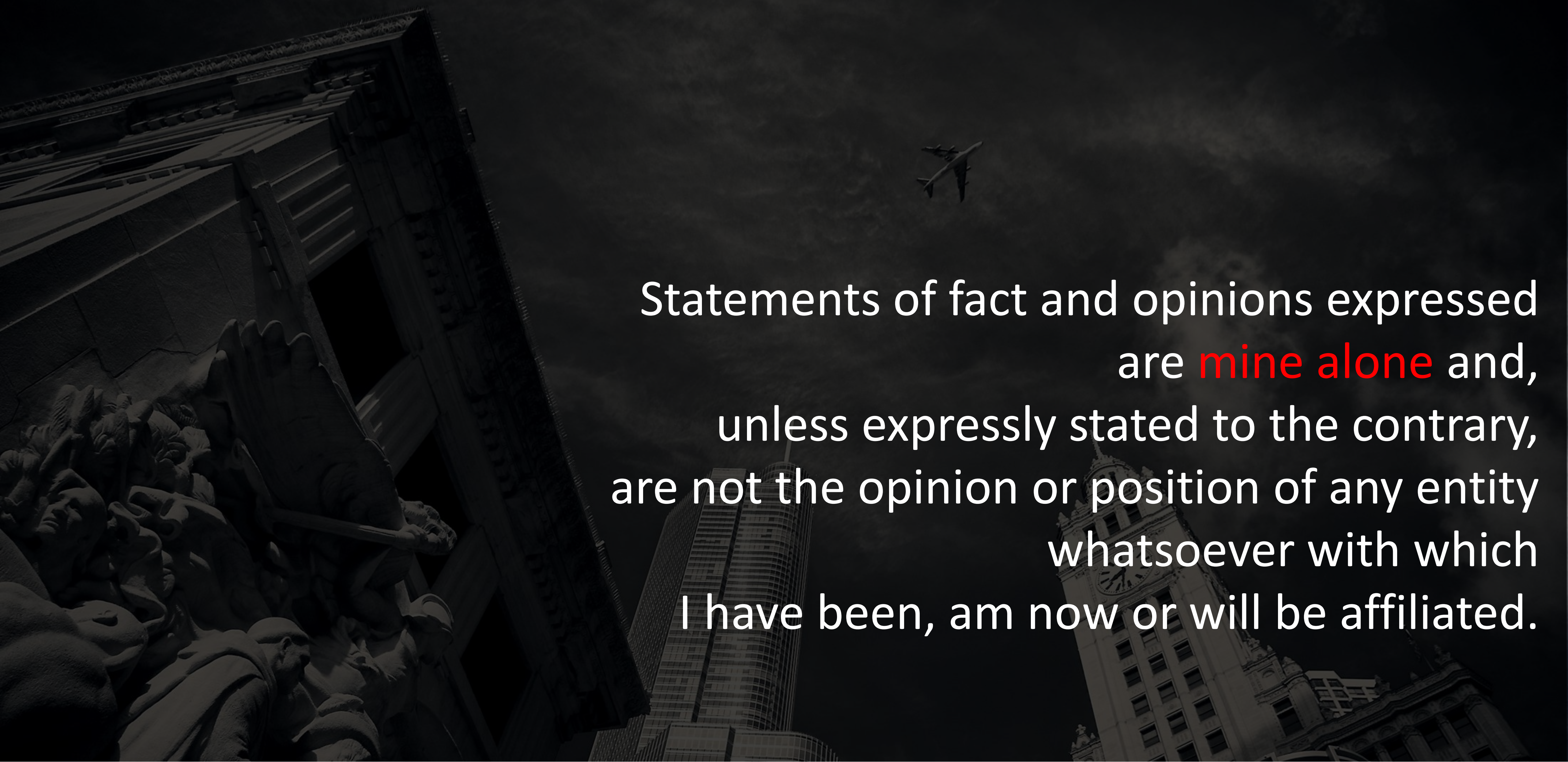
**Email:** robertesell@gmail.com

# Value Proposition

- Social Engineering Intro
- Defcon SE CTF Overview
- Open Source Intelligence (OSINT)
- Vishing (Techniques & Pretexts)
- How to Defend
- Tools & Resources

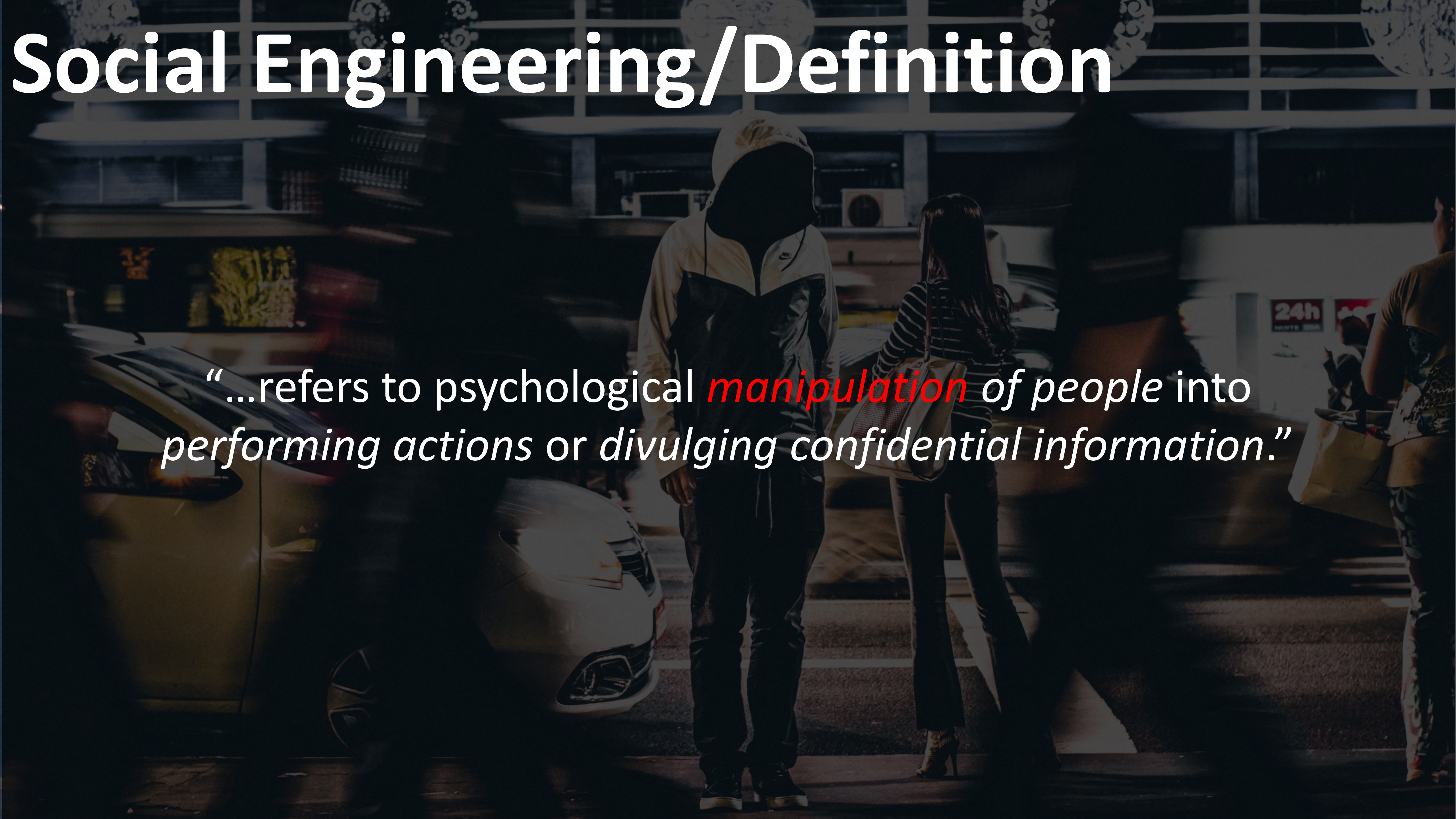
YOU BETTER HURRY UP AND START BEING AWESOME
BECAUSE I'M NOT WAITING FOR YOU

# 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/Definition

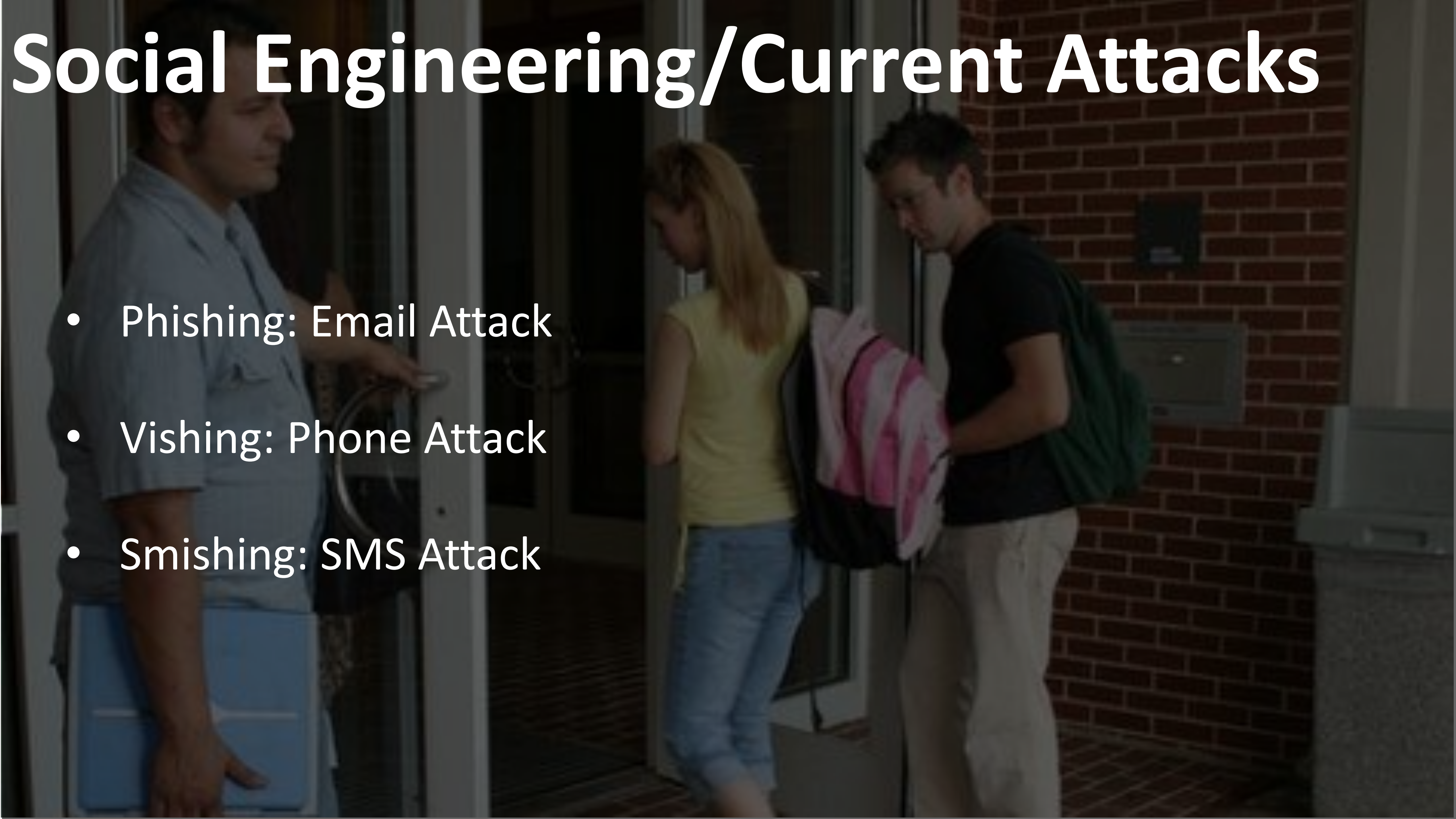


“…refers to psychological *manipulation of people* into *performing actions* or *divulging confidential information*.”

