Operational Security in a Weaponized World

Aaron Crawford
Insider Security Agency

INSIDER
SECURITY AGENCY

Aaron Crawford

whoami

INSIDER

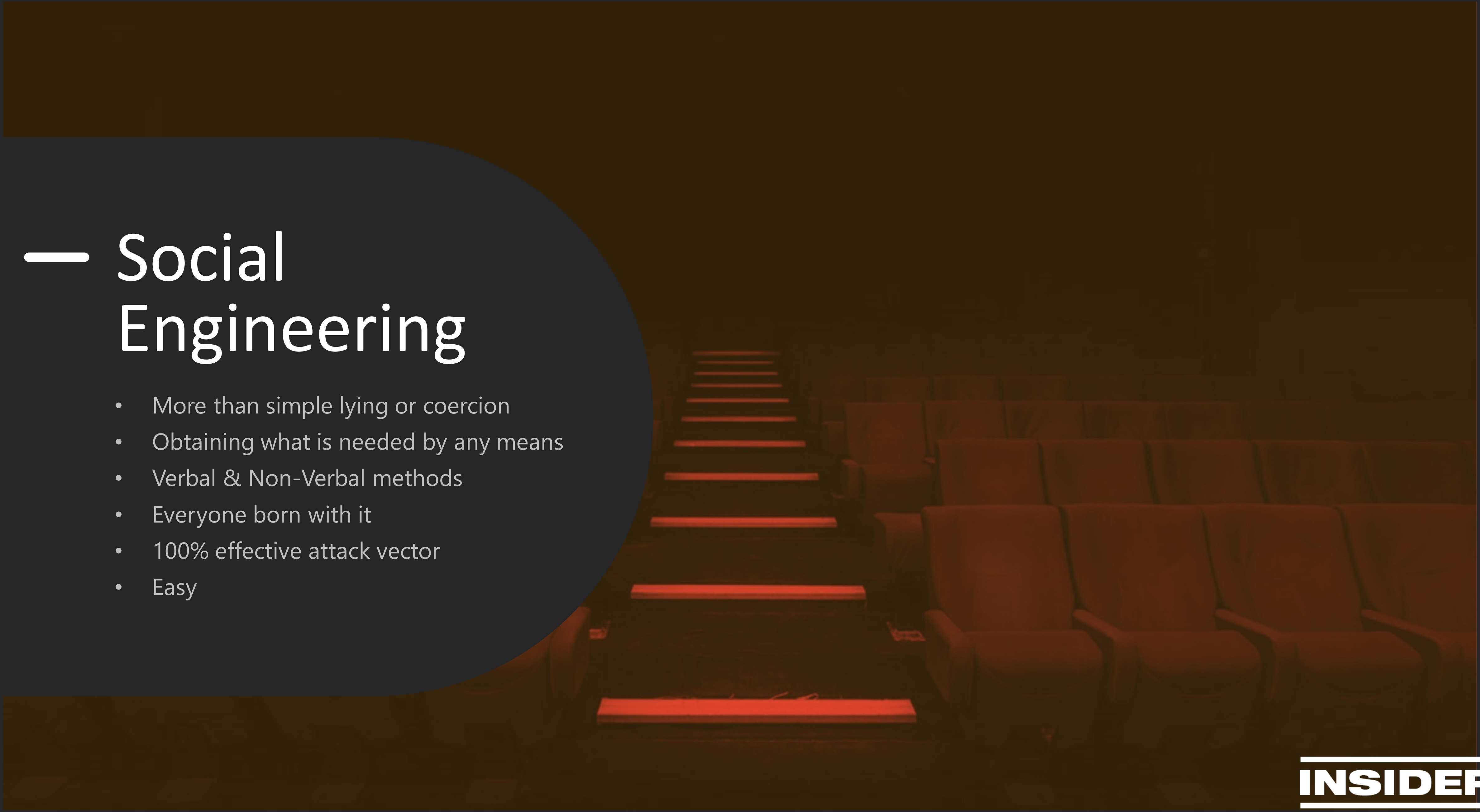
SECURITY AGENCY

Not enough time here to explain.
Find me after this talk.

Twitter: @Insider_Agency

web: www.theinsideragency.com

Hashtags: #SocialEngineeringTips #SocialOperator #LearnSocialEngineering #HackerHired #HackHunger



Social Engineering

- More than simple lying or coercion
- Obtaining what is needed by any means
- Verbal & Non-Verbal methods
- Everyone born with it
- 100% effective attack vector
- Easy

Red vs Blue

Civilian security testing defensive posture through live assessments.

Red teams = adversary

Blue teams = defensive

— Security Assessments

Why?

To verify the integrity of perimeter defenses without scope restrictions.

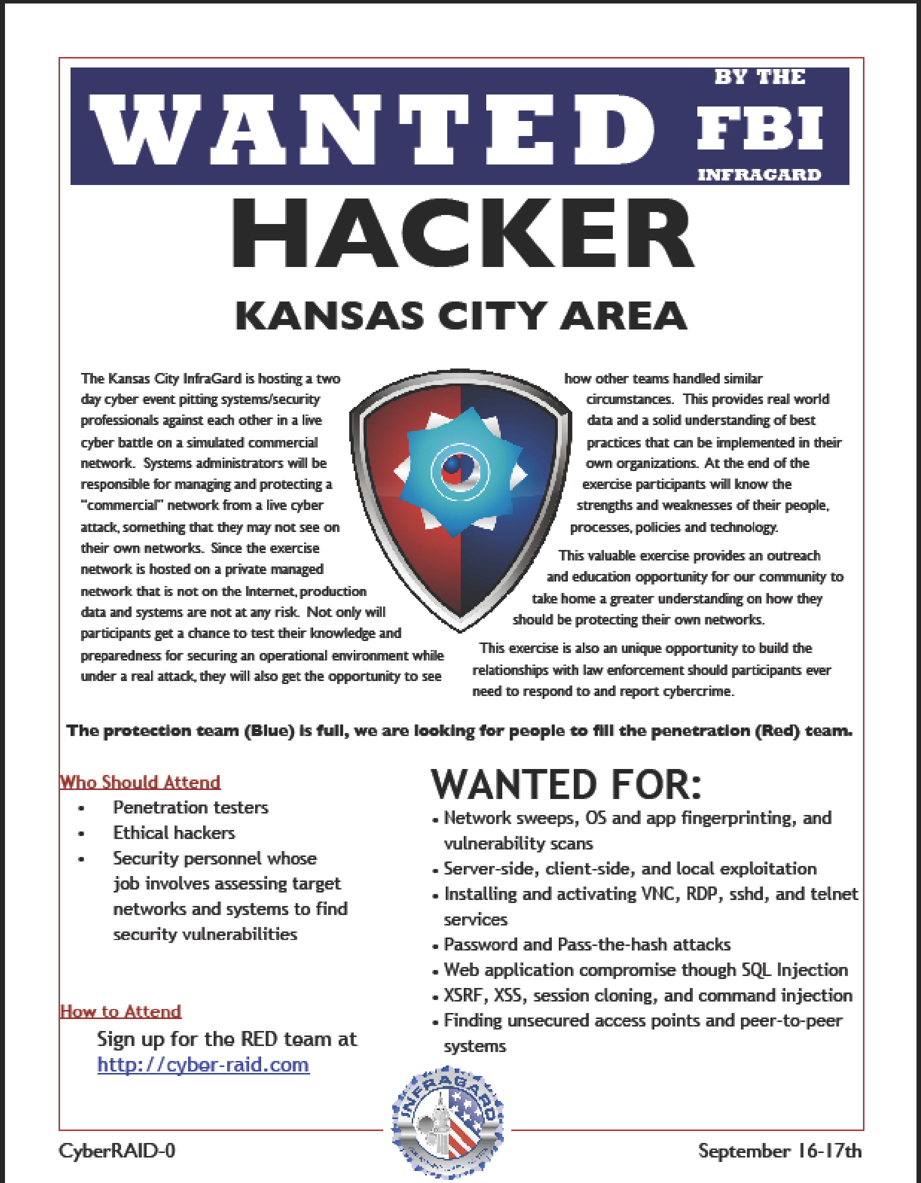
It is easier to understand how to look for opportunities and to take advantage of them, rather than train someone to think like a criminal.

Criminals are only people who take advantage of opportunities that society does not yet recognize as safe or beneficial.

INSIDER
SECURITY AGENCY

Origin Story

- Infragard sponsored event
- Red vs Blue
- Work within restrictions
- Think within the box
- Use the box



WANTED BY THE FBI INFRAGARD

HACKER

KANSAS CITY AREA

The Kansas City InfraGard is hosting a two day cyber event pitting systems/security professionals against each other in a live cyber battle on a simulated commercial network. Systems administrators will be responsible for managing and protecting a "commercial" network from a live cyber attack, something that they may not see on their own networks. Since the exercise network is hosted on a private managed network that is not on the Internet, production data and systems are not at any risk. Not only will participants get a chance to test their knowledge and preparedness for securing an operational environment while under a real attack, they will also get the opportunity to see how other teams handled similar circumstances. This provides real world data and a solid understanding of best practices that can be implemented in their own organizations. At the end of the exercise participants will know the strengths and weaknesses of their people, processes, policies and technology.

This valuable exercise provides an outreach and education opportunity for our community to take home a greater understanding on how they should be protecting their own networks.

This exercise is also an unique opportunity to build the relationships with law enforcement should participants ever need to respond to and report cybercrime.

The protection team (Blue) is full, we are looking for people to fill the penetration (Red) team.

Who Should Attend

- Penetration testers
- Ethical hackers
- Security personnel whose job involves assessing target networks and systems to find security vulnerabilities

How to Attend

Sign up for the RED team at http://cyber-raid.com

WANTED FOR:

- Network sweeps, OS and app fingerprinting, and vulnerability scans
- Server-side, client-side, and local exploitation
- Installing and activating VNC, RDP, sshd, and telnet services
- Password and Pass-the-hash attacks
- Web application compromise though SQL Injection
- XSRF, XSS, session cloning, and command injection
- Finding unsecured access points and peer-to-peer systems

CyberRAID-0

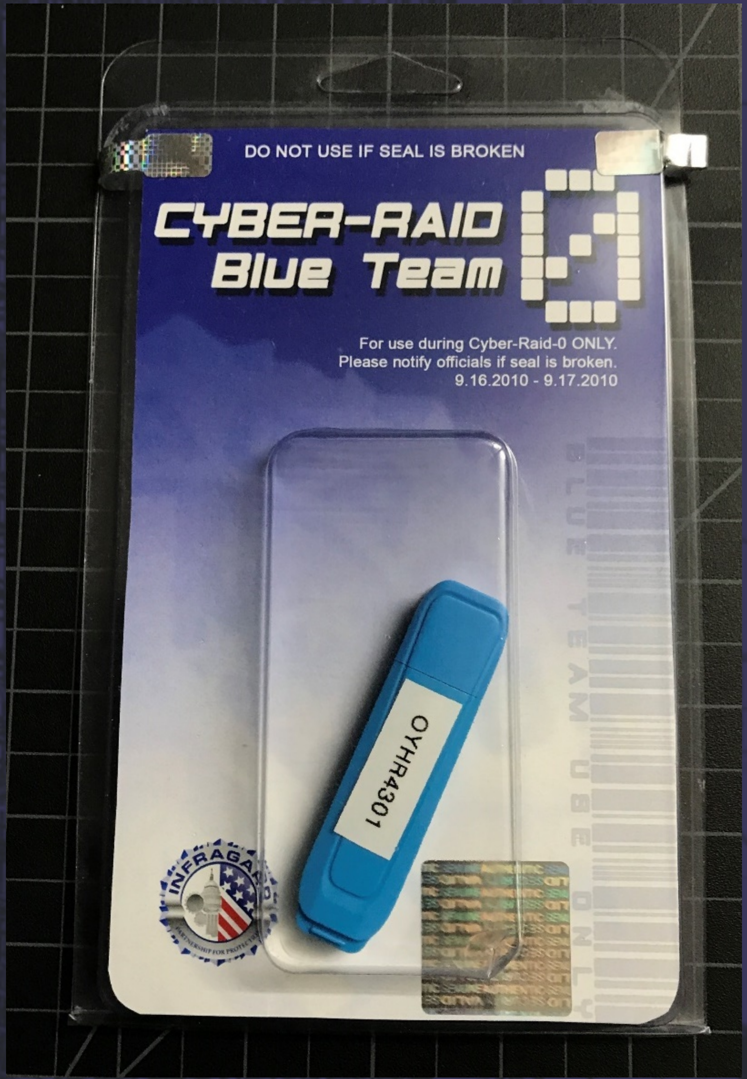
September 16-17th

Violating Trust Models

What and who do you trust?
We all trust the packaging and supply chains of products. These can be used against us and should be constantly evaluated.

