Midwest Meets Middle East: Targeted Security Program Tips for an Evolving Cyber Battlefield

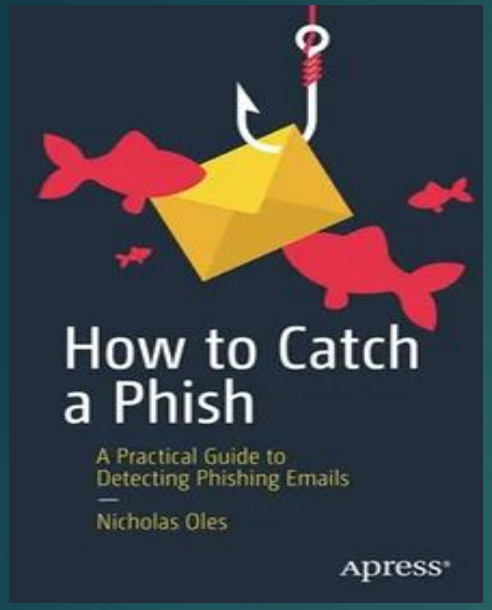
PRESENTED BY NICK OLES

THE NET DEFENDER

Agenda

- Introduction
- Three Rules of Special Operations with an IR Twist
- Building Networks – ISAC Way
- War Story 1
- Effective Communication
- War Story 2
- Impostor Syndrome
- Key Terrain
- Compliance Programs
- Tips/Tricks
- Questions

Who Am I?



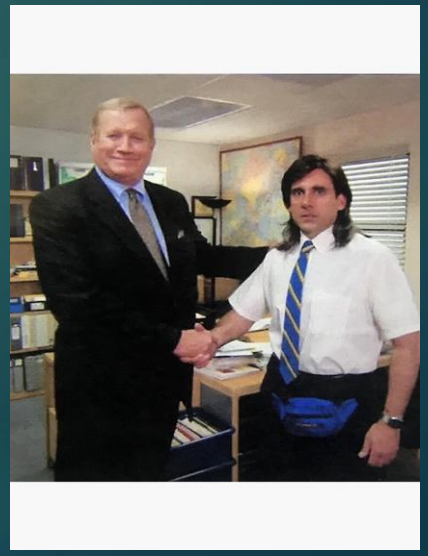
- 15 years in IT/Cybersecurity.
- Military, government, civilian roles.
- Published author and speaker.
- Responded to thousands of email and security incidents.
- Midwest to Middle East.
- Special Operations Advisor and veteran.
- BA in Accounting MS in Cybersecurity.
- 7 certifications (no CISSP).
- 1000's of hours of formalized government and private sector training.

Three Rules of Special Operations

- **1. Always look cool.**
- **2. Never get lost.**
- **3. If you get lost, look cool.**

Three Rules of Special Operations

- **1. Always look cool.**
  - **Take care of yourself.**
    - **Do something you love everyday.**
  - **Be a good person.**
  - **Dress well.**



Three Rules of Special Operations

- **2. Never get lost.**
  - **One is none, two is one. Bring 2 of everything.**
    - **Hard copies of policies.**
  - **Anticipate adjusting your plan.**
    - **External comms plans. Burner emails/phone numbers.**
  - **Train hard, communicate often.**
    - **Purple team, TTX's, do what your plan says you are going do to.**

Three Rules of Special Operations

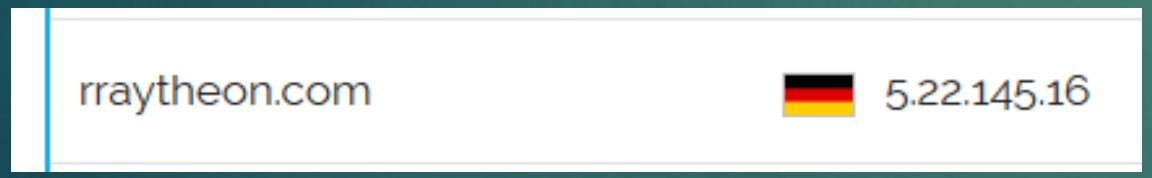
- **3. If you get lost, look cool.**
  - **Confidence breeds confidence.**
    - **Anxiety breeds anxiety.**
  - **Get back to a point of reference.**
  - **Airline pilots are cool, they need to be. Be like an airline pilot.**