# Social Engineering/Golden Oldies

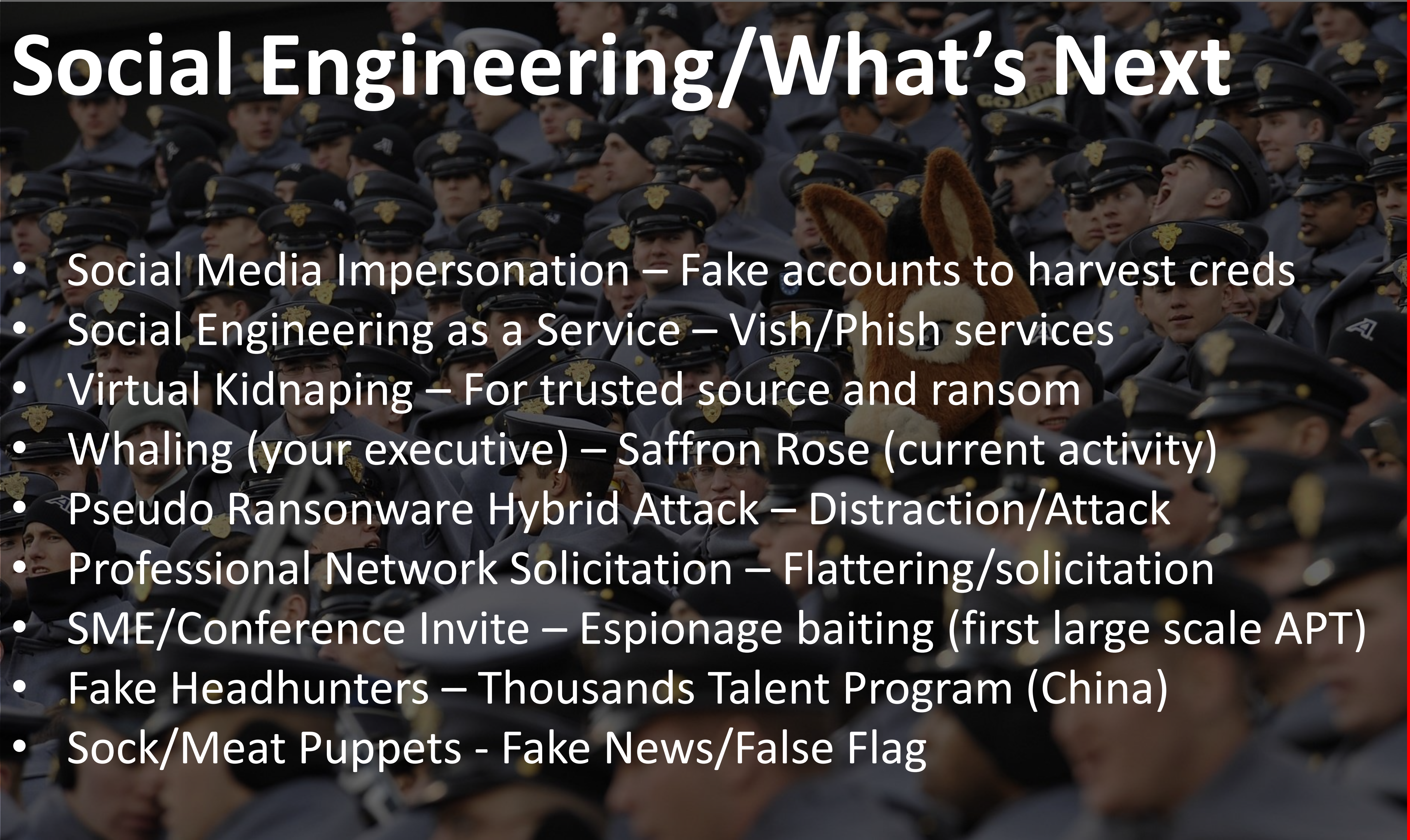
- Impersonation
- Tailgating
- Shoulder surfing
- Dumpster diving

# Social Engineering/Current Attacks



- Phishing: Email Attack
- Vishing: Phone Attack
- Smishing: SMS Attack

# Social Engineering/What's Next



- Social Media Impersonation – Fake accounts to harvest creds
- Social Engineering as a Service – Vish/Phish services
- Virtual Kidnaping – For trusted source and ransom
- Whaling (your executive) – Saffron Rose (current activity)
- Pseudo Ransonware Hybrid Attack – Distraction/Attack
- Professional Network Solicitation – Flattering/solicitation
- SME/Conference Invite – Espionage baiting (first large scale APT)
- Fake Headhunters – Thousands Talent Program (China)
- Sock/Meat Puppets - Fake News/False Flag

*** V2: ALL NEW CONTENT ***

# Social Engineering/What's Next

**Astroturfing:** the practice of masking the sponsors of a message or organization (political, advertising, religious or public relations) to make it appear as though it originates from and is supported by a grassroots participant(s).

Every nation state has a SE division now:

- China: 50 Cent Army (the pioneers!)
- Russia: Web Brigades

Large corporations have been doing this for years. Huge market.

*** V2: ALL NEW CONTENT ***

# 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%.

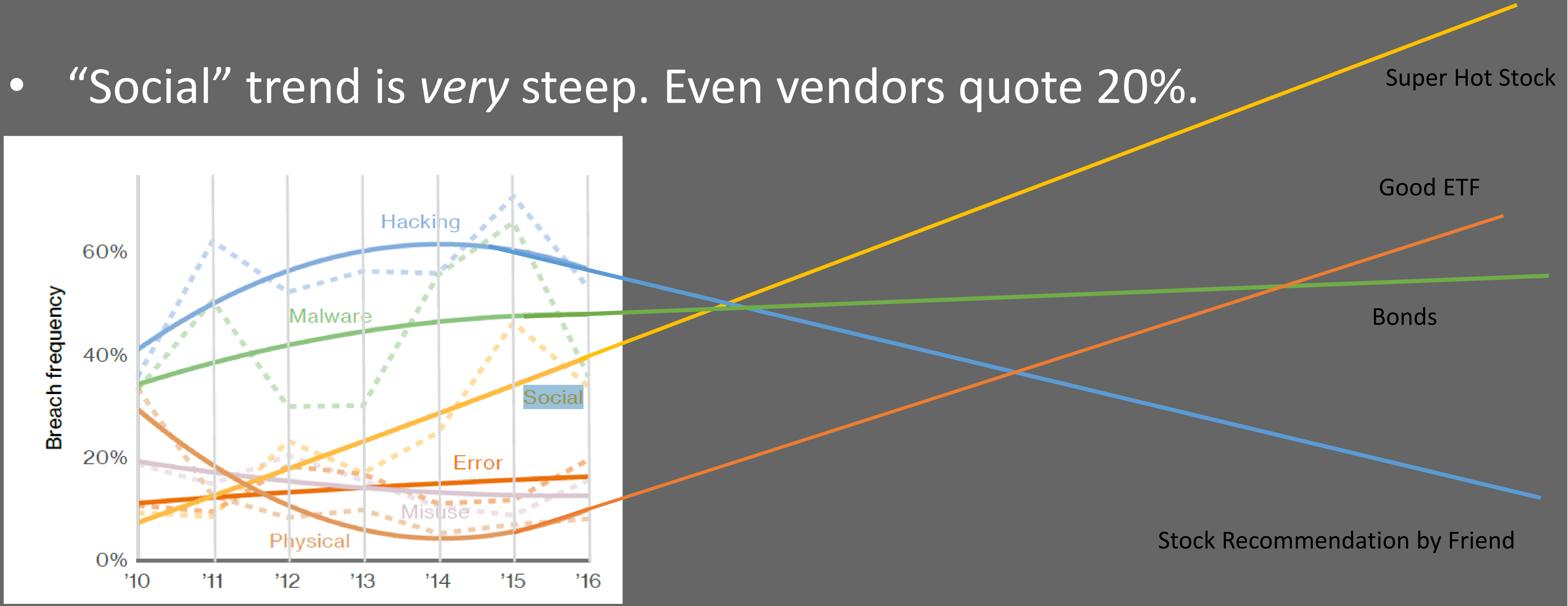
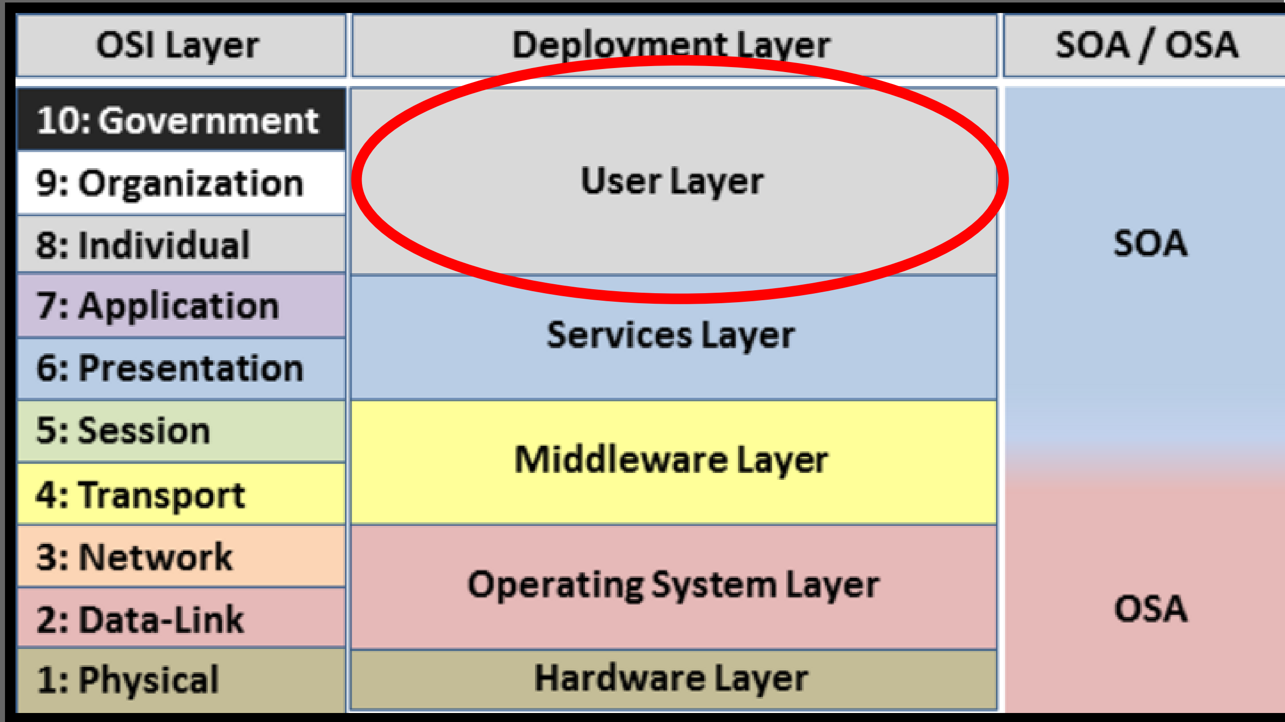


Chart source: DBIR 2017 Verizon Report – Page 7

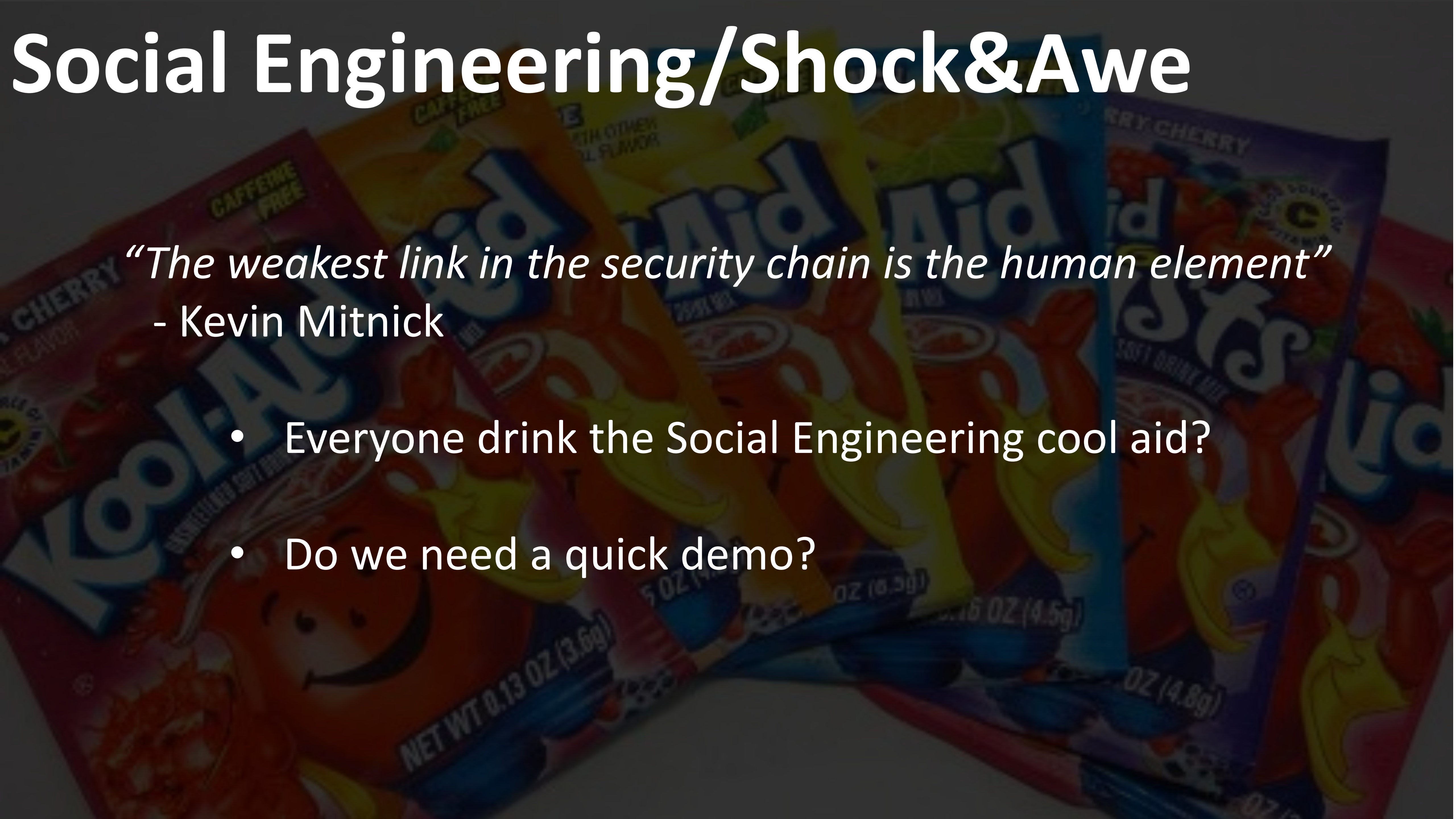
# Social Engineering/Models

- The infamous OSI model: historically has been all about technology
- “User Layer” is a very cost effective target.
- Just ask for the password
  (and they will give it to you).



| OSI Layer | Deployment Layer | SOA / OSA |
|---|---|---|
| 10: Government | User Layer | SOA |
| 9: Organization | | |
| 8: Individual | | |
| 7: Application | Services Layer | |
| 6: Presentation | | |
| 5: Session | Middleware Layer | |
| 4: Transport | | OSA |
| 3: Network | Operating System Layer | |
| 2: Data-Link | | |
| 1: Physical | Hardware Layer | |

# Social Engineering/Shock&Awe



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

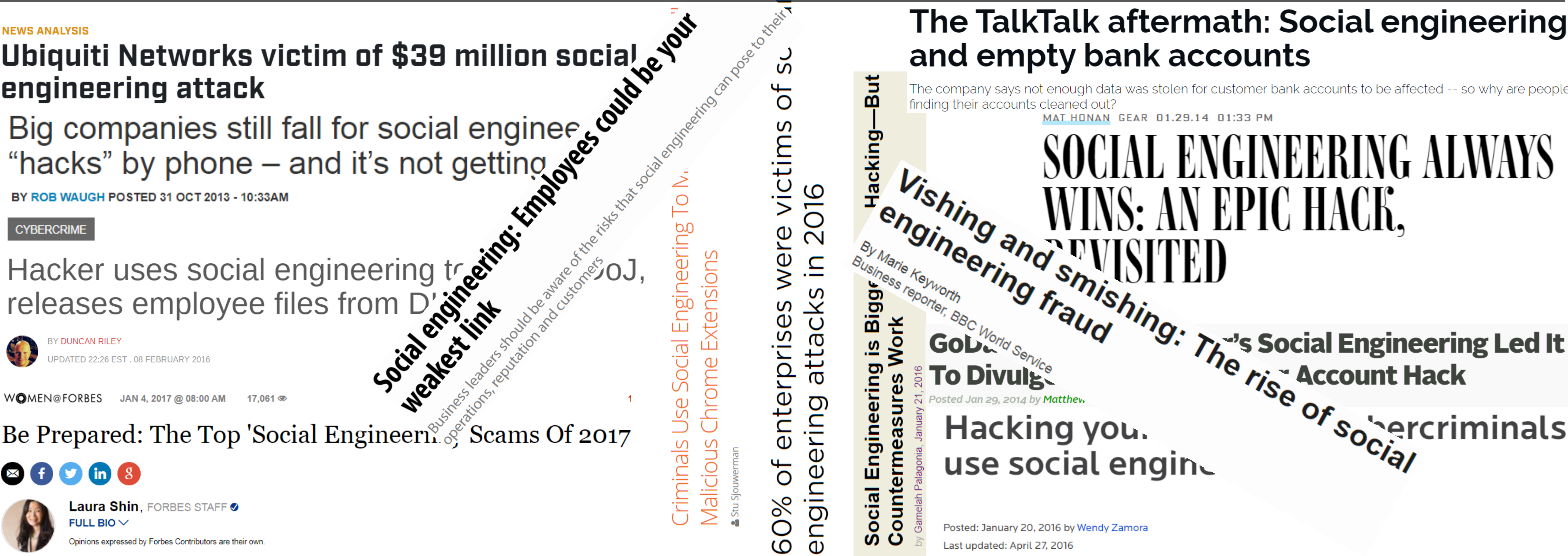
- Everyone drink the Social Engineering cool aid?
- Do we need a quick demo?

# I am sorry!

Can we move on?

# Social Engineering/News

Still need evidence to support investment in a phishing program?
just Google it.



NEWS ANALYSIS

Ubiquiti Networks victim of $39 million social engineering attack

Big companies still fall for social enginee
“hacks” by phone – and it’s not getting

BY ROB WAUGH POSTED 31 OCT 2013 - 10:33AM

CYBERCRIME

Hacker uses social engineering t… DoJ, releases employee files from D…

BY DUNCAN RILEY
UPDATED 22:26 EST . 08 FEBRUARY 2016

WOMEN@FORBES JAN 4, 2017 @ 08:00 AM 17,061

Be Prepared: The Top 'Social Engineeri… Scams Of 2017

Laura Shin, FORBES STAFF
FULL BIO
Opinions expressed by Forbes Contributors are their own.

Social engineering: Employees could be your weakest link

Business leaders should be aware of the risks that social engineering can pose to their operations, reputation and customers

Criminals Use Social Engineering To M…
Malicious Chrome Extensions

Stu Sjouwerman

60% of enterprises were victims of so…
engineering attacks in 2016

Social Engineering is Bigge… Hacking—But
Countermeasures Work

by Gamelah Palagonia, January 21, 2016

The TalkTalk aftermath: Social engineering and empty bank accounts

The company says not enough data was stolen for customer bank accounts to be affected -- so why are people finding their accounts cleaned out?

MAT HONAN GEAR 01.29.14 01:33 PM

SOCIAL ENGINEERING ALWAYS WINS: AN EPIC HACK, REVISITED

Vishing and smishing: The rise of social engineering fraud

By Marie Keyworth
Business reporter, BBC World Service

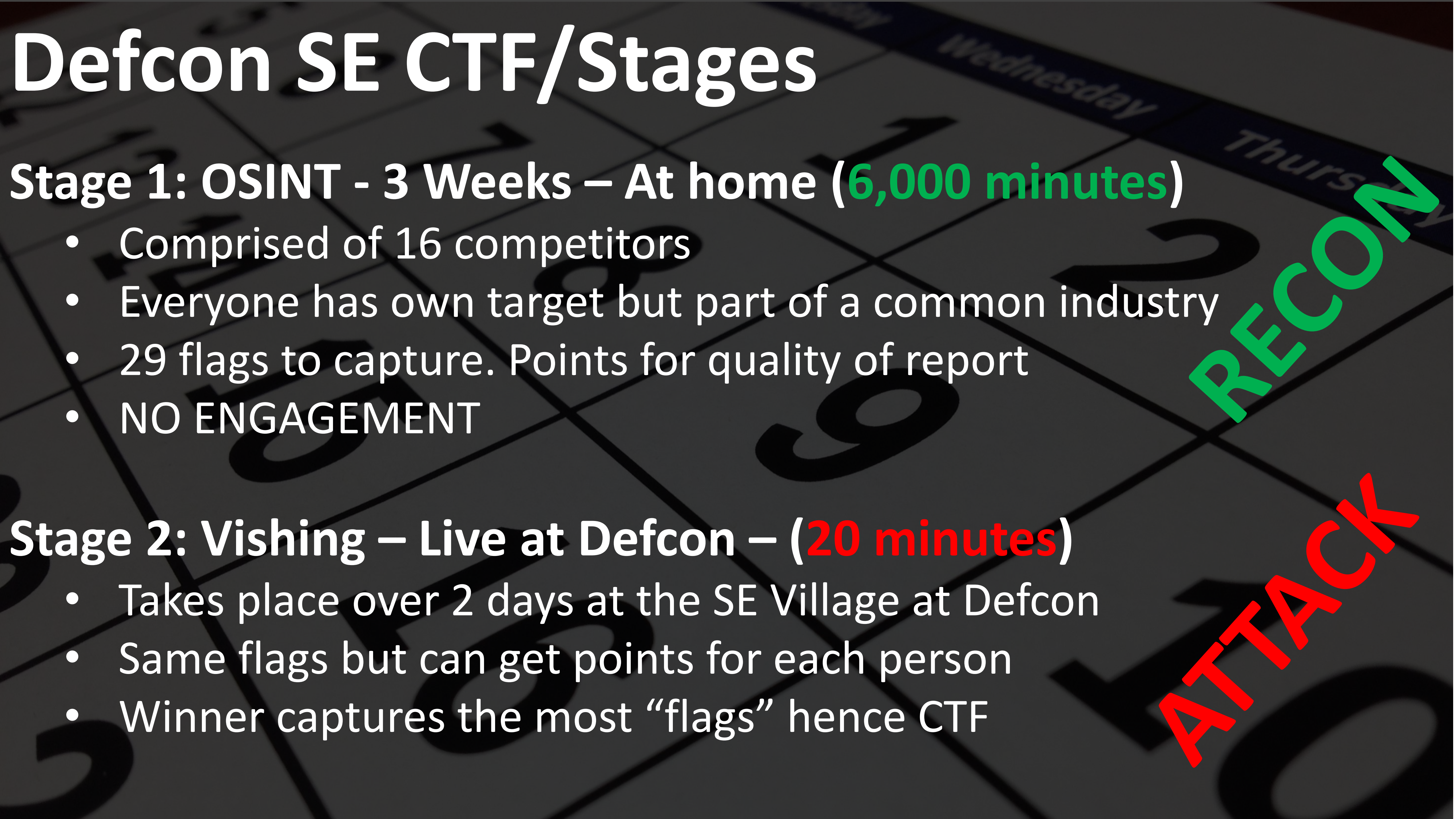
GoD… …'s Social Engineering Led It
To Divulg… … Account Hack