INSIDER
SECURITY AGENCY

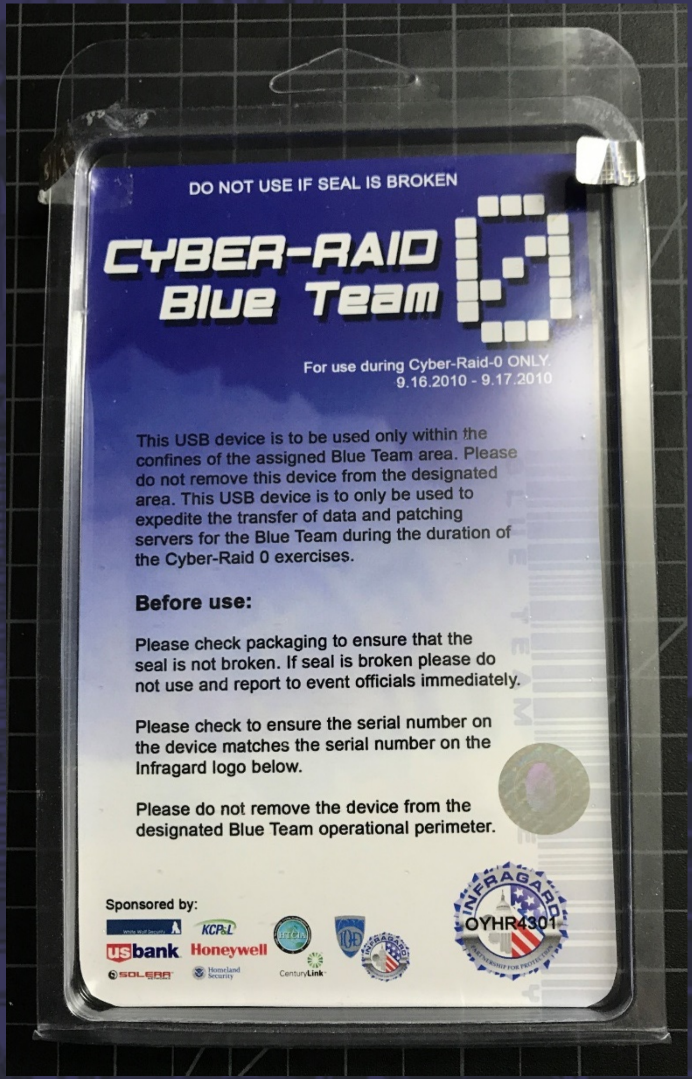
Packaging Deception



DO NOT USE IF SEAL IS BROKEN

CYBER-RAID Blue Team 0

For use during Cyber-Raid-0 ONLY.
Please notify officials if seal is broken.
9.16.2010 - 9.17.2010



DO NOT USE IF SEAL IS BROKEN

CYBER-RAID Blue Team 0

For use during Cyber-Raid-0 ONLY.
9.16.2010 - 9.17.2010

This USB device is to be used only within the confines of the assigned Blue Team area. Please do not remove this device from the designated area. This USB device is to only be used to expedite the transfer of data and patching servers for the Blue Team during the duration of the Cyber-Raid 0 exercises.

Before use:

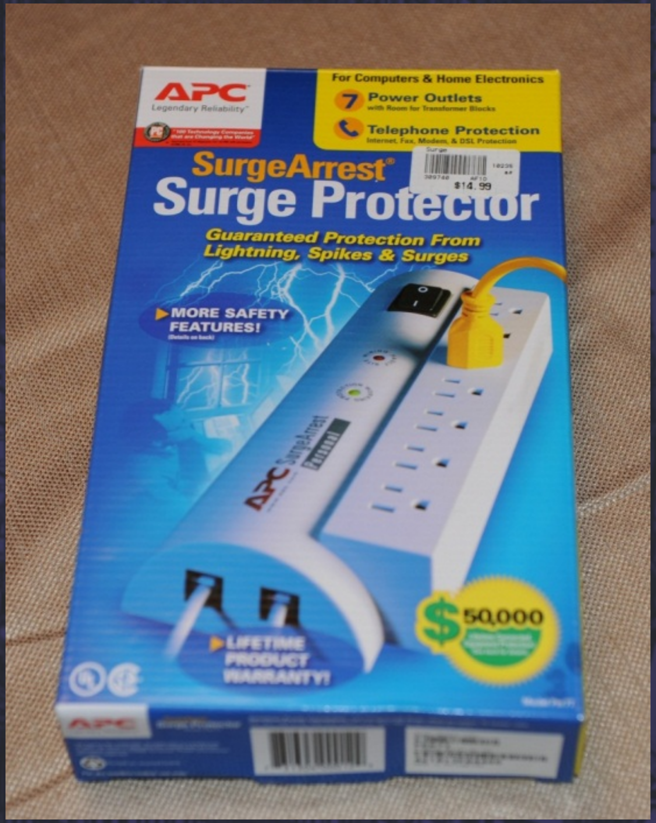
Please check packaging to ensure that the seal is not broken. If seal is broken please do not use and report to event officials immediately.

Please check to ensure the serial number on the device matches the serial number on the Infragard logo below.

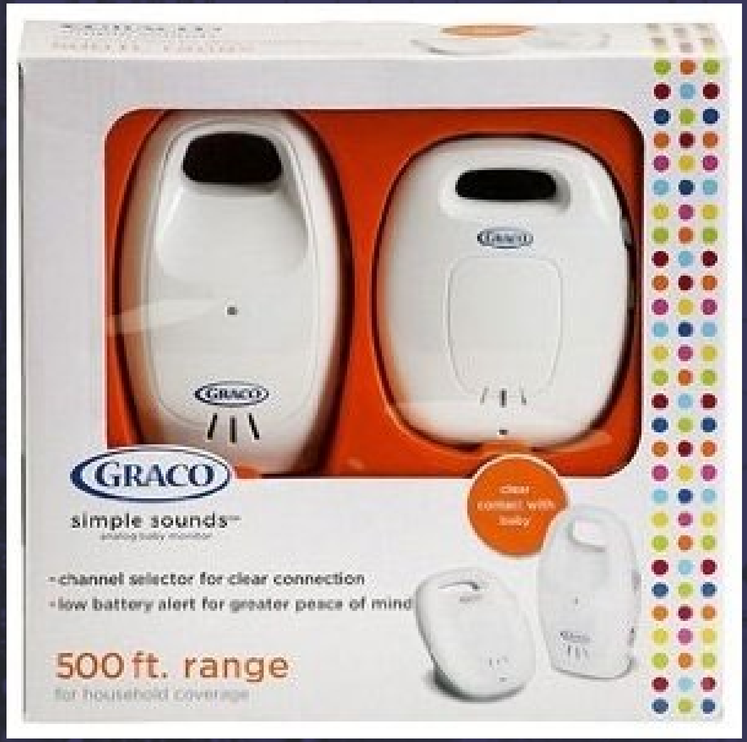
Please do not remove the device from the designated Blue Team operational perimeter.

Sponsored by:

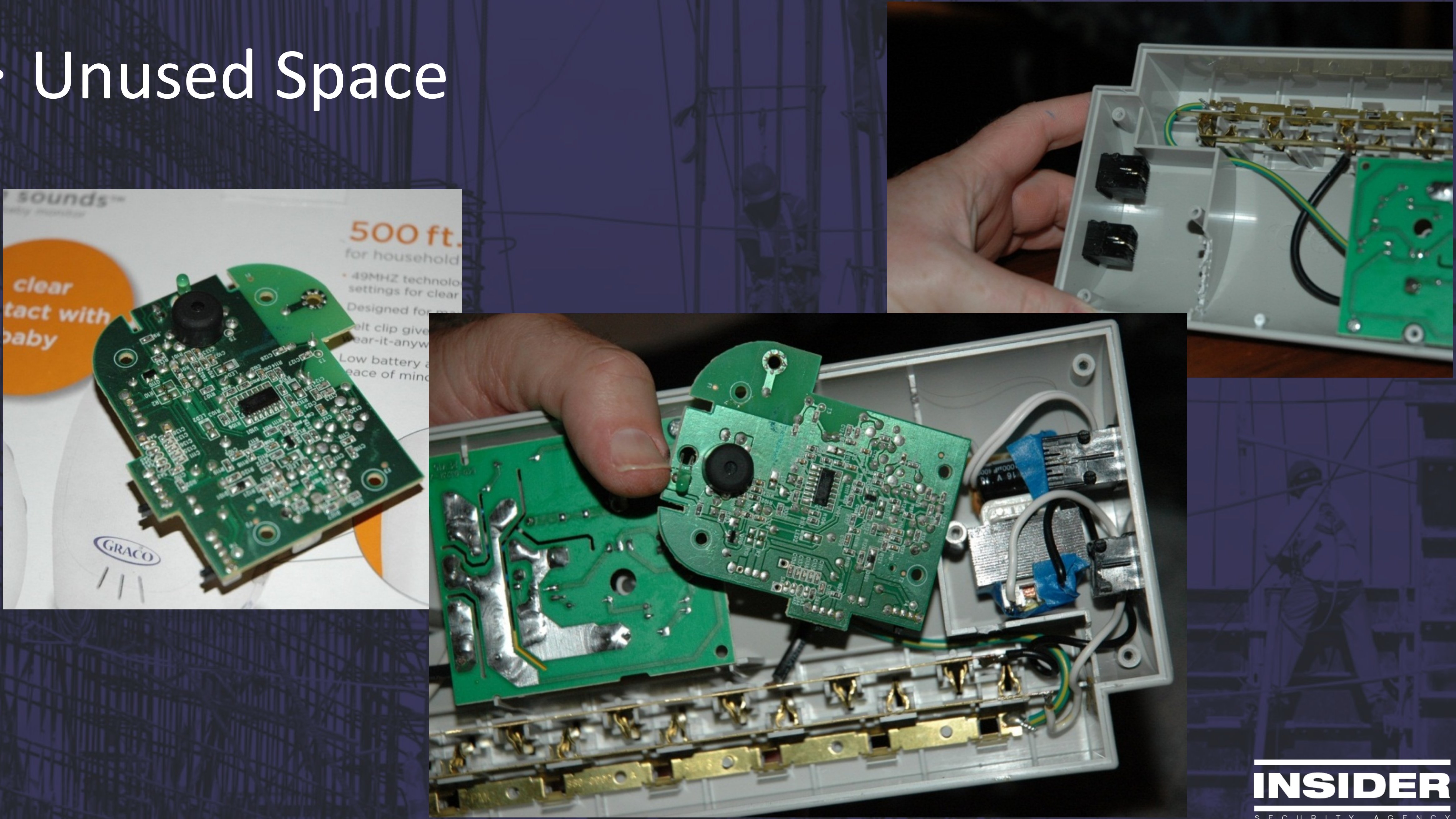
Surveillance Math



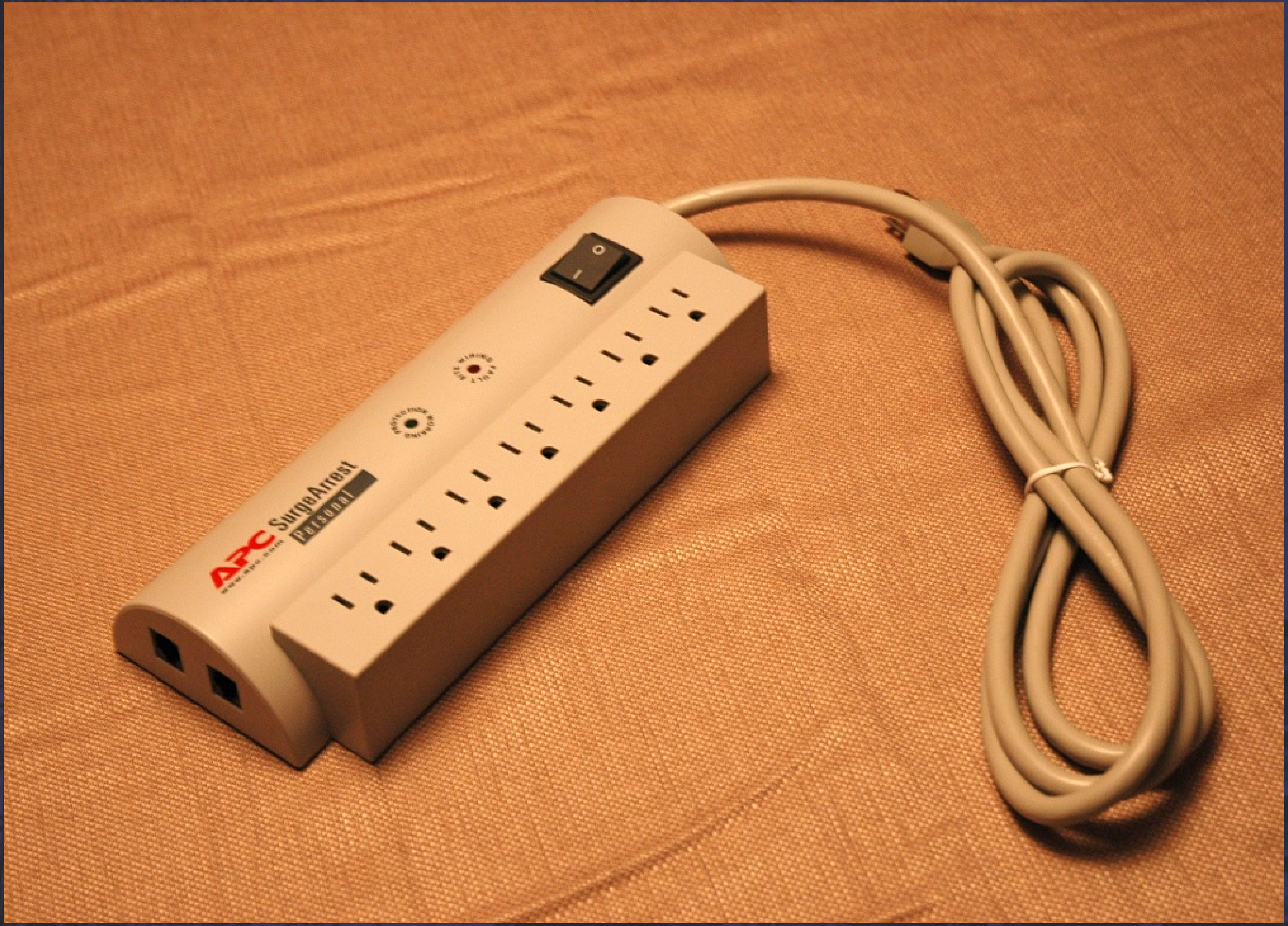
+



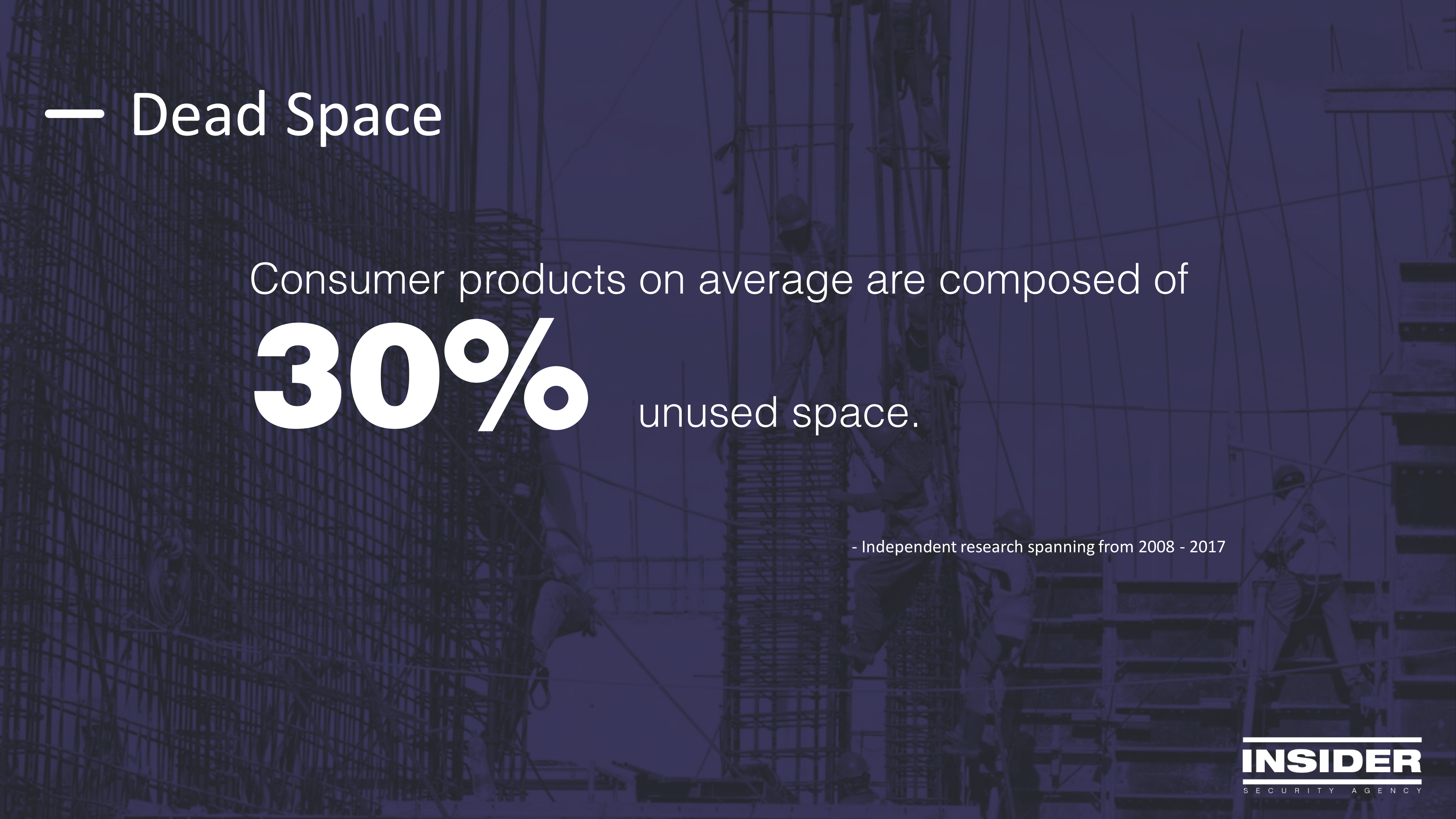
— Unused Space



Final Product



— Dead Space



Consumer products on average are composed of

30% unused space.

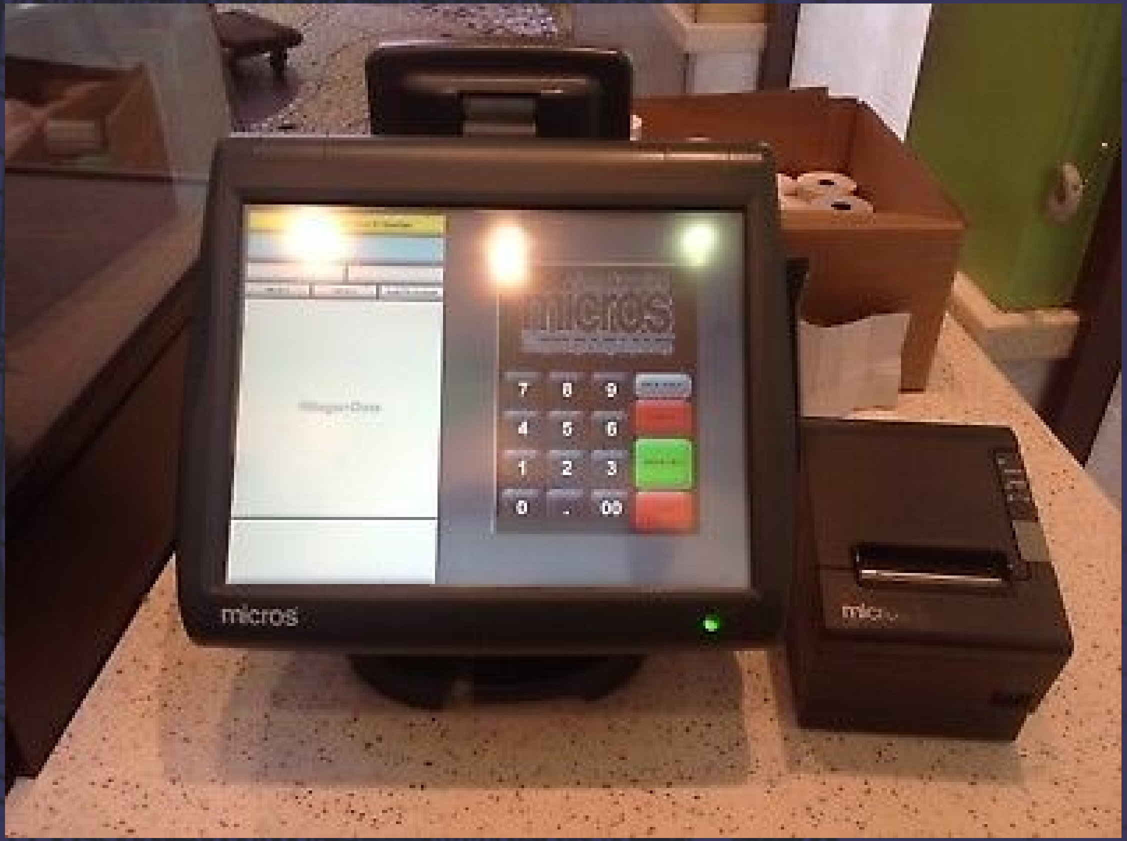
- Independent research spanning from 2008 - 2017

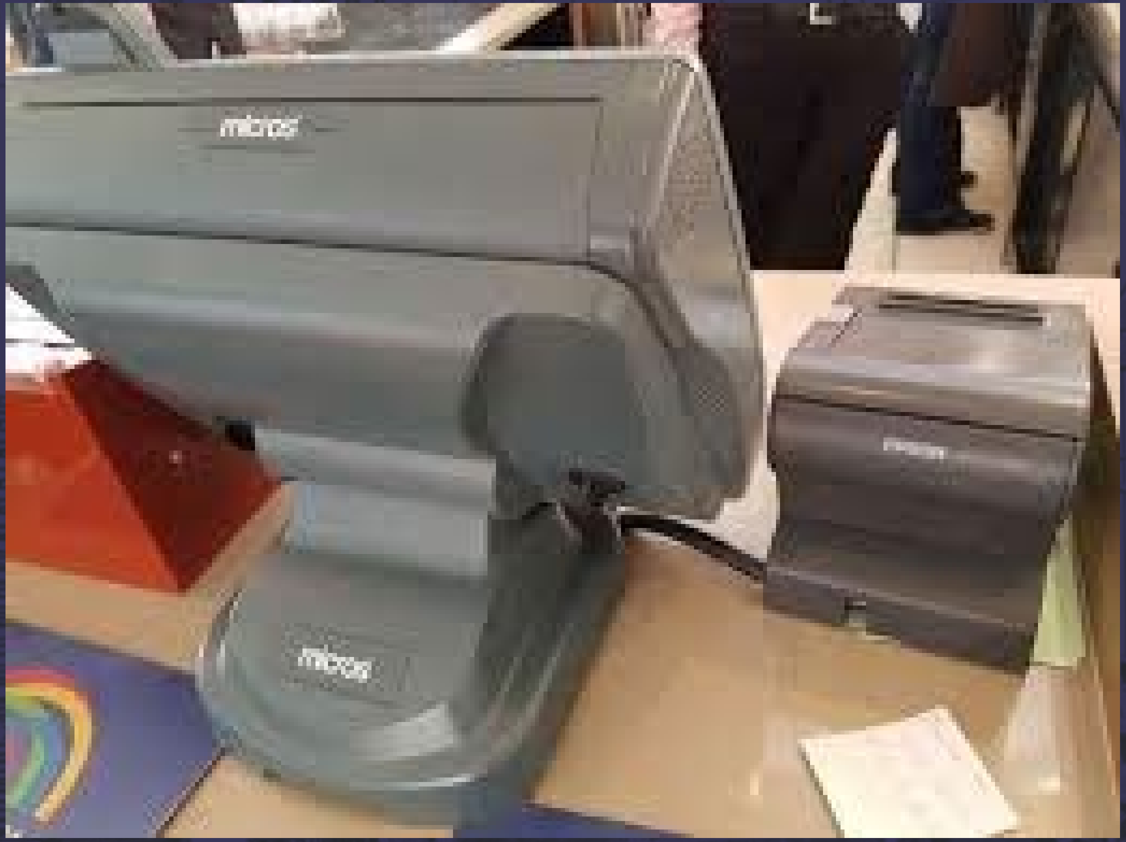
— Under Your Desk

— To the Point?

INSIDER SECURITY AGENCY

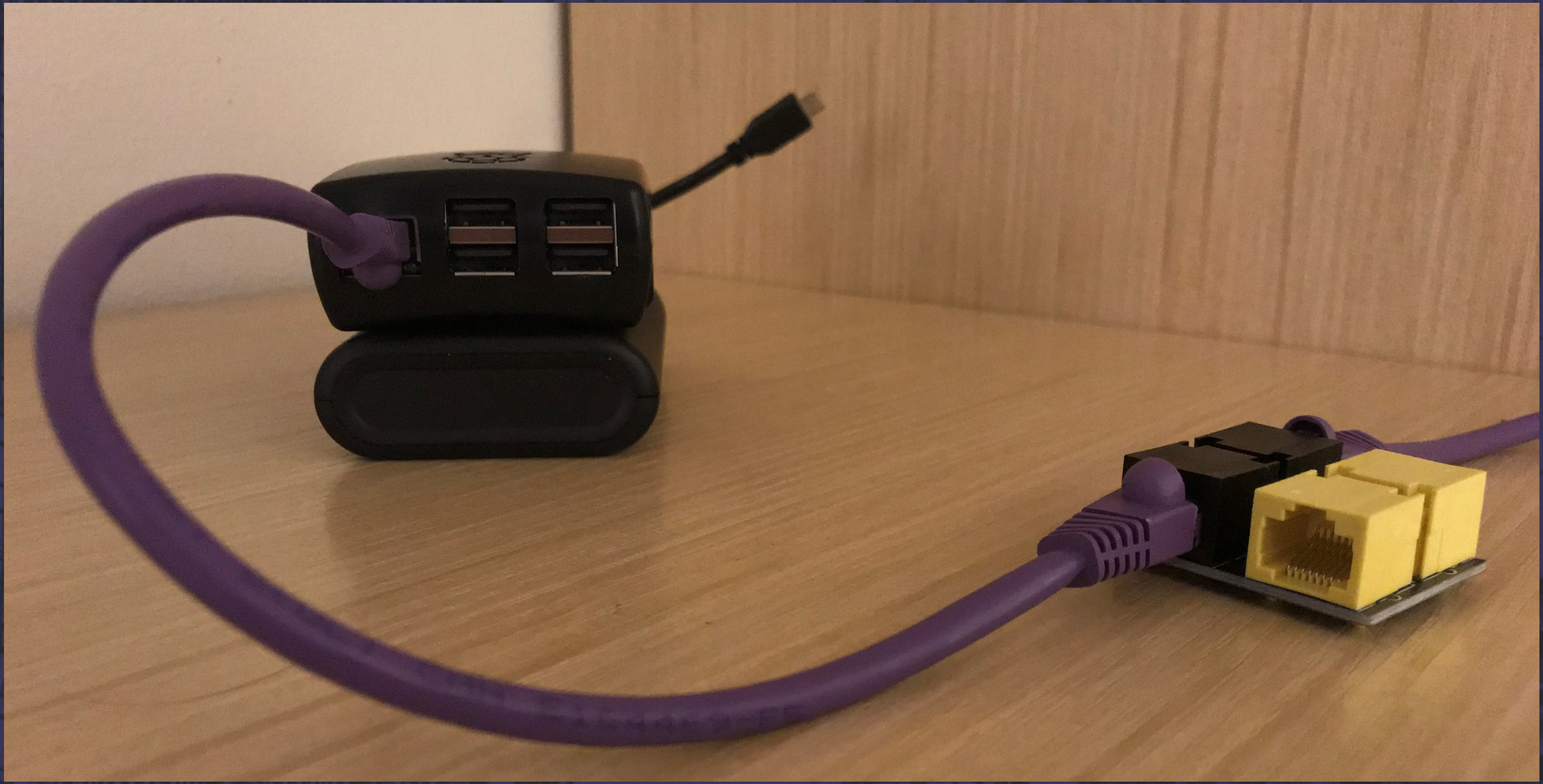
— Point of Sale (POS)





— Point of Sale (POS)

POS Implant

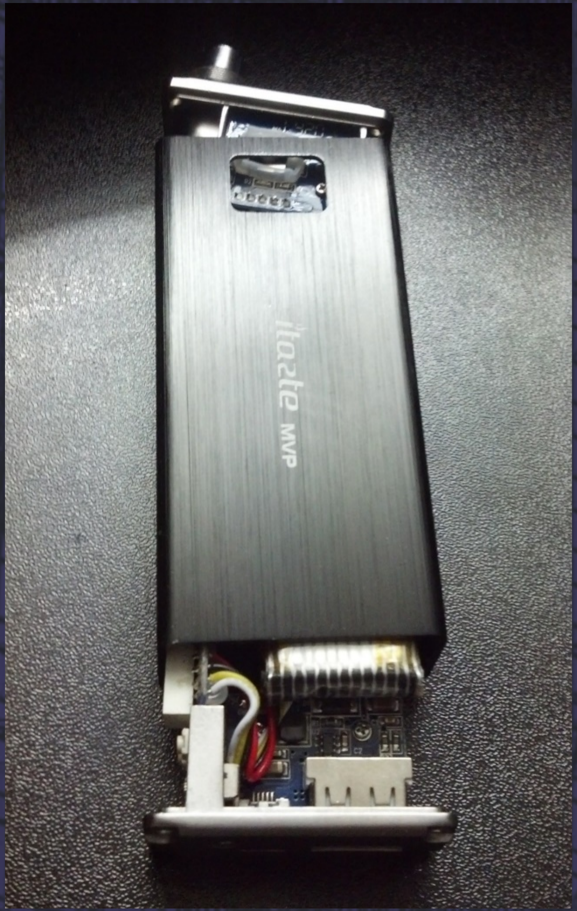


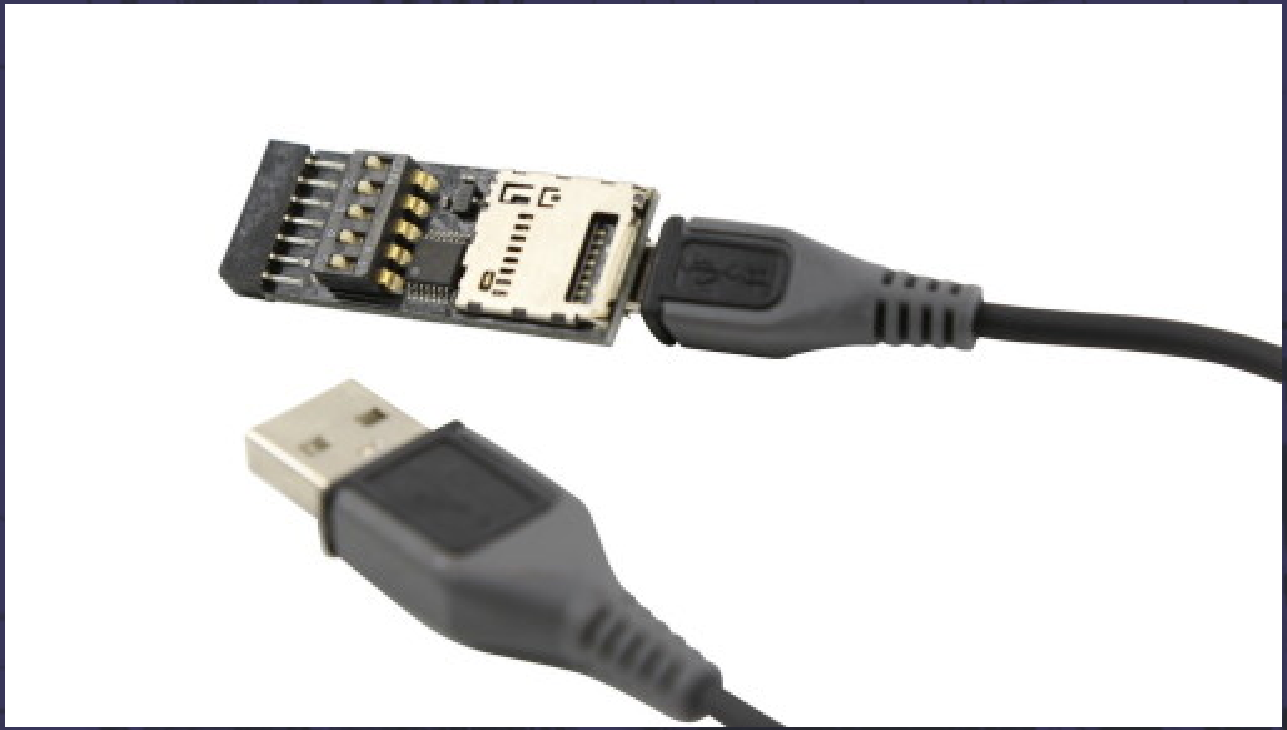
INSIDER
SECURITY AGENCY

- No Smoking = No Social Engineering?

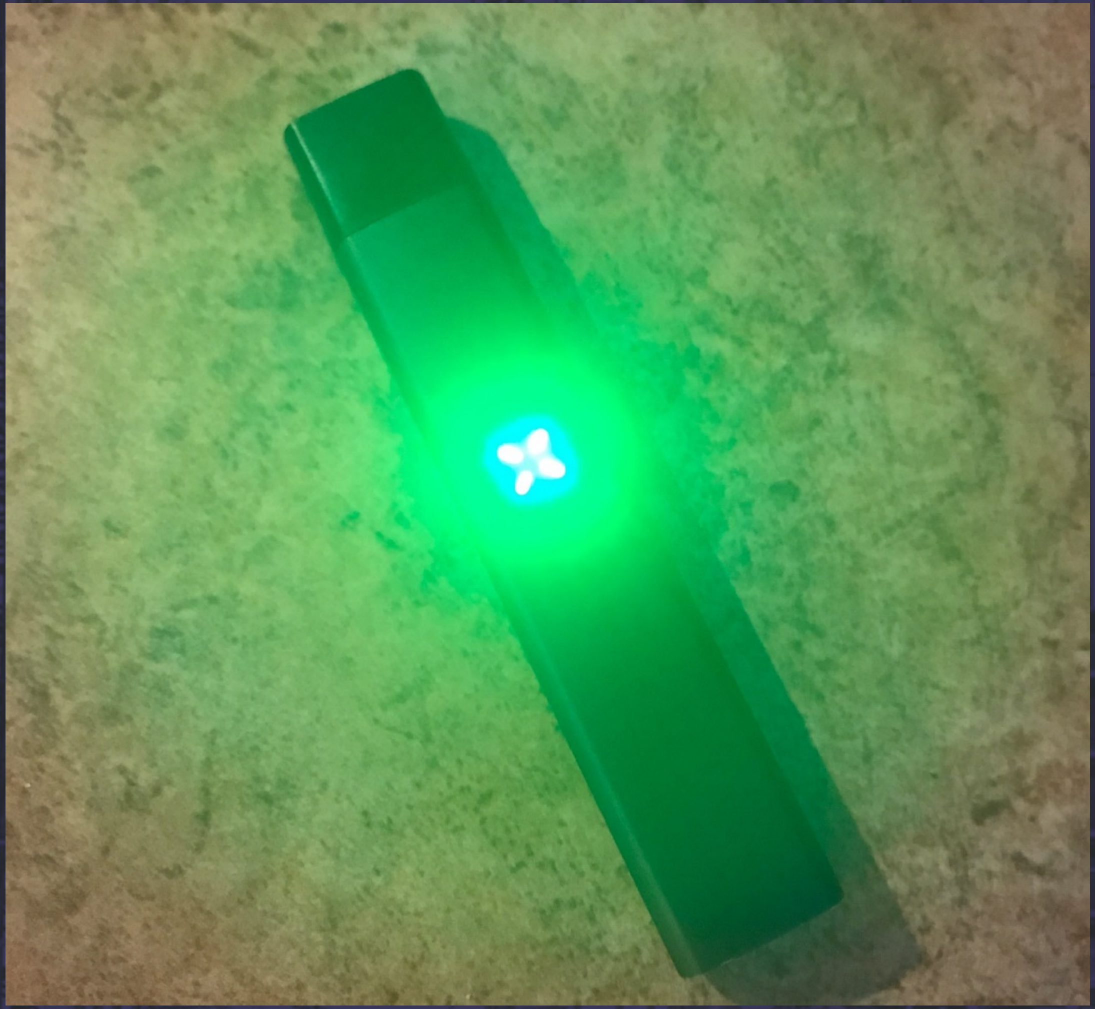
INSIDER
SECURITY AGENCY

— Vaporizer Shells



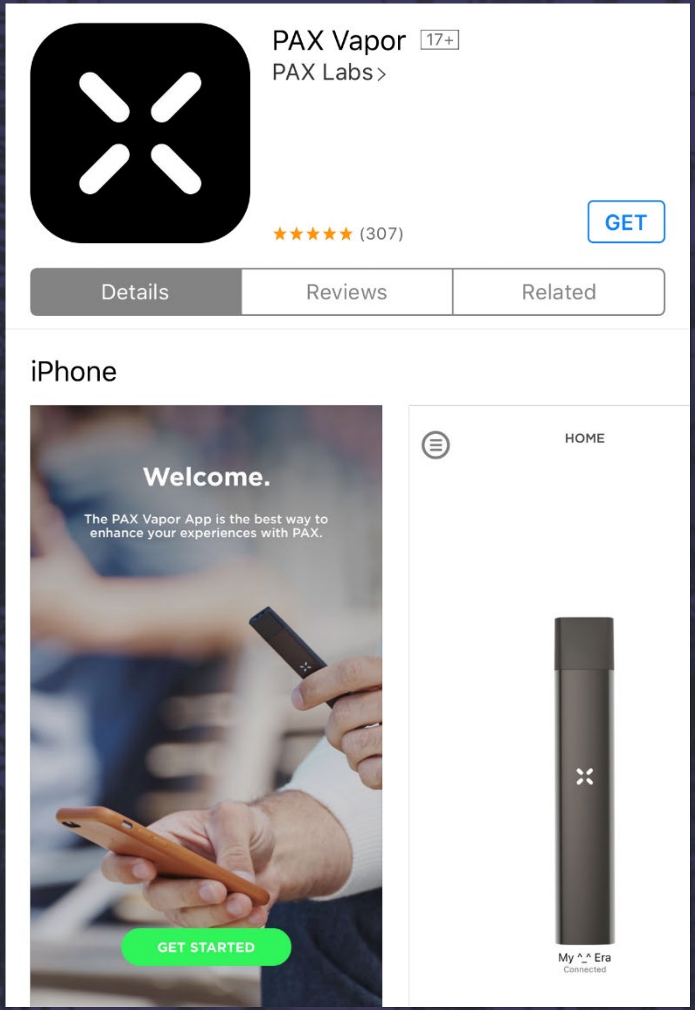


— Size Limitations?



INSIDER SECURITY AGENCY

— No Problem



PAX Vapor 17+

PAX Labs >

★★★★★ (307)

iPhone

Welcome.

The PAX Vapor App is the best way to enhance your experiences with PAX.

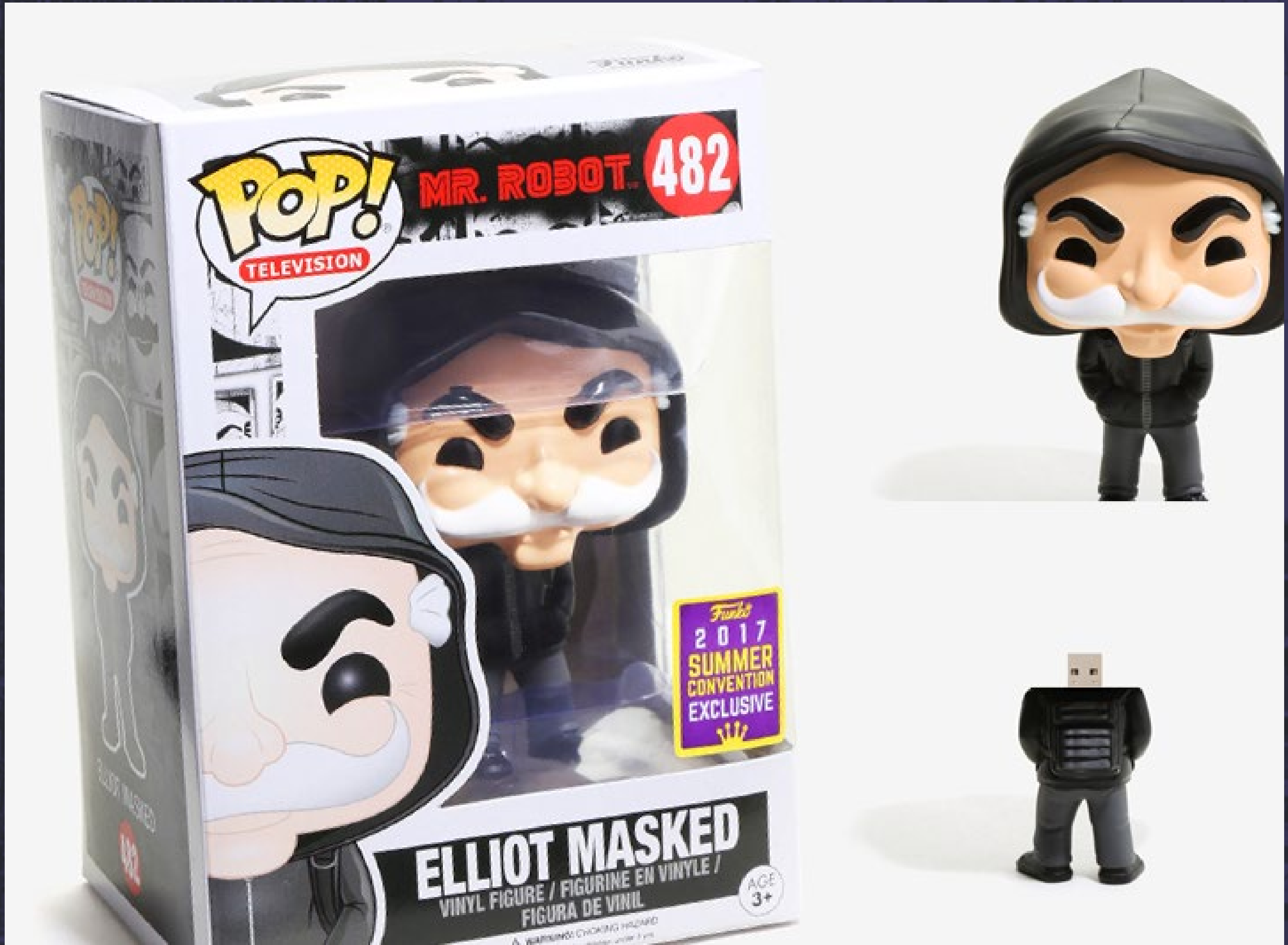
— USB?

INSIDER
SECURITY AGENCY

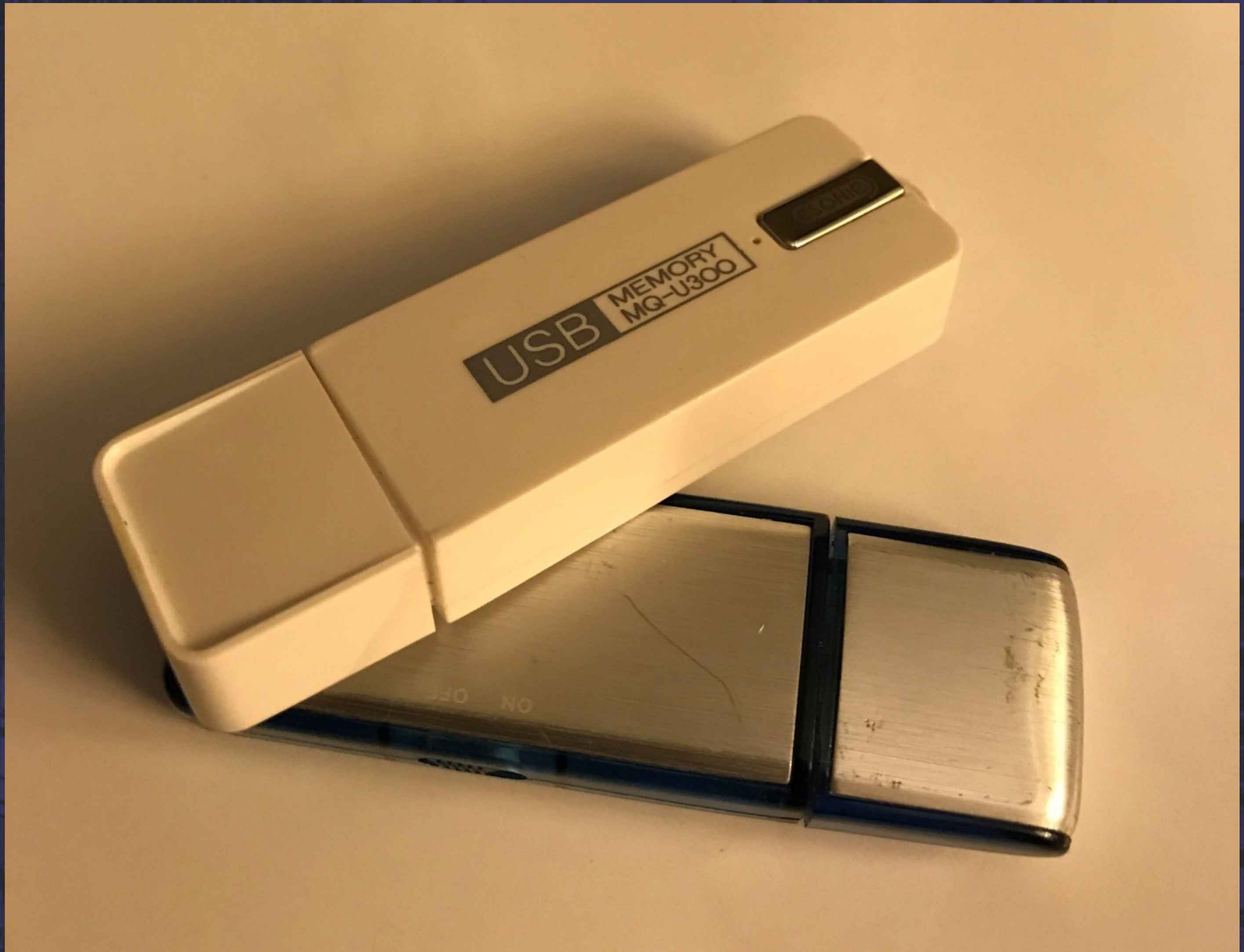
— It’s Always a Trap

INSIDER
SECURITY AGENCY

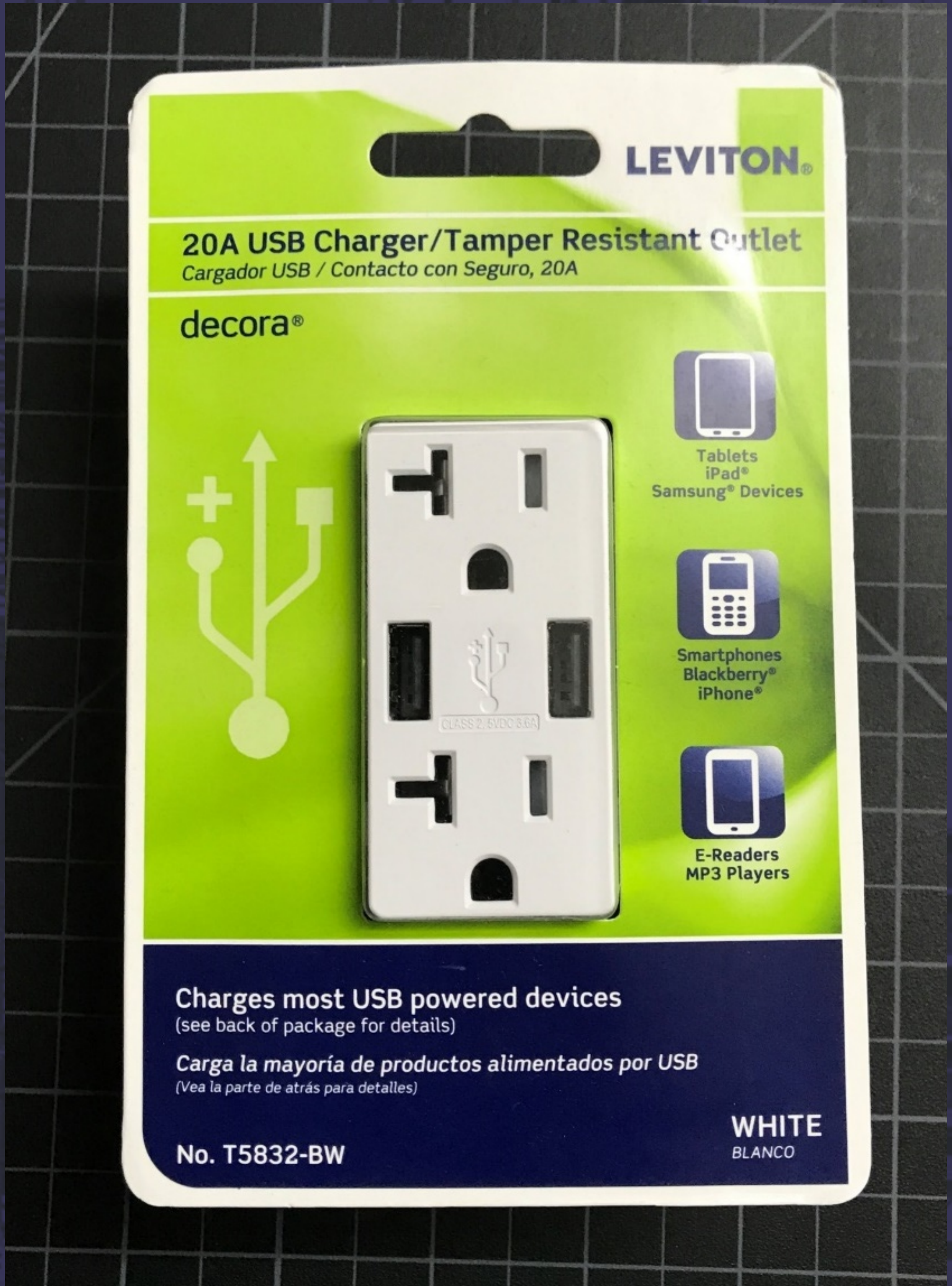
— Conference Swag



USB for the Record



— Wall Outlets

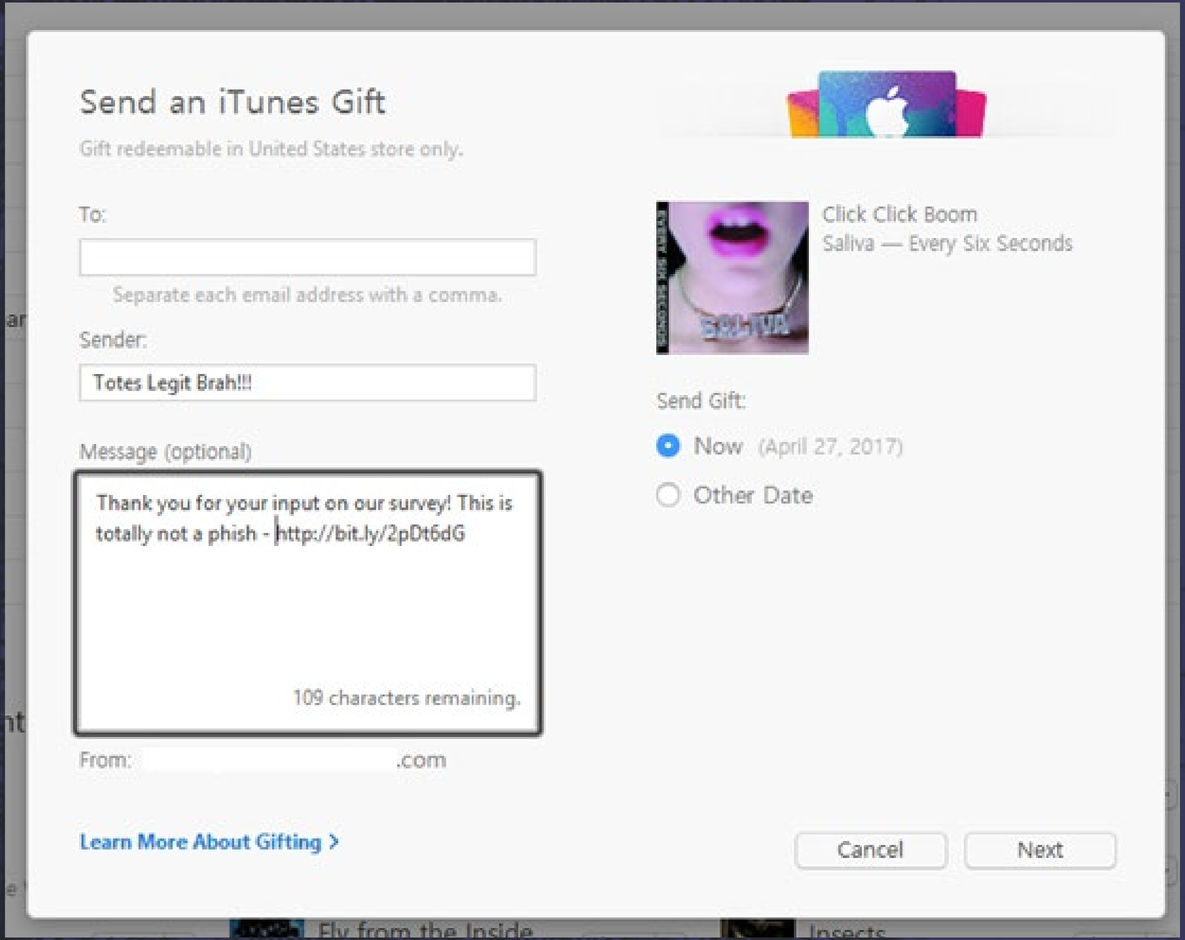

LEVITON
20A USB Charger/Tamper Resistant Outlet
Cargador USB / Contacto con Seguro, 20A
decora
Tablets
iPad
Samsung Devices
Smartphones
Blackberry
iPhone
E-Readers
MP3 Players
CLASS 2 5VDC 3.6A
Charges most USB powered devices
(see back of package for details)
Carga la mayoría de productos alimentados por USB
(Vea la parte de atrás para detalles)
No. T5832-BW
WHITE
BLANCO

INSIDER
SECURITY AGENCY

— Cell Charging Stations

— Solution or Threat?

— iPhishing



Send an iTunes Gift

Gift redeemable in United States store only.

To:

Separate each email address with a comma.

Sender:

Totes Legit Brah!!!

Message (optional)

Thank you for your input on our survey! This is totally not a phish - http://bit.ly/2pDt6dG

109 characters remaining.

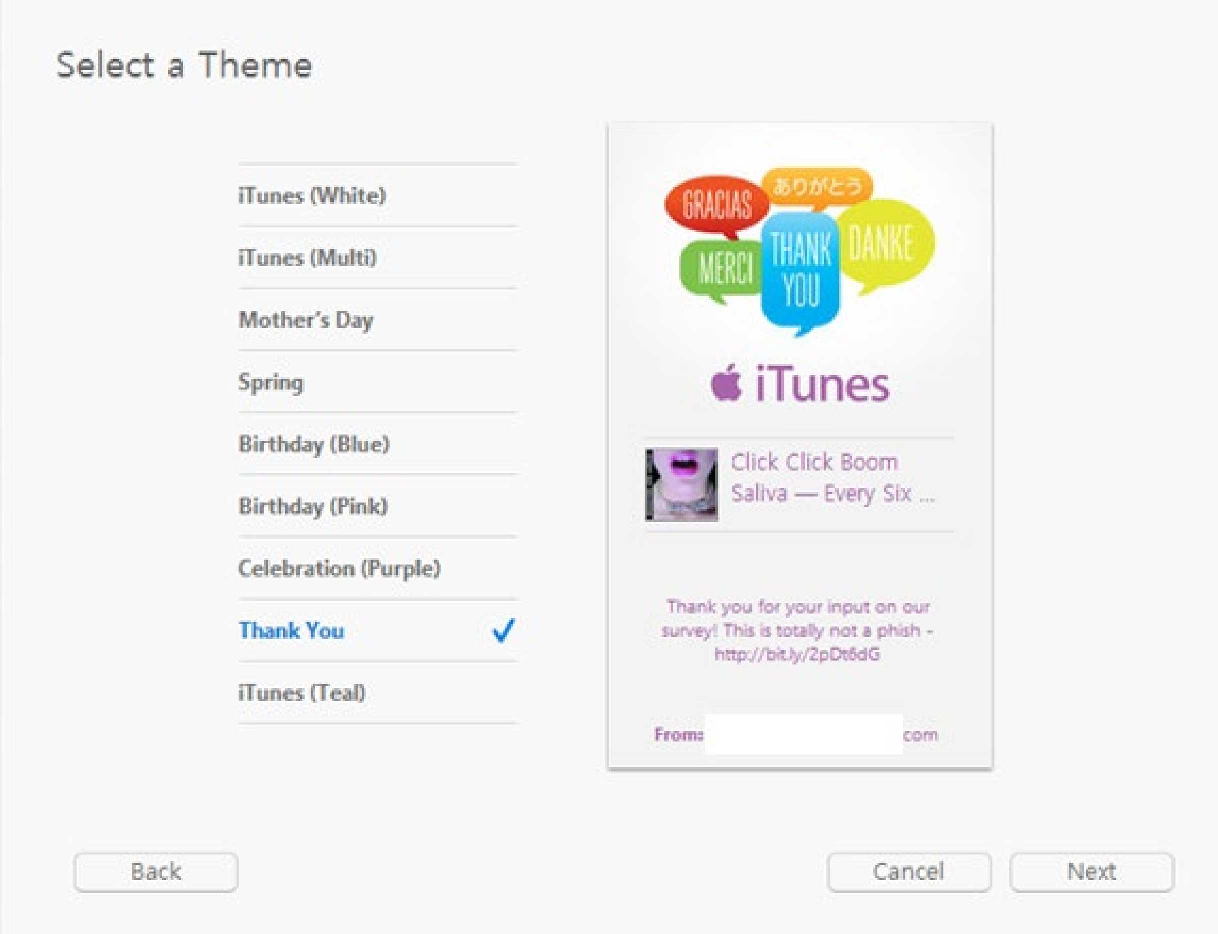
From: .com

Click Click Boom
Saliva — Every Six Seconds

Send Gift:

● Now (April 27, 2017)

○ Other Date



Select a Theme

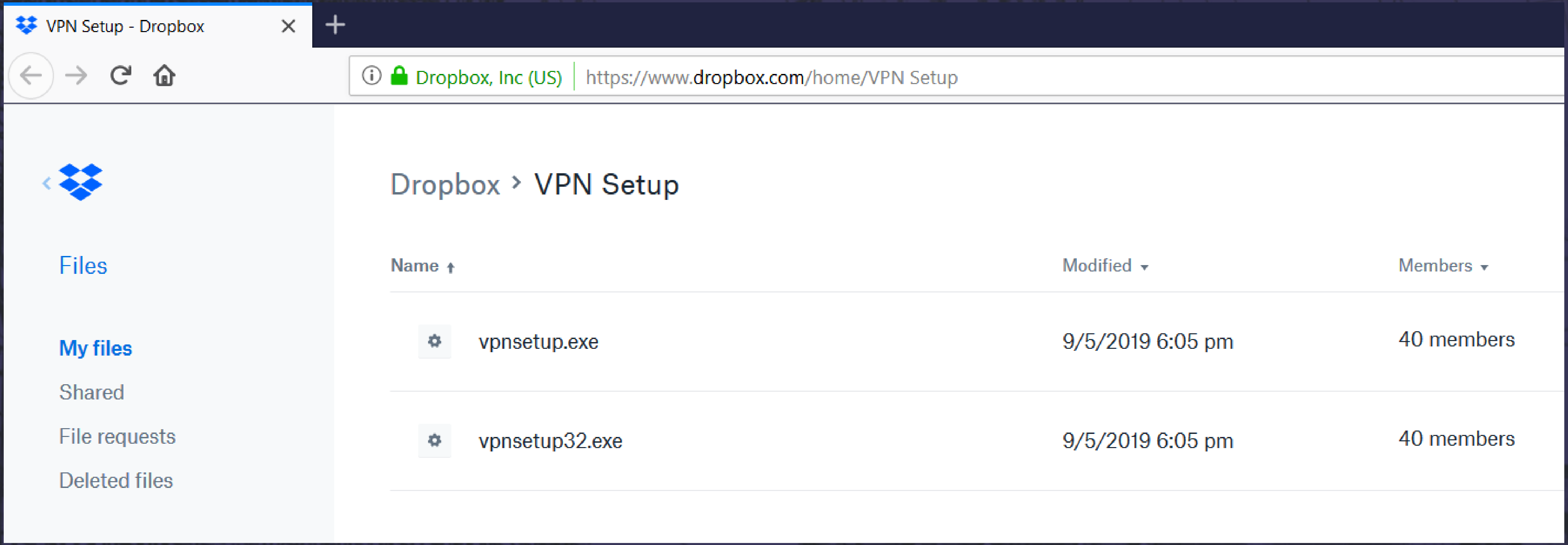
- iTunes (White)
- iTunes (Multi)
- Mother's Day
- Spring
- Birthday (Blue)
- Birthday (Pink)
- Celebration (Purple)
- Thank You ✓
- iTunes (Teal)

Click Click Boom
Saliva — Every Six ...

Thank you for your input on our survey! This is totally not a phish - http://bit.ly/2pDt6dG

From: com

— DropBox?

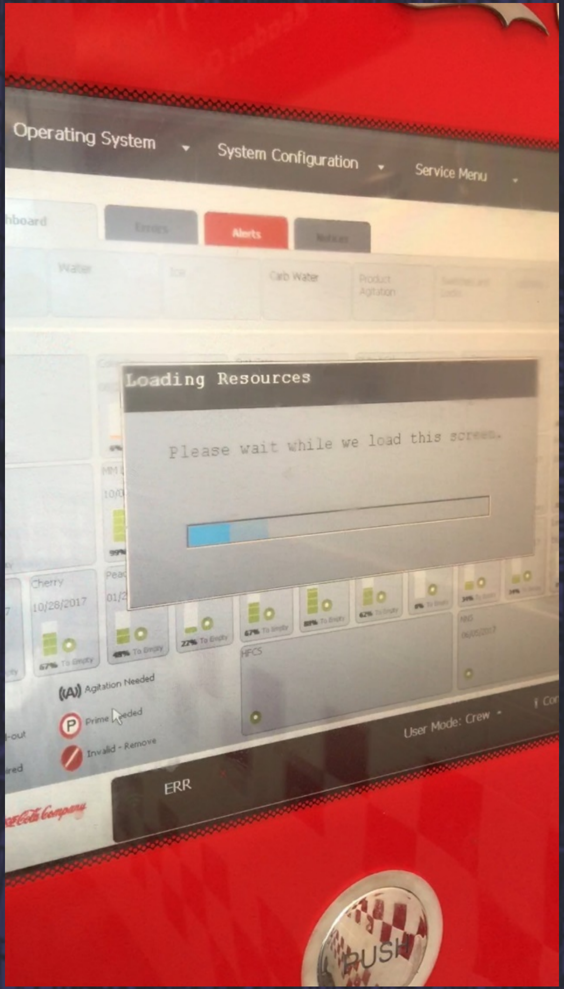


Dropbox › VPN Setup

Name	Modified	Members
vpnsetup.exe	9/5/2019 6:05 pm	40 members
vpnsetup32.exe	9/5/2019 6:05 pm	40 members

INSIDER
SECURITY AGENCY

What’s in Your Breakroom?



Loading Resources

Please wait while we load this screen.

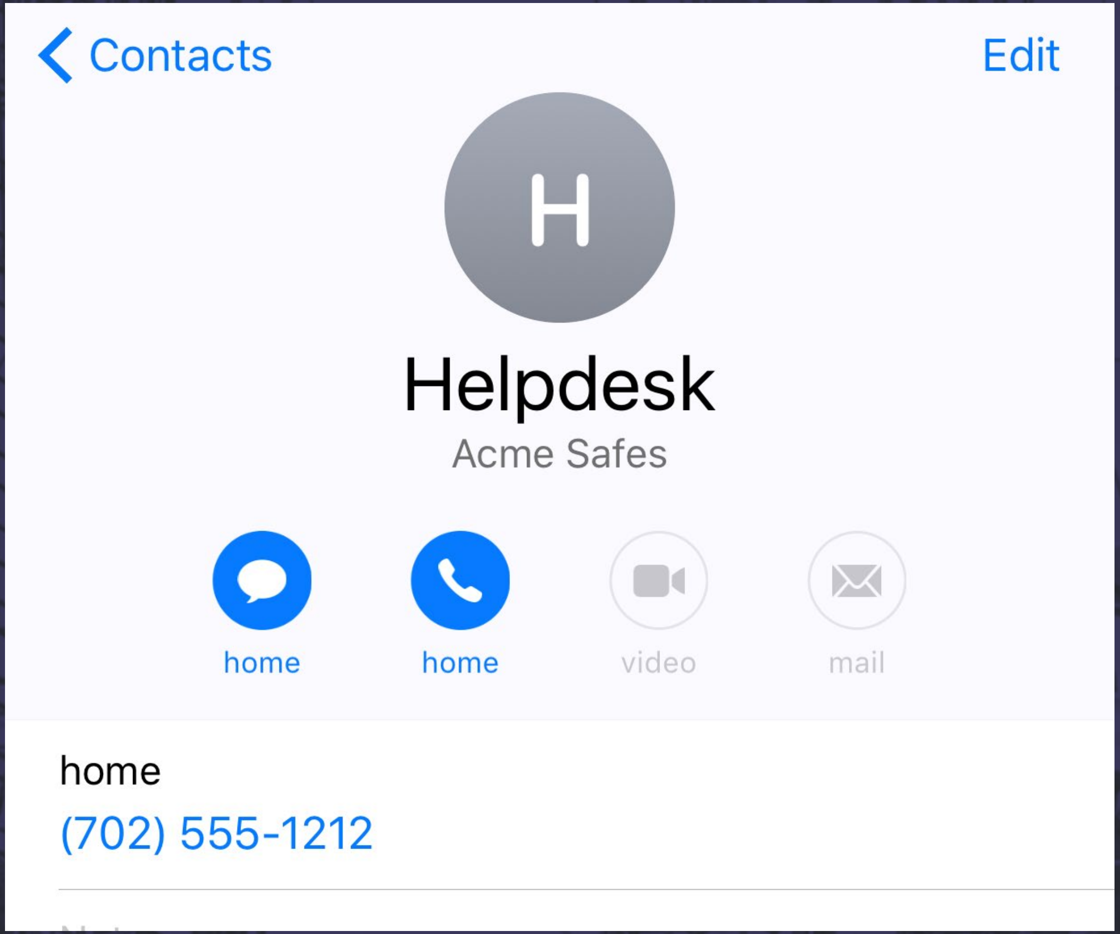
Demo Time

INSIDER
SECURITY AGENCY

RFID and NFC can be integrated into business cards, stickers and much more.

Do you have policies and guidance for your employees?

— Attack Vector



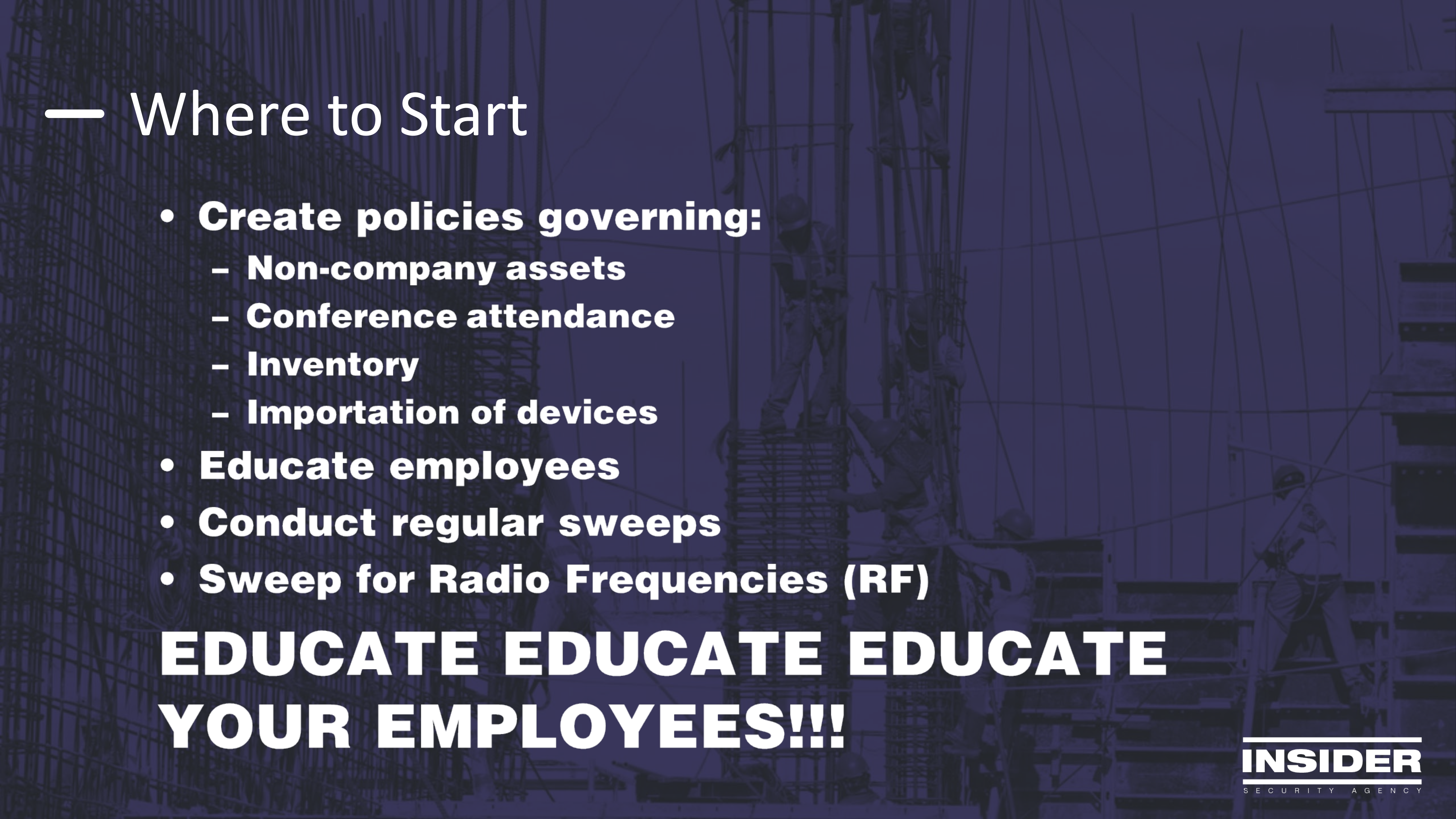
Helpdesk

Acme Safes

home

(702) 555-1212

Safe for Now



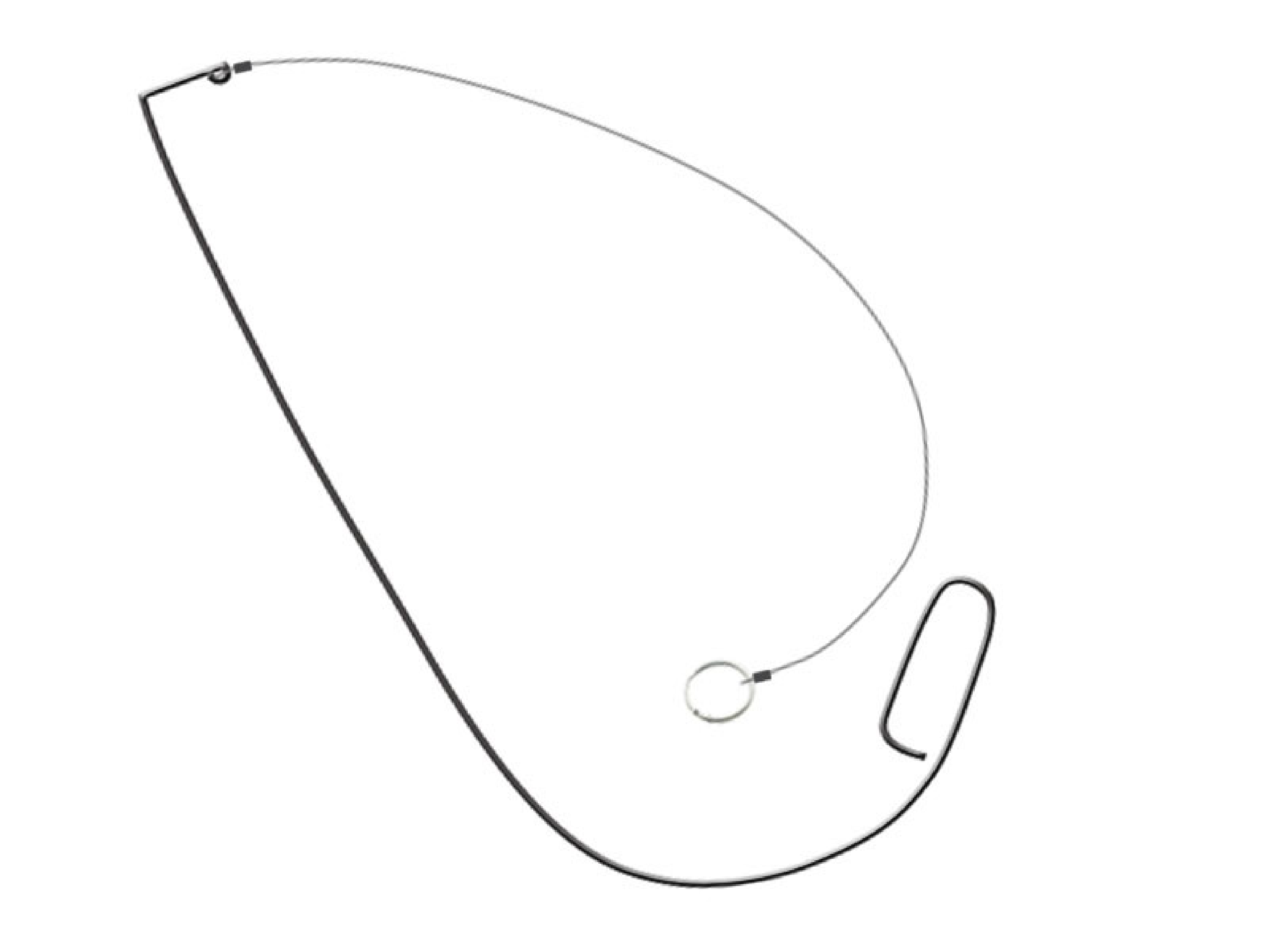
Where to Start

- **Create policies governing:**
  - **Non-company assets**
  - **Conference attendance**
  - **Inventory**
  - **Importation of devices**
- **Educate employees**
- **Conduct regular sweeps**
- **Sweep for Radio Frequencies (RF)**

EDUCATE EDUCATE EDUCATE YOUR EMPLOYEES!!!

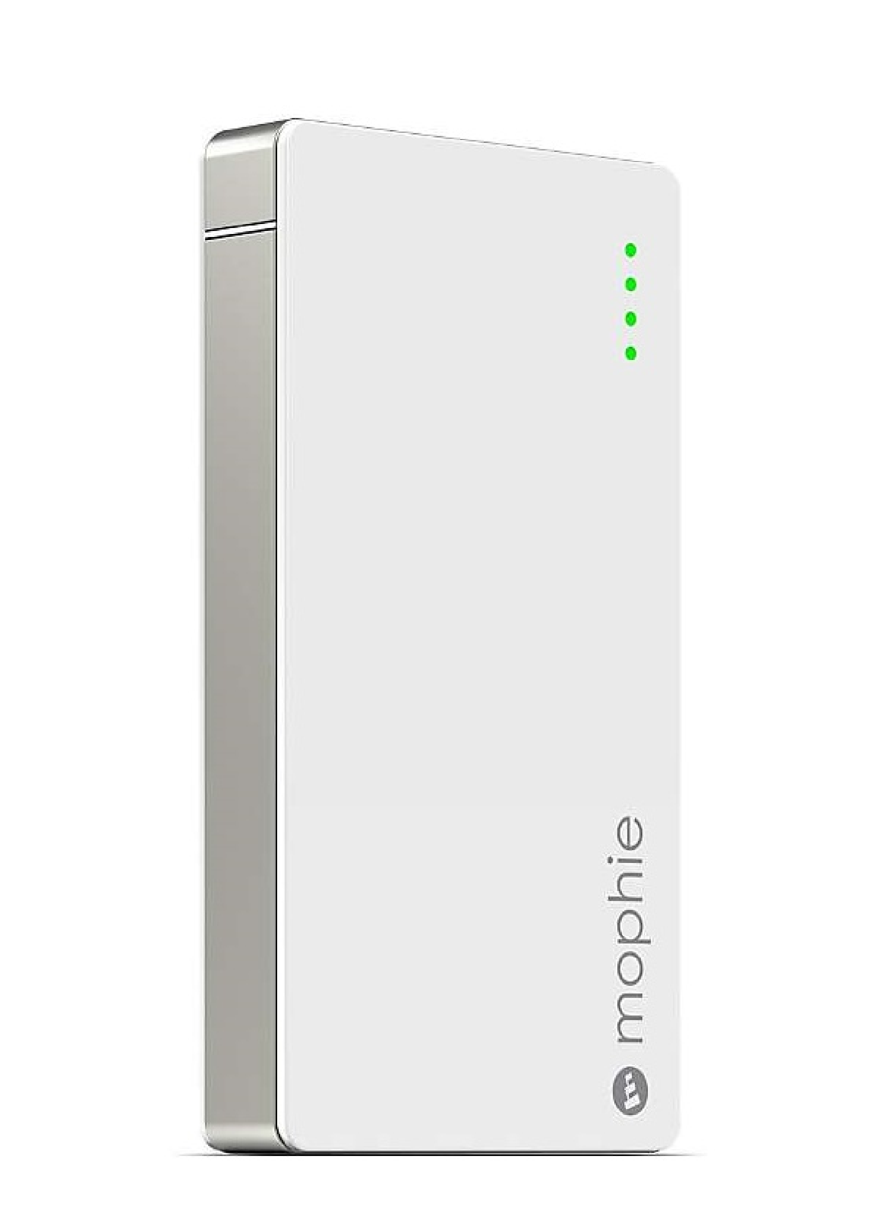
INSIDER
SECURITY AGENCY

Physical Security



Travel Safety

— Clean Power



RFID Badges

— Shielding

INSIDER

SECURITY AGENCY

Thank You

for your attention & consideration

Questions?

Twitter: @Insider_Agency

web: www.theinsideragency.com

Hashtags: #SocialEngineeringTips #SocialOperator #LearnSocialEngineering #HackerHired #HackHunger

INSIDER
SECURITY AGENCY