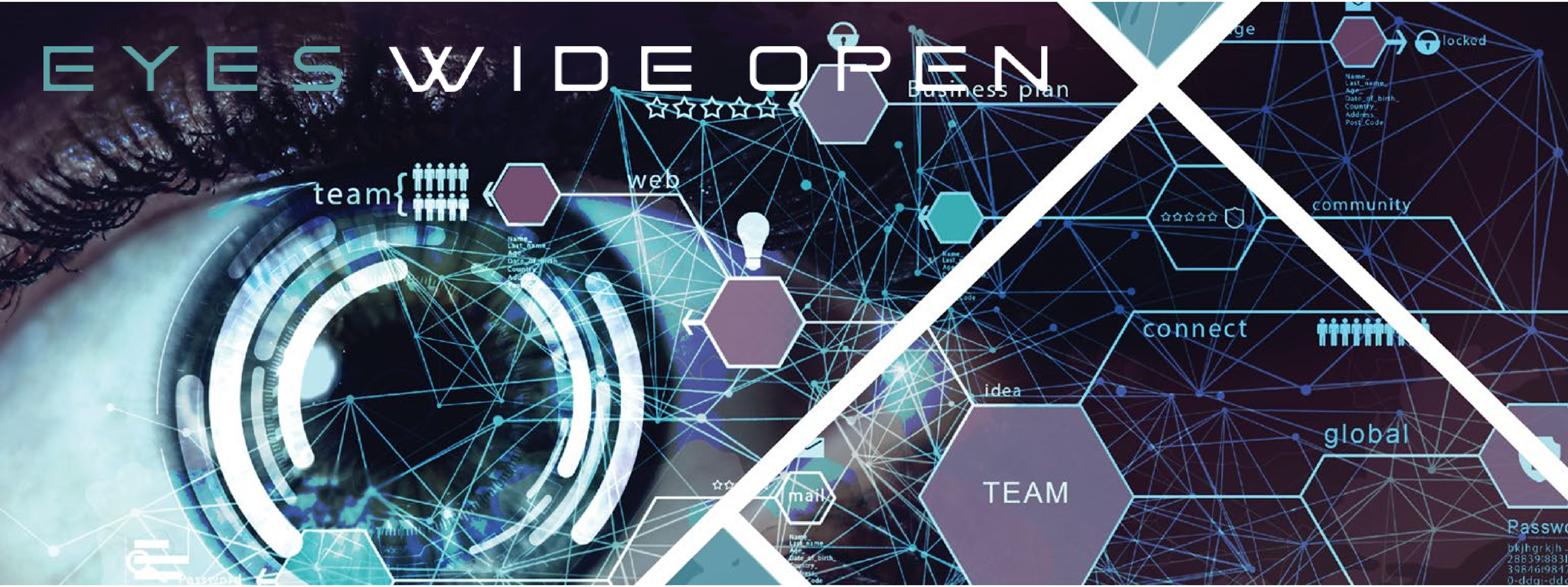
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

EYES WIDE OPEN



Not Your Average Bug Bounty: How an Email, a Shirt, and a Sticker Compromised a High Security Datacenter

Monday, October 24

2:30 –3:20 PM CT

Room:

NETSPI™

Meet Dalin from NETSPI™

- OSCP - CCNA Security - Crest CSP
- 5+ years in Penetration Testing
- 7+ in industry
- Network and Web Pen-Tester
- Lead for On-Site Social Engineering

Dalin McClellan

Senior Security Consultant

NETSPI™

What is On-Site Social Engineering?

- Penetration test focused on physical and human controls rather than technical
- Pretend to be an employee, walk around acting weird, and see what people do.
- Awesome.

NETSPI™

What are we talking about today?

Let’s Learn From Failures!