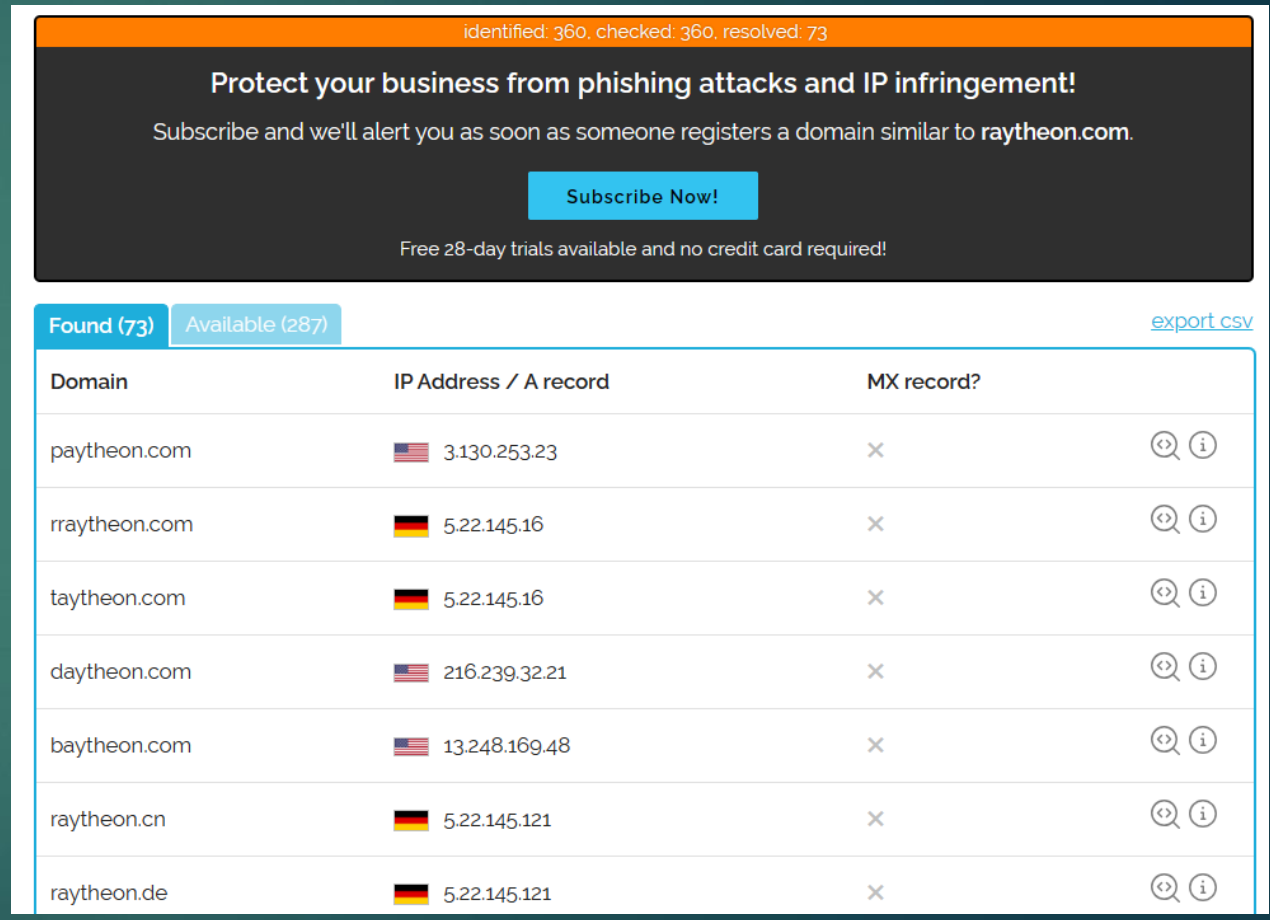
Building Networks

- Human networks are built before a crisis or conflict occurs. Think IR.
- Building trust takes time and information. We trust people the more credible and sensitive information they provide.
- Create a working group (reverse engineering) on a topic you need to grow in. Attract others to get better, build a skillset collectively. Cash in.
- Use multiple forms of communication to build networks. Teams, conferences, portals, texts ect.
- Leverage this during an incident to be better and win.

War Story 1

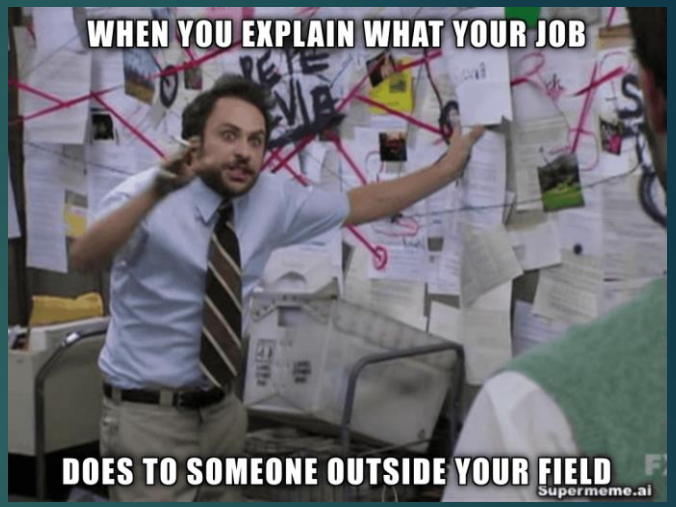

DNSTWISTER
raytheon.com
The anti-phishing domain name search engine and
DNS monitoring service


rraytheon.com
5.22.145.16

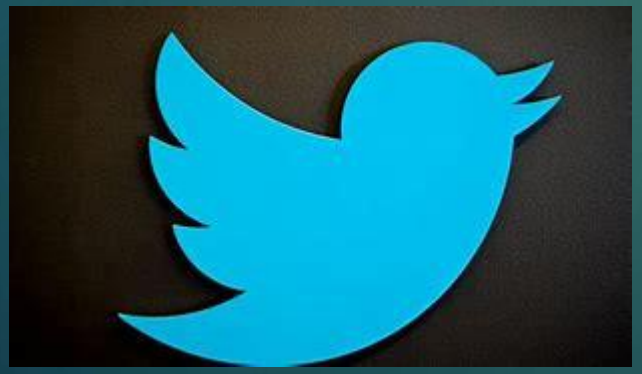

identified: 360, checked: 360, resolved: 73
Protect your business from phishing attacks and IP infringement!
Subscribe and we'll alert you as soon as someone registers a domain similar to raytheon.com.
Subscribe Now!
Free 28-day trials available and no credit card required!
Found (73)
Available (287)
export csv
Domain
IP Address / A record
MX record?
paytheon.com
3.130.253.23
rraytheon.com
5.22.145.16
taytheon.com
5.22.145.16
daytheon.com
216.239.32.21
baytheon.com
13.248.169.48
raytheon.cn
5.22.145.121
raytheon.de
5.22.145.121

Effective Communication

- "If I had more time, I would have written a shorter letter" – Nick Oles/Mark Twain
- Less is more, be concise.
- Thank your users for reporting suspicious emails or incidents. An auto reply costs you nothing and encourages positive behavior.
- How are you sharing incident or emerging threat information with your team or users? Hint a monthly/quarterly email or newsletters does wonders to establish and maintain your credibility.



War Story 2



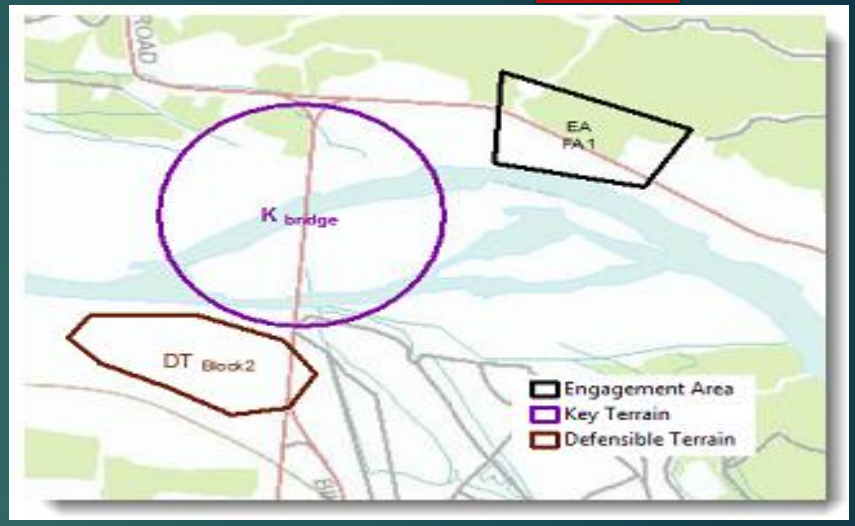
- **June 27, 2017**: The NotPetya attack begins in Ukraine. The initial infection is traced back to a compromised software update for accounting software widely used in the country.
- **Within hours**: NotPetya spreads rapidly through Ukraine's networks, infecting government agencies, banks, power companies, and critical infrastructure.
- **International spread**: NotPetya quickly crosses international borders, affecting organizations in various countries, including Russia, the United States, the United Kingdom, Germany, France, and many others.
- **June 28-29, 2017**: The attack gains significant media attention as organizations worldwide report being affected by NotPetya. Panic and confusion ensue as the full extent of the attack becomes apparent.
- **July 1, 2017**: The Ukrainian government and cybersecurity firms publicly attribute the attack to the Russian military.

Imposter Syndrome