Posted Jan 29, 2014 by Matthew

Hacking you… …bercriminals
use social engin…

Posted: January 20, 2016 by Wendy Zamora
Last updated: April 27, 2016

# 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)**

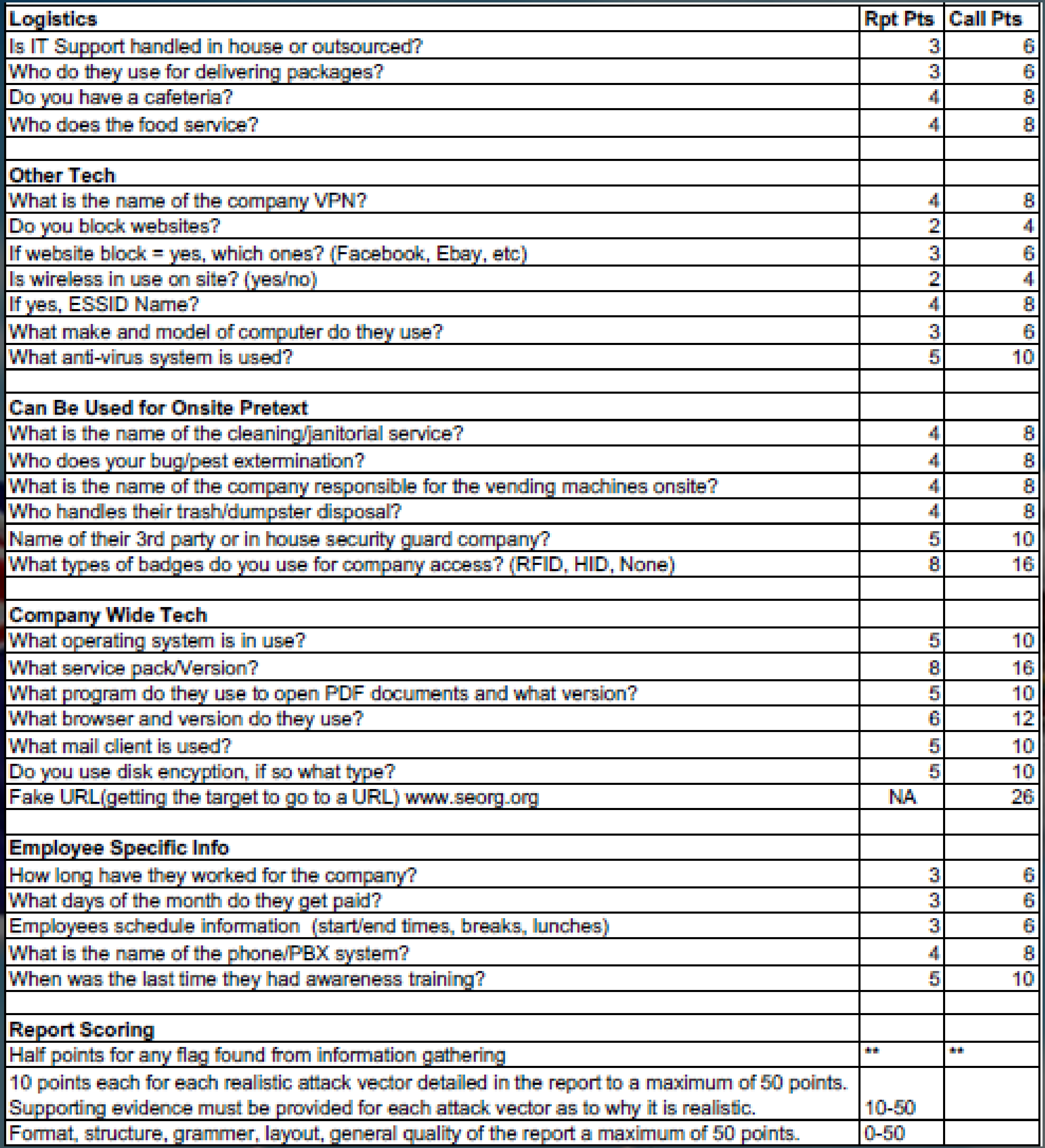
- Takes place over 2 days at the SE Village at Defcon
- Same flags but can get points for each person
- Winner captures the most “flags” hence CTF

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/Evil Attacker Flags

**Based on Lockheed Cyber Kill Chain:**

- Environment: Technologies, Response Capabilities, Assets
- Weaponization: Available exploits (patch level)
- Delivery Methods: Email, web or  on prem (USB)
- Exploitation: AV, endpoint and perimeter protection
- Installation: Alerting, logging, monitoring, SIEM
- Command/Control: Ports, hours, machine naming scheme
- Actions on Objectives: Data exfil or data encryption – location of assets, hours of operations, backups, staffing, vendors, incident response, retainment, RTO/RPO, DRP, policies & procedures

*** V2: ALL NEW CONTENT ***

# OSINT/Acquire 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/

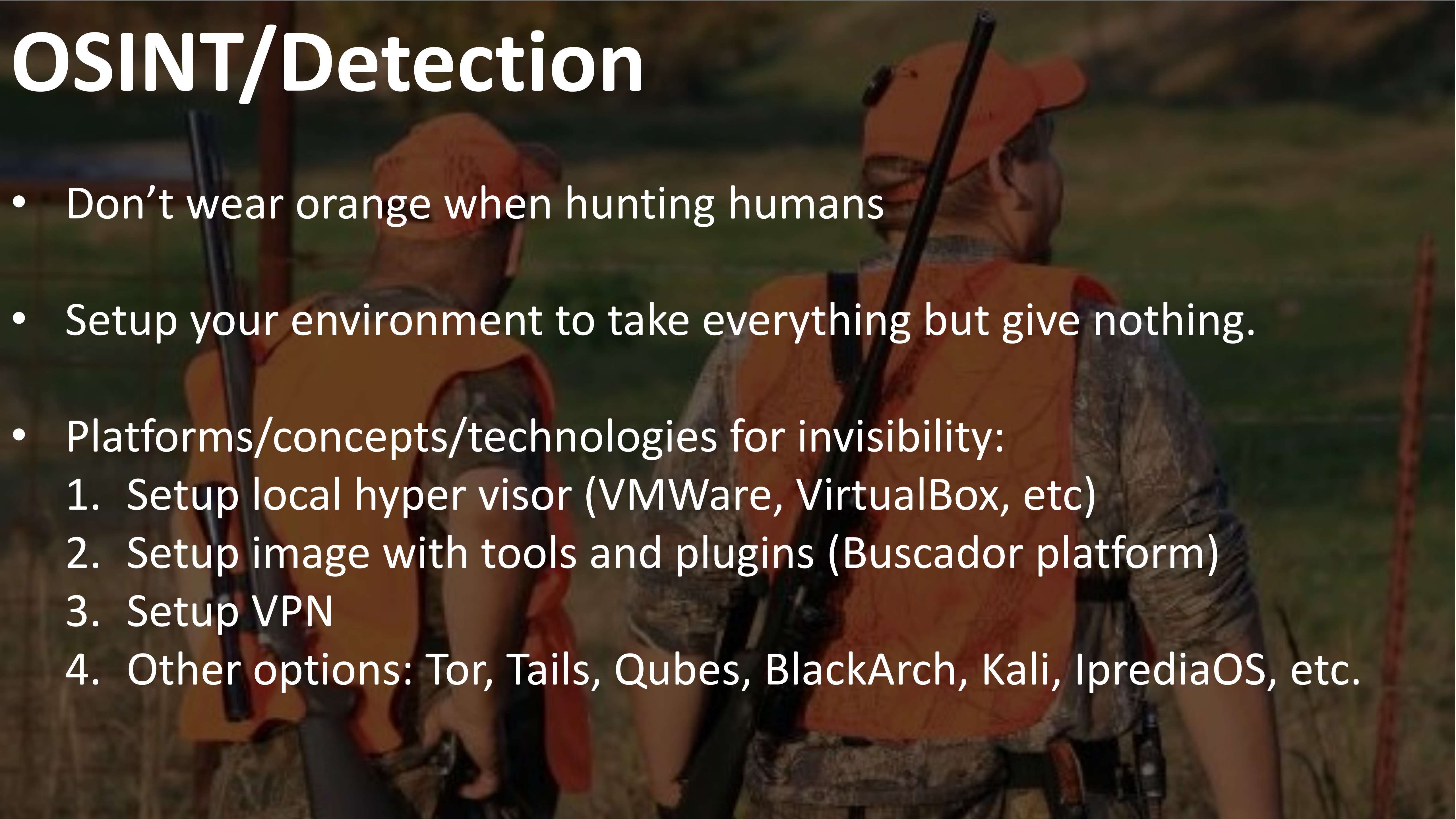
I DON'T KNOW WHO YOU ARE...
BUT I WILL LOOK YOU UP ON LINKEDIN AND I WILL FIND YOU
memegenerator.net

# 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

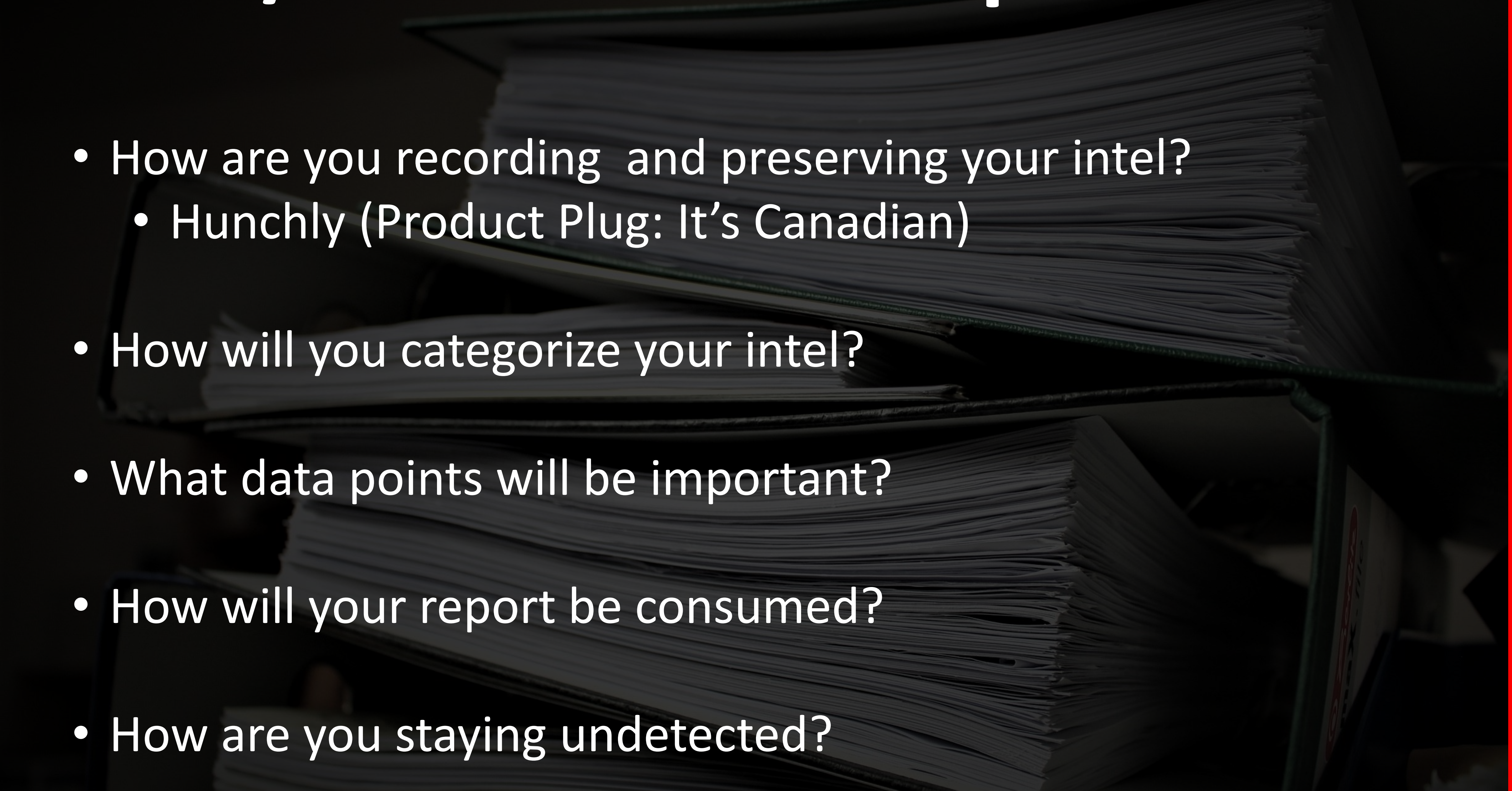


- Don’t wear orange when hunting humans

- Setup your environment to take everything but give nothing.

- Platforms/concepts/technologies for invisibility:
  1. Setup local hyper visor (VMWare, VirtualBox, etc)
  2. Setup image with tools and plugins (Buscador platform)
  3. Setup VPN
  4. Other options: Tor, Tails, Qubes, BlackArch, Kali, IprediaOS, etc.

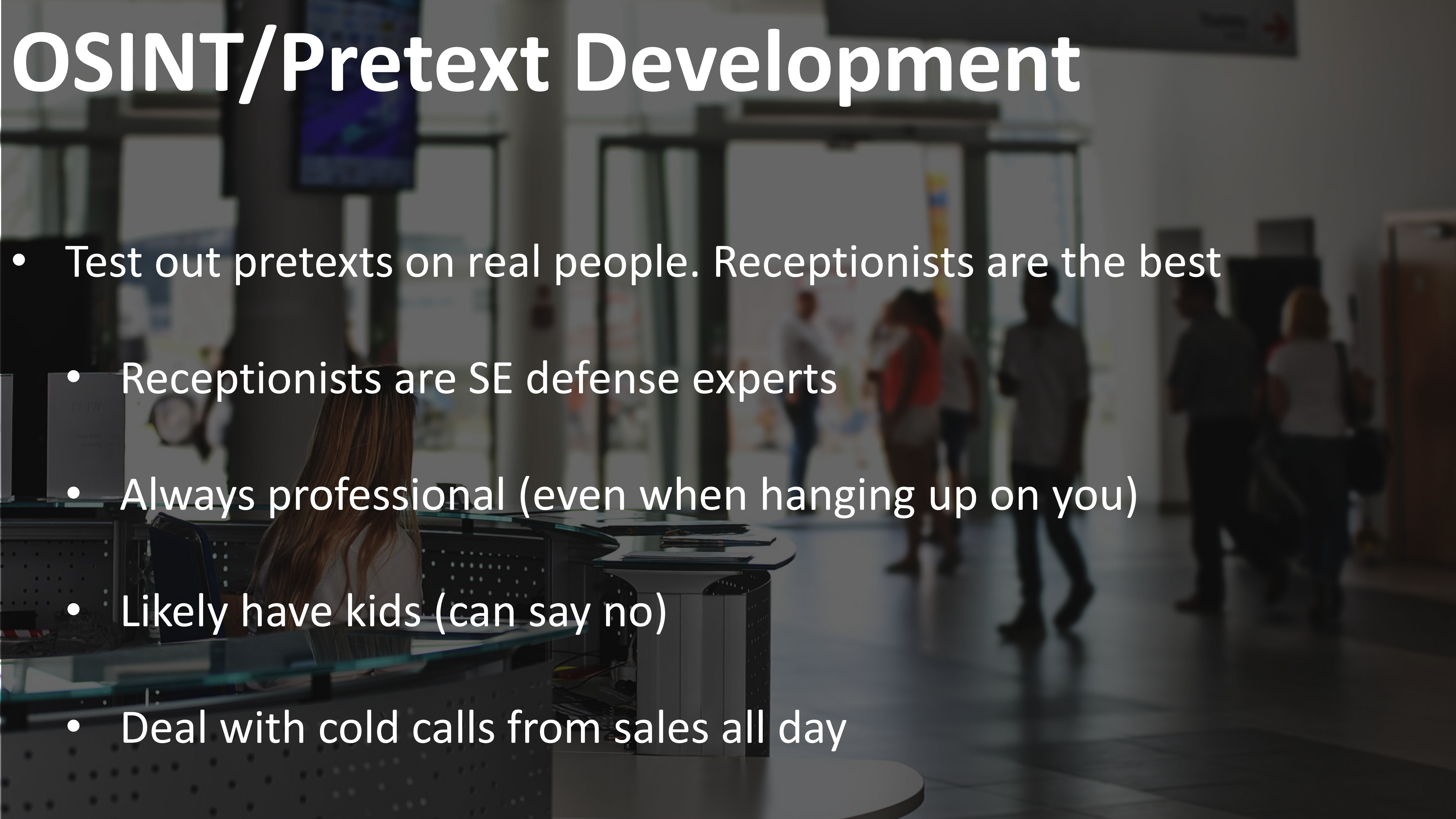
# OSINT/Evil Attacker Preparations



- How are you recording  and preserving your intel?
  - Hunchly (Product Plug: It’s Canadian)
- How will you categorize your intel?
- What data points will be important?
- How will your report be consumed?
- How are you staying undetected?

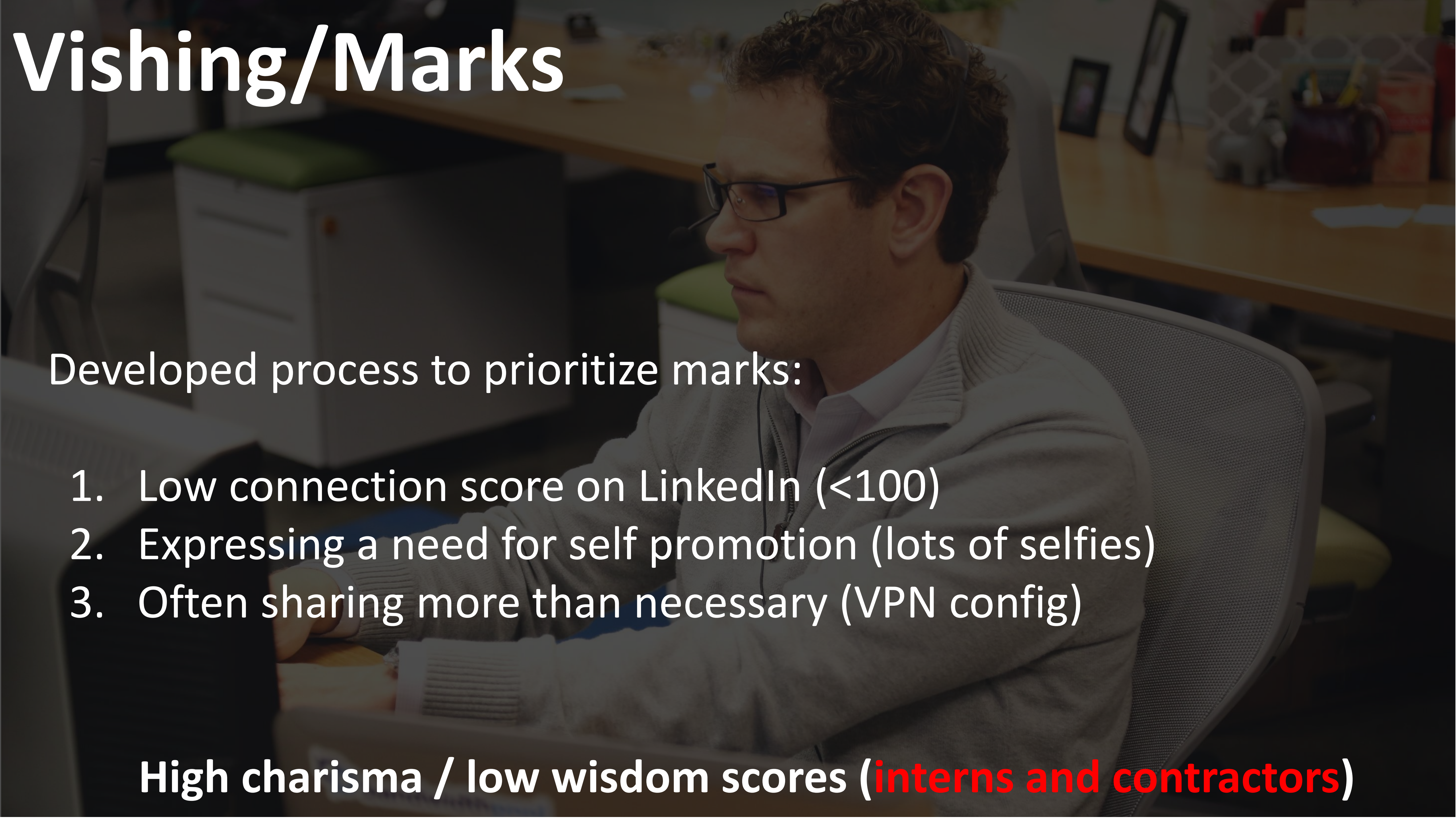
*** V2: ALL NEW CONTENT ***

# 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/Marks

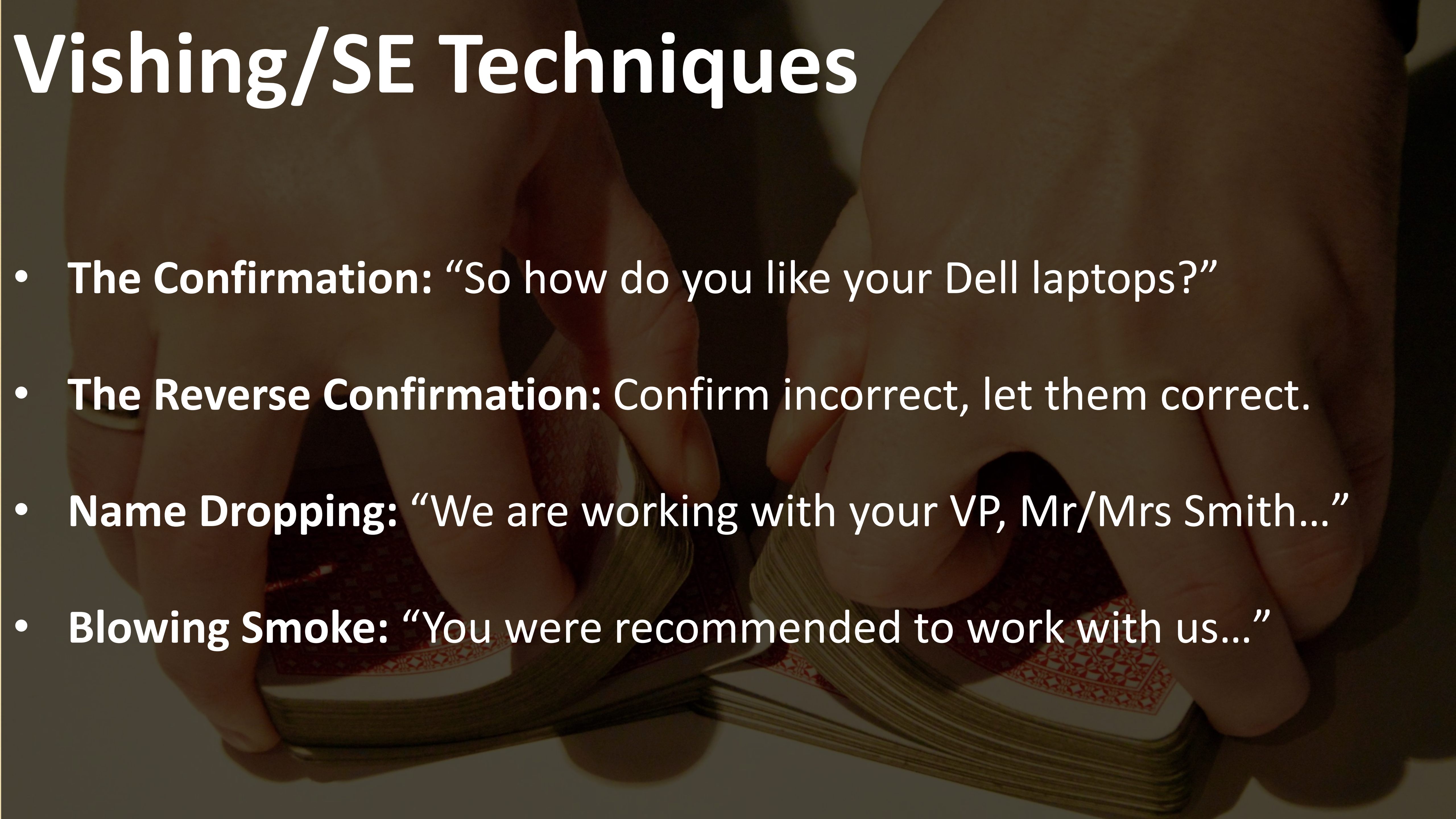


Developed process to prioritize marks:

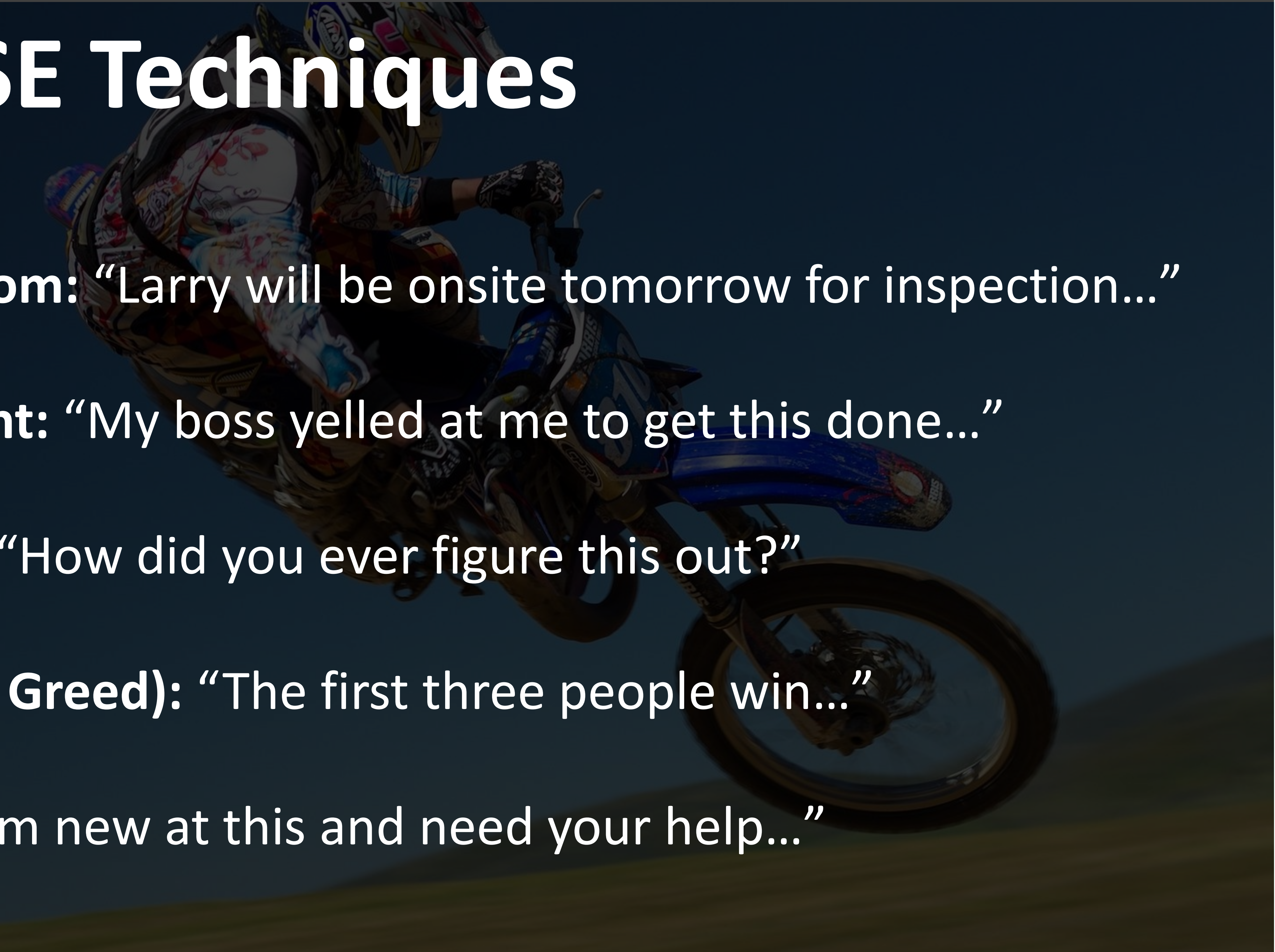
1. Low connection score on LinkedIn (<100)
2. Expressing a need for self promotion (lots of selfies)
3. Often sharing more than necessary (VPN config)

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

# Vishing/SE Techniques



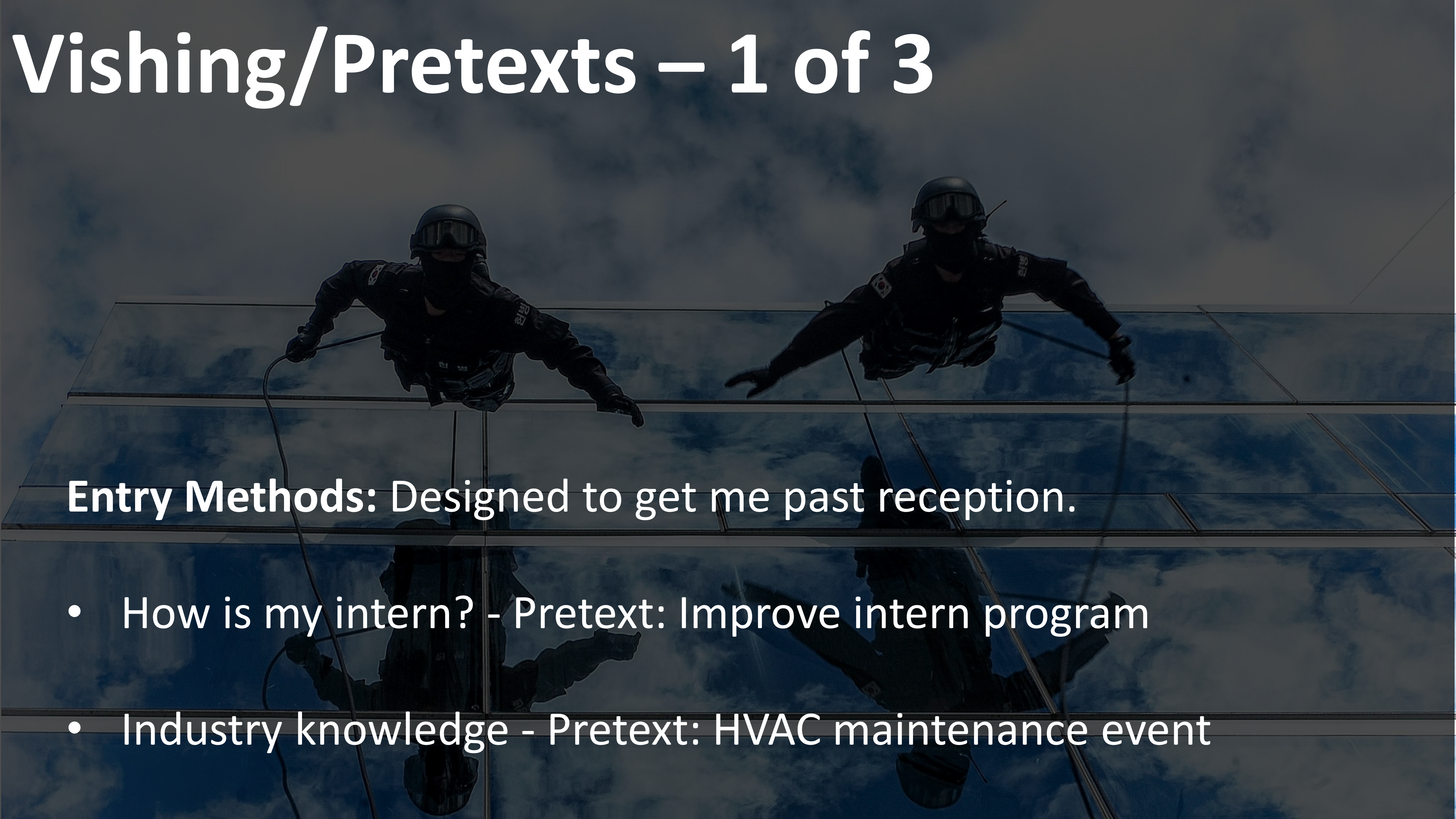
- **The Confirmation:** “So how do you like your Dell laptops?”
- **The Reverse Confirmation:** Confirm incorrect, let them correct.
- **Name Dropping:** “We are working with your VP, Mr/Mrs Smith…”
- **Blowing Smoke:** “You were recommended to work with us…”



# Vishing/SE Techniques

- **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…”

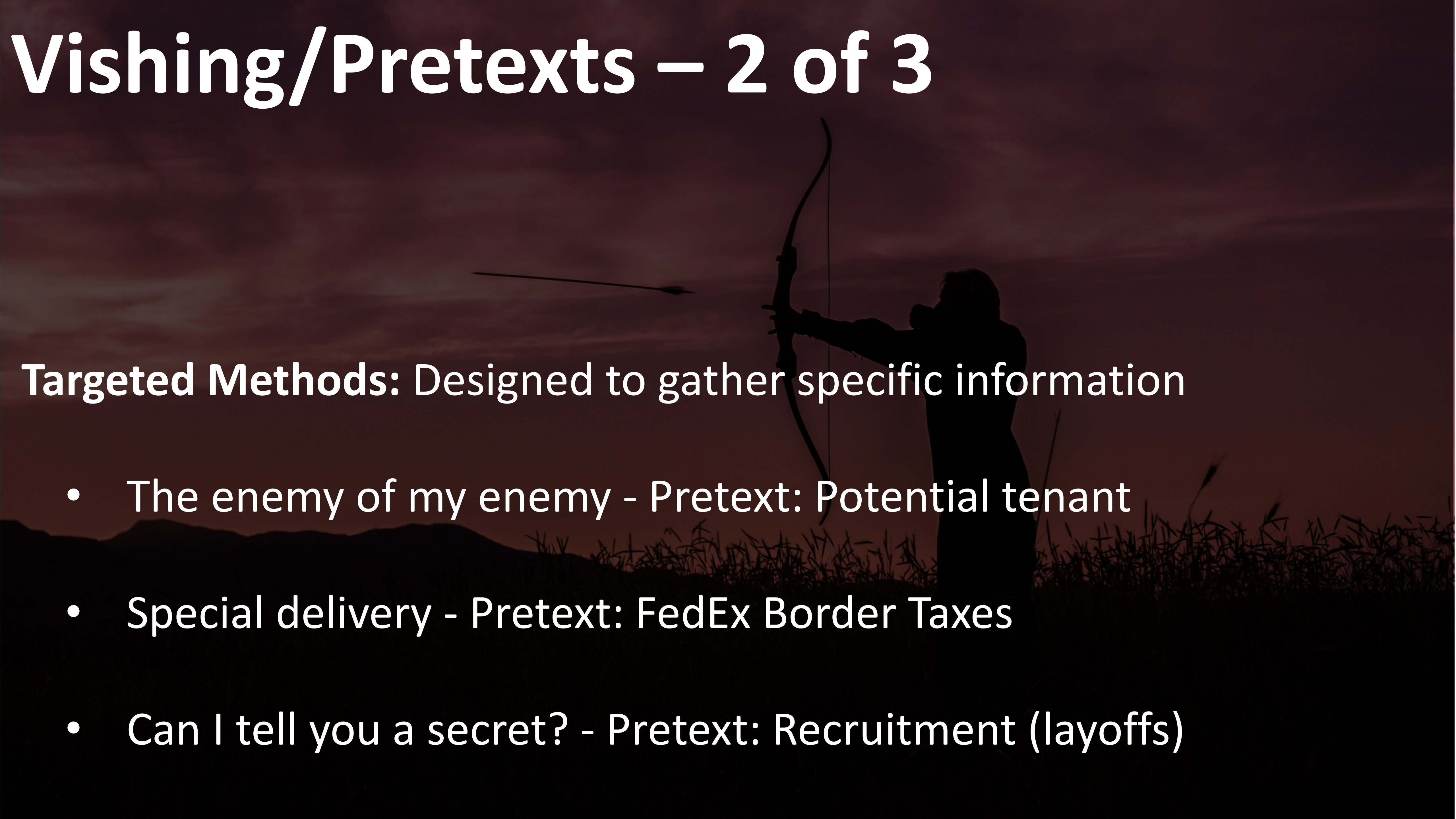
# Vishing/Pretexts – 1 of 3



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

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

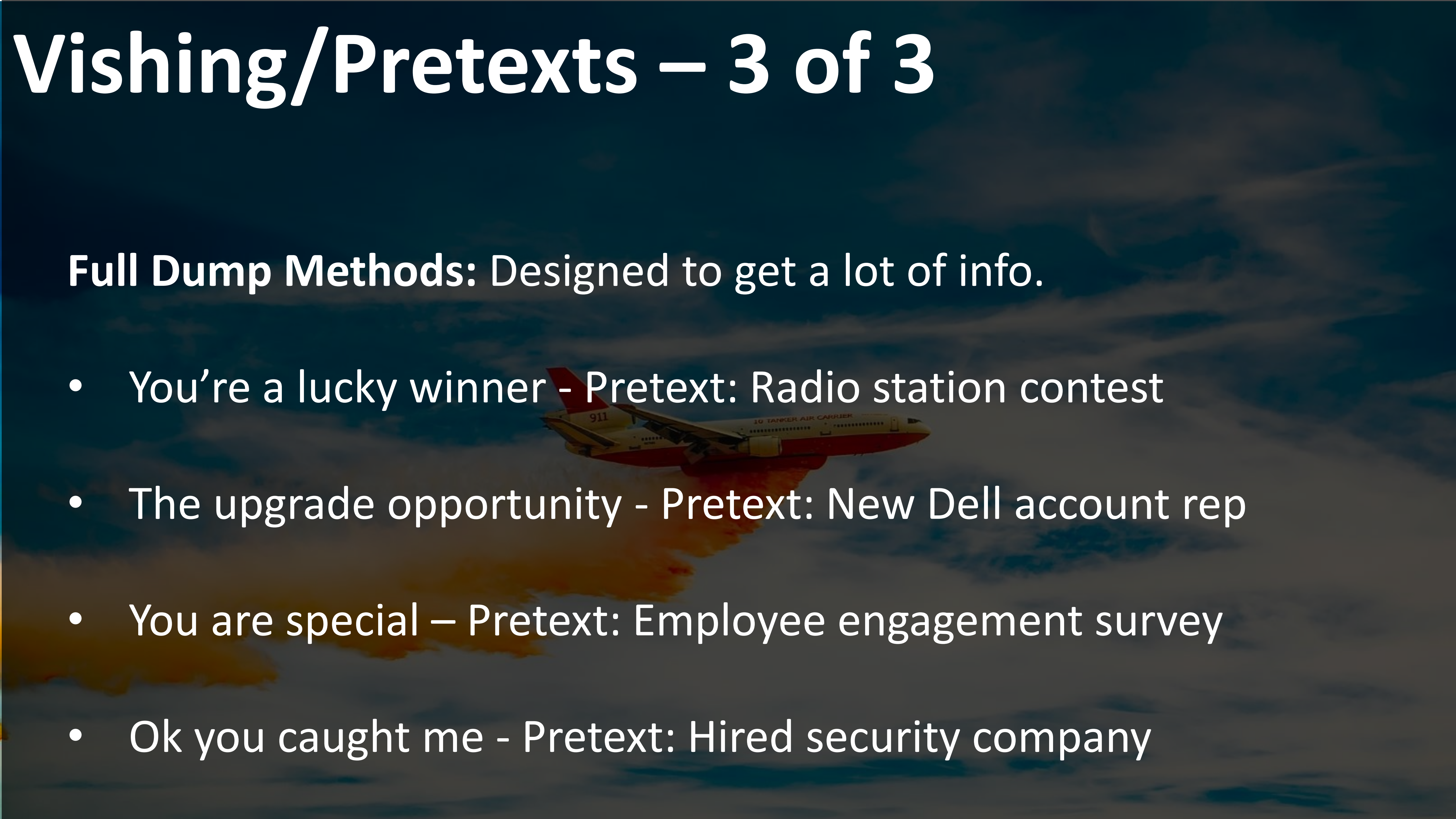
# Vishing/Pretexts – 2 of 3



**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)

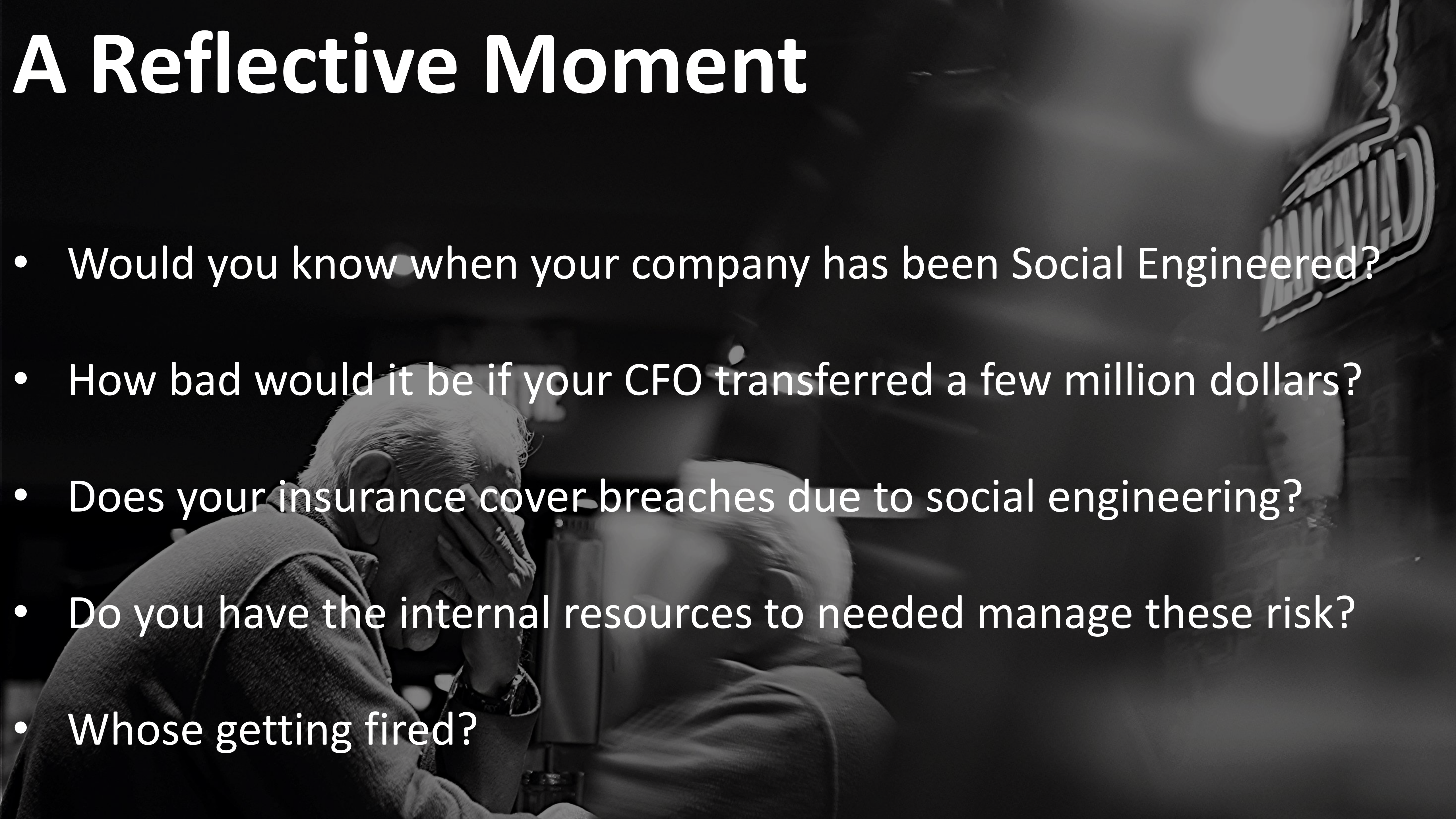
# Vishing/Pretexts – 3 of 3



**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



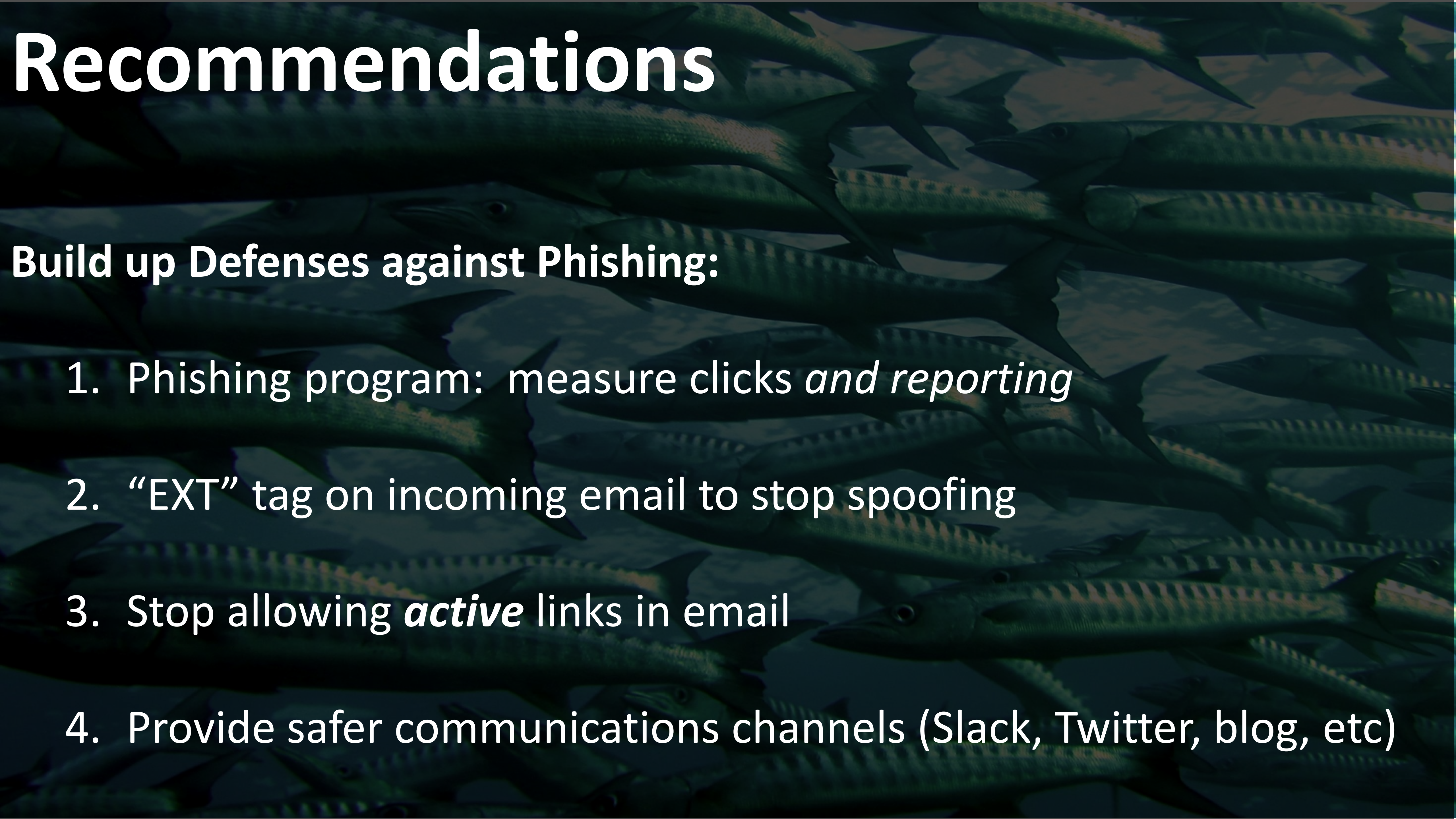
- Would you know when your company has been Social Engineered?
- How bad would it be if your CFO transferred a few million dollars?
- Does your insurance cover breaches due to social engineering?
- Do you have the internal resources to needed manage these risk?
- Whose getting fired?

# Recommendations

## Understand your Exposure:

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

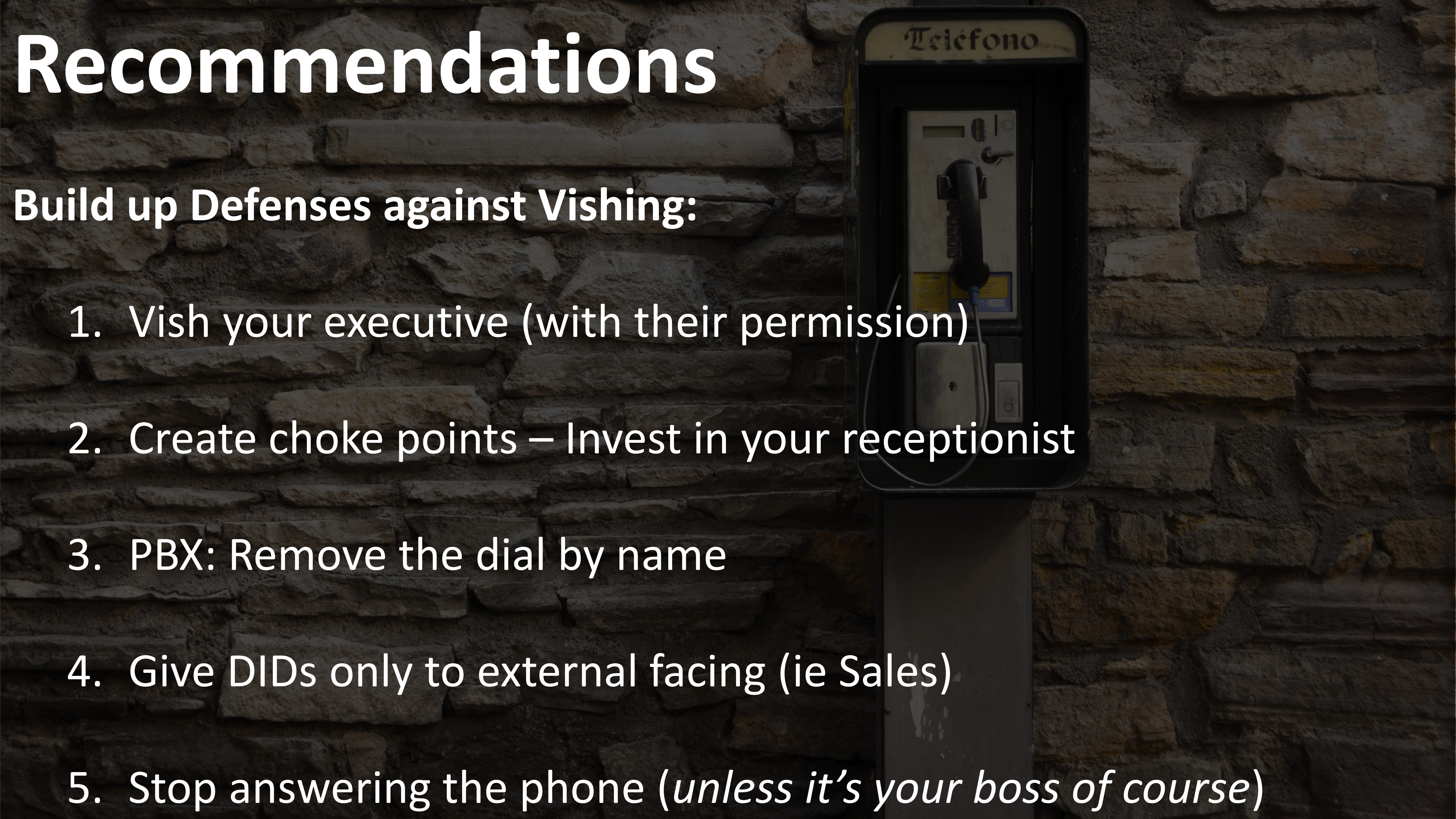
# Recommendations



**Build up Defenses against Phishing:**

1. Phishing program:  measure clicks *and reporting*
2. "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:**

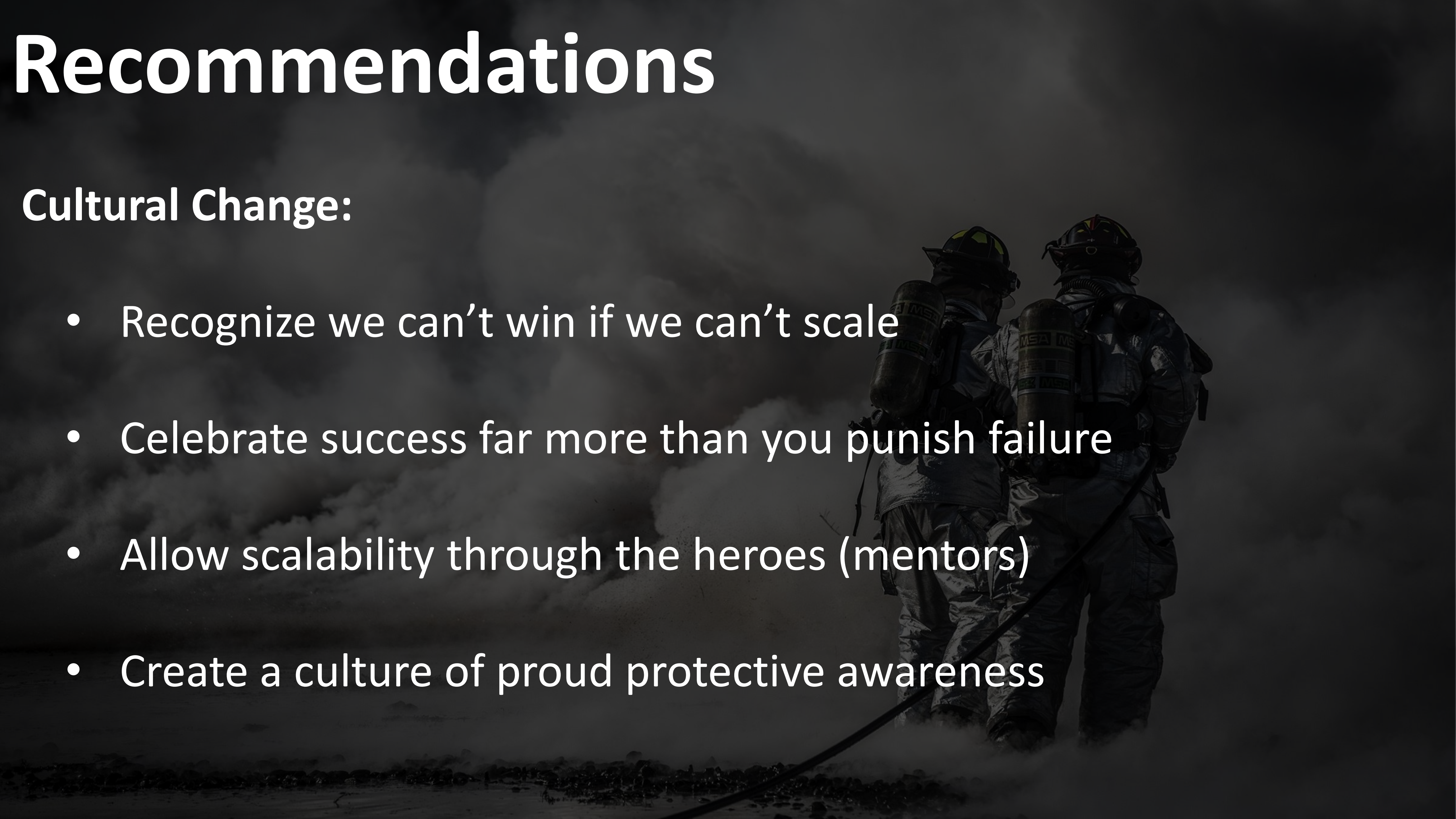
1. Vish your executive (with their permission)
2. Create choke points – Invest in your receptionist
3. PBX: Remove the dial by name
4. Give DIDs only to external facing (ie Sales)
5. Stop answering the phone (*unless it's your boss of course*)

# 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

# Evil Attacker Defense Cheat Sheet

Evil attackers hate it when we do these things:

- Remove specific technologies from job descriptions
- Assume your technical forum posts are read by bad people
- Train users (start with phishing)
- Patch. No really stop everything you are doing and patch
- VLANS are nice but not truly effective – SDN?
- Signature based AV to Behavior based. Configure it to respond
- Block everything but 80 and 443 outbound (C&C, mining, etc)
- 2FA everything (your OWA is an open door)
- Put everything inside the firewall (at least DMZ it)
- I’m already in - Come find me - Spend time hunting (beacons)

*** V2: ALL NEW CONTENT ***

# Tools/Physical

- Start with physical address (the basics):
  - 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

- Robert B Cialdini: 6 Principles of Influence (Books and YouTube)

Thank you!

# Q&A

@robertesell