NETSPI™

The Mission

(Should You Choose To Accept It)

NETSPI™

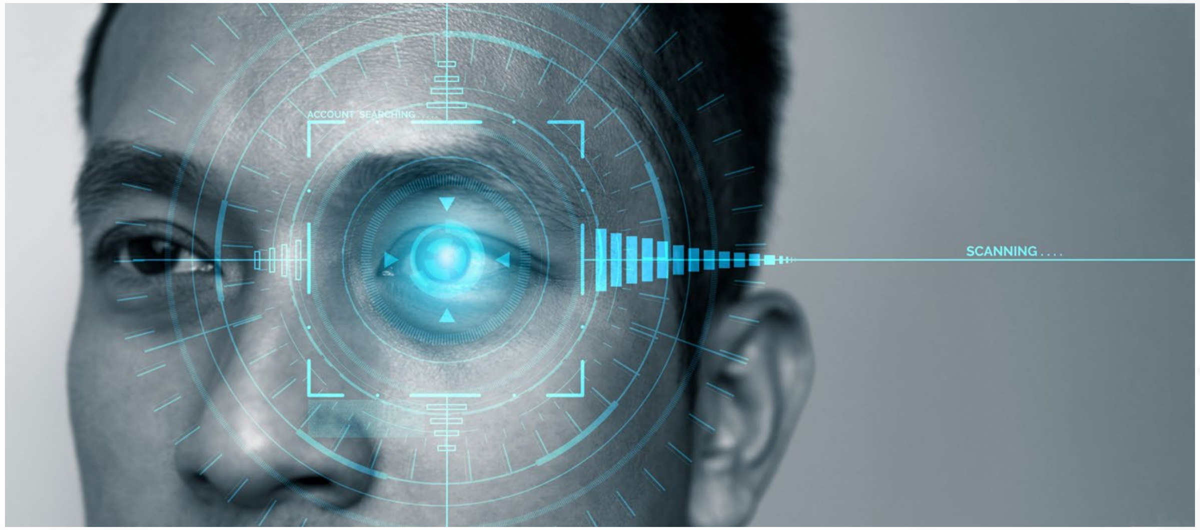
Assignment Overview

- High Security, multi-tenant Data Center
- Entire building, and the grounds are in scope.
- Phishing and Vishing in advance are ok.

That's the good news……

NETSPI™

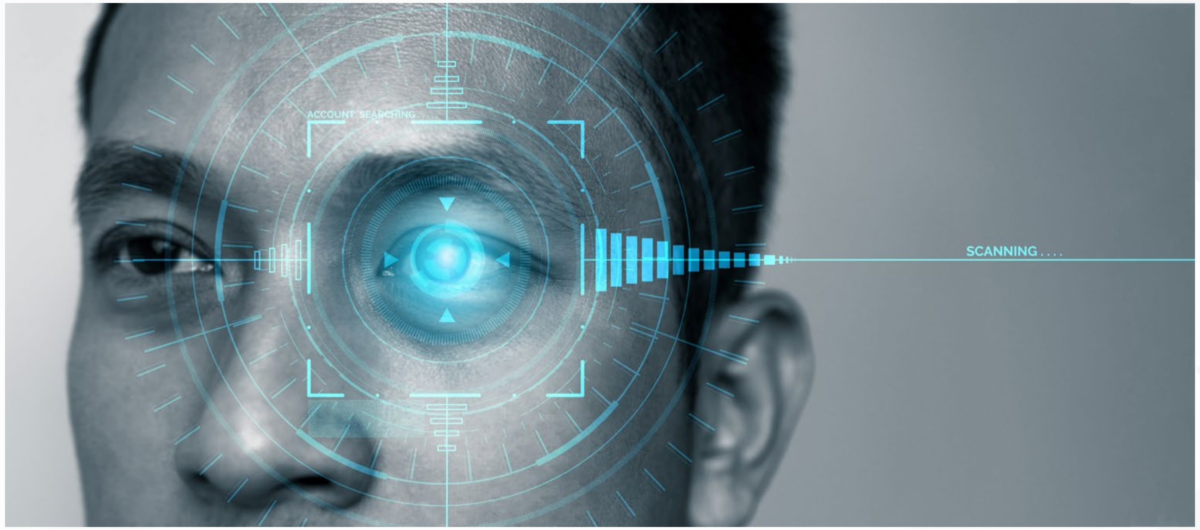
The Bad News



NETSPI™

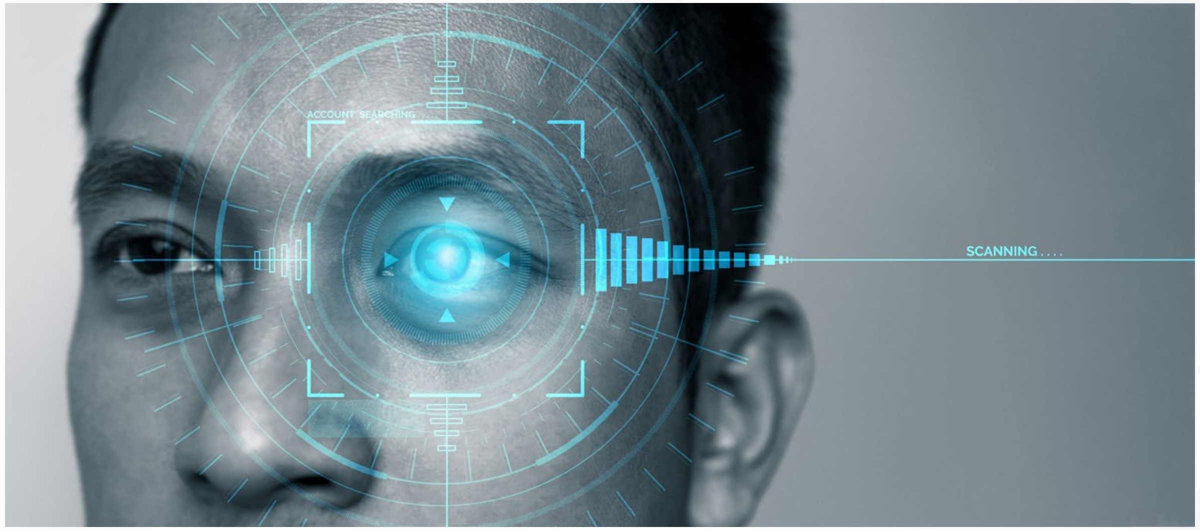
The Bad News

- 6 foot high razor-wire fence, with single gate



The Bad News

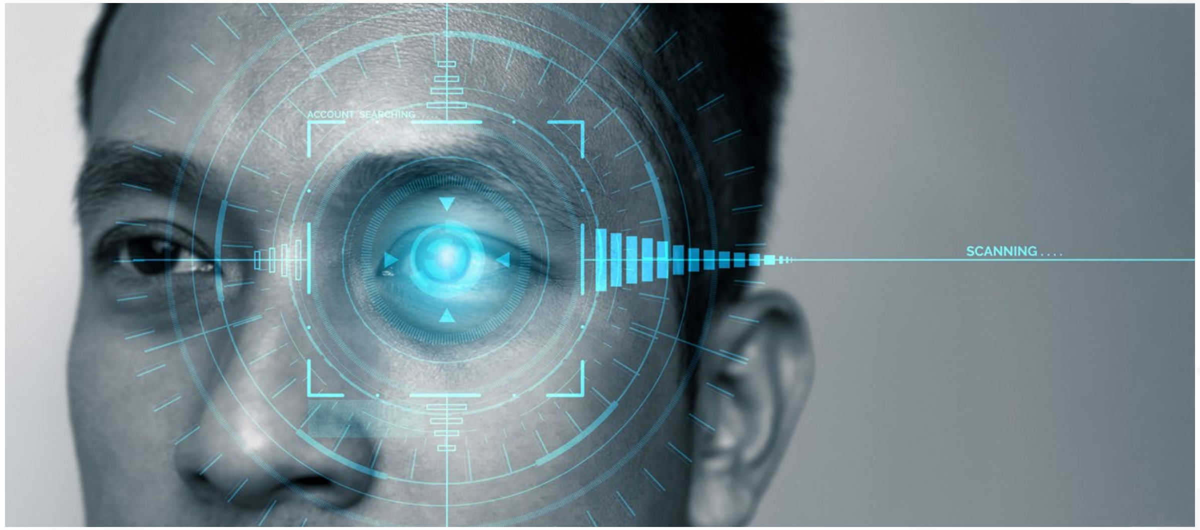
- 6 foot high razor-wire fence, with single gate
- Man-trapped doors



NETSPI™

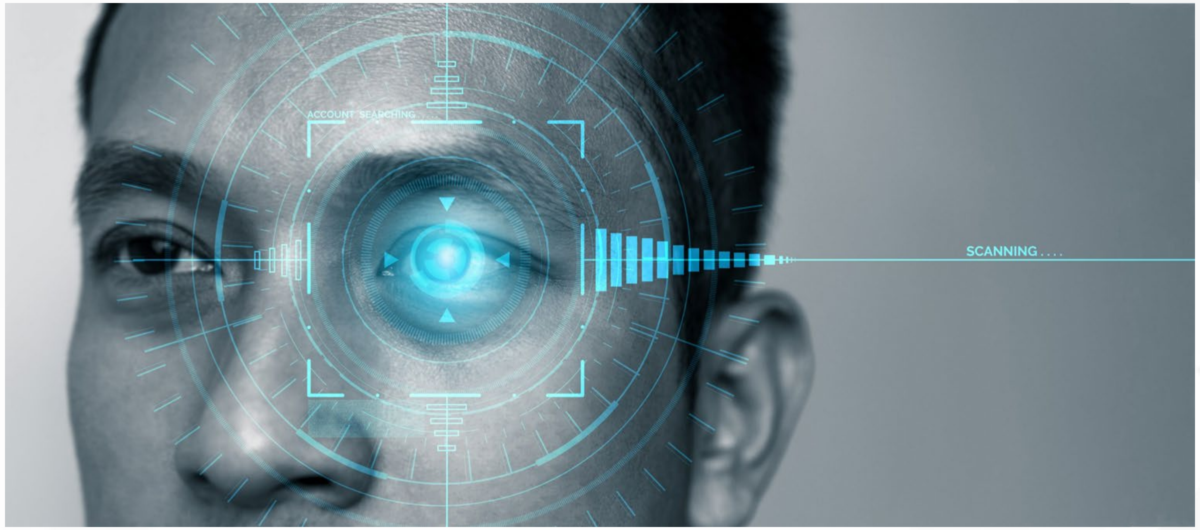
The Bad News

- 6 foot high razor-wire fence, with single gate
- Man-trapped doors
- Retina scanners



The Bad News

- 6 foot high razor-wire fence, with single gate
- Man-trapped doors
- Retina scanners
- Only two regular on-site employees, plus a third-party security guard.



NETSPI™

NETSPI™

Initial Plan

- Data center gives tours to potential clients
- Pretend to be potential new customers, schedule tour, try to break away

NETSPI™

Initial Plan

- Data center gives tours to potential clients
- Pretend to be potential new customers, schedule tour, try to break away
- “The likelihood of your injury or detainment would be high.”

NETSPI™

Initial Plan

- Data center gives tours to potential clients
- Pretend to be potential new customers, schedule tour, try to break away
- “The likelihood of your injury or detainment would be high.”

Communication is CRITICAL

NETSPI™

Preparation

- Very little time for OSINT
  - (Open-Source Intelligence)

- Who has access to the target? How do we become that person, or enlist their help?

NETSPI™

Pretext

- Results of OSINT are used to form your pretext
- Who are you, why are you here, why should you have access?

NETSPI™

Partner With Your Client

- White-box your OSINT

Partner With Your Client

- White-box your OSINT

- *Key information:*
  Access Policies | Employee names | Email Addresses | Outside Vendors

NETSPI™

The Set Up

- Recent service emails as templates
- Lookalike domain to send email from one employee to the other
- Phishing Email

Pretext

- Pest Control, coming in to do “Winter Pest Proofing”
- T-shirt, vinyl decal, etc. Less than a day
- On site: truck, ladder, bag, rat traps
- Total cost: <$150

How I Thought I Looked…

NETSPI™

How I Actually Looked…

How I Actually Looked…

Whatever, it was good enough!

NETSPI™

Success!

- Security guard opened the gate. Employee swiped badge, let us follow through mantrap, scanned his eyeballs

NETSPI™

Success!

- Security guard opened the gate. Employee swiped badge, let us follow through mantrap, scanned his eyeballs
- Full tour of the facility including power center, central networking, and DEMARC. Access to ceiling space and under-floor space with lots of unsecured network cables.

Success!

- Security guard opened the gate. Employee swiped badge, let us follow through mantrap, scanned his eyeballs

- Full tour of the facility including power center, central networking, and DEMARC. Access to ceiling space and under-floor space with lots of unsecured network cables.

- Photos of customers screens, and security room monitors.

Success!

- Security guard opened the gate. Employee swiped badge, let us follow through mantrap, scanned his eyeballs

- Full tour of the facility including power center, central networking, and DEMARC. Access to ceiling space and under-floor space with lots of unsecured network cables.

- Photos of customers screens, and security room monitors.

- Walked out undetected.

But wait, there's more….

NETSPI™

But wait, there's more….

- No network access.

But wait, there's more….

- No network access.
- "Need to print some paperwork"

NETSPI™

But wait, there's more….

- No network access.
- "Need to print some paperwork"
- Let us back in, got us on the Wi-Fi.

NETSPI™

But wait, there's more….

- No network access.
- "Need to print some paperwork"
- Let us back in, got us on the Wi-Fi.
- Accepted an email with a document attachment, opened the attachment, and printed it for us.

NETSPI™

LESSONS LEARNED

NETSPI™

Identify the Problem

- There's some major problems here with a single individual, and they need to be fixed.
- This guy really needs to reexamine the way he's doing his job
- We need talk about…..

NETSPI™

THIS GUY

Let's Start Over

NETSPI™

Policy and Procedure

- Primary Vulnerability: Vendor visits have no clearly defined policy.

- You can’t hold someone accountable for not following rules which don’t exist.

NETSPI™

Policy and Procedure

- Primary Vulnerability: Vendor visits have no clearly defined policy.

- You can't hold someone accountable for not following rules which don't exist.

- **Visual identification is terrible, especially in 2022.**

NETSPI™

Remember this guy?

This is what the actual companies uniform looks like.

NETSPI™

Don’t expect people will know who belongs and who doesn’t based on how they look. PERIOD.

NETSPI™

Email Phishing

- Phishing is the number one source of breaches.
  (Has been for a long time)

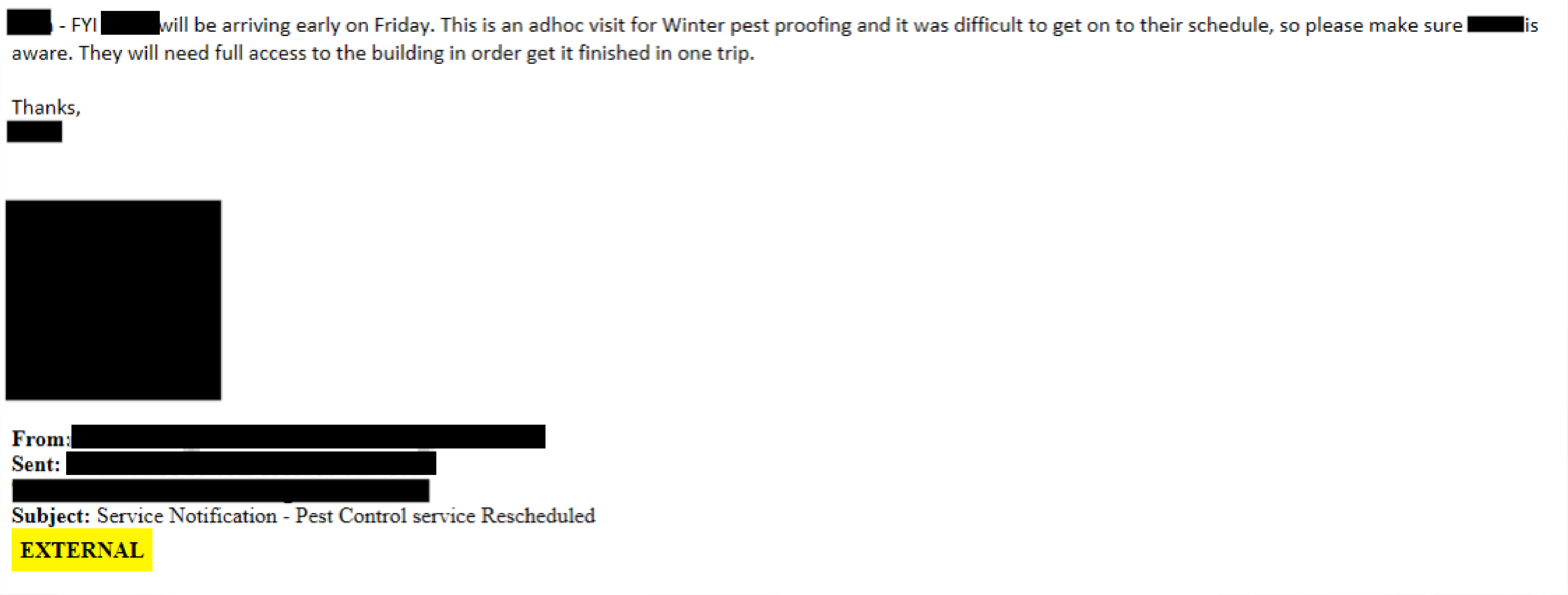
- Humans will fail eventually, but technology can help

- Lookalike domain was less than 1 day old, and only 1 letter different than recipient domain.

- Why was it even delivered in the first place?

NETSPI™

- Screenshot of email, as received.



[redacted] - FYI [redacted] will be arriving early on Friday. This is an adhoc visit for Winter pest proofing and it was difficult to get on to their schedule, so please make sure [redacted] is aware. They will need full access to the building in order get it finished in one trip.

Thanks,
[redacted]

[redacted]

From: [redacted]
Sent: [redacted]
[redacted]
Subject: Service Notification - Pest Control service Rescheduled

EXTERNAL

Successes

- Plenty of things went right, and they were all him.
- We never actually got hands on a computer, not for lack of trying.
- We were never left unescorted, not for lack of trying.
- Isolated guest Wi-Fi, temporary credentials

NETSPI™

Recommendations

- Look for edge cases. Have default plans if something arises which hasn’t been considered before.
- Implement strong technical controls wherever possible
- Defense in depth – If one person can make a small mistake which results in total compromise of the organization, the problem is the organization.
- Make Victims Your Advisors and Advocates, Not Your Scapegoats.

NETSPI™

Final Thoughts

- Don’t be a jerk.
- Highlight successes along with addressing failures.
- Security needs to be a collaborative process between everyone.
- The story you tell may be impressive, but HOW you tell the story will determine if anything good ever comes of it.

NETSPI™

Connect With Me!

Twitter: @mdalin
LinkedIn: mdalin

Visit me at
NetSPI's booth **#200**

Dalin McClellan

Senior Security Consultant

NETSPI™

MUCH MORE THAN A PENTESTING COMPANY

WWW.NETSPI.COM

NETSPI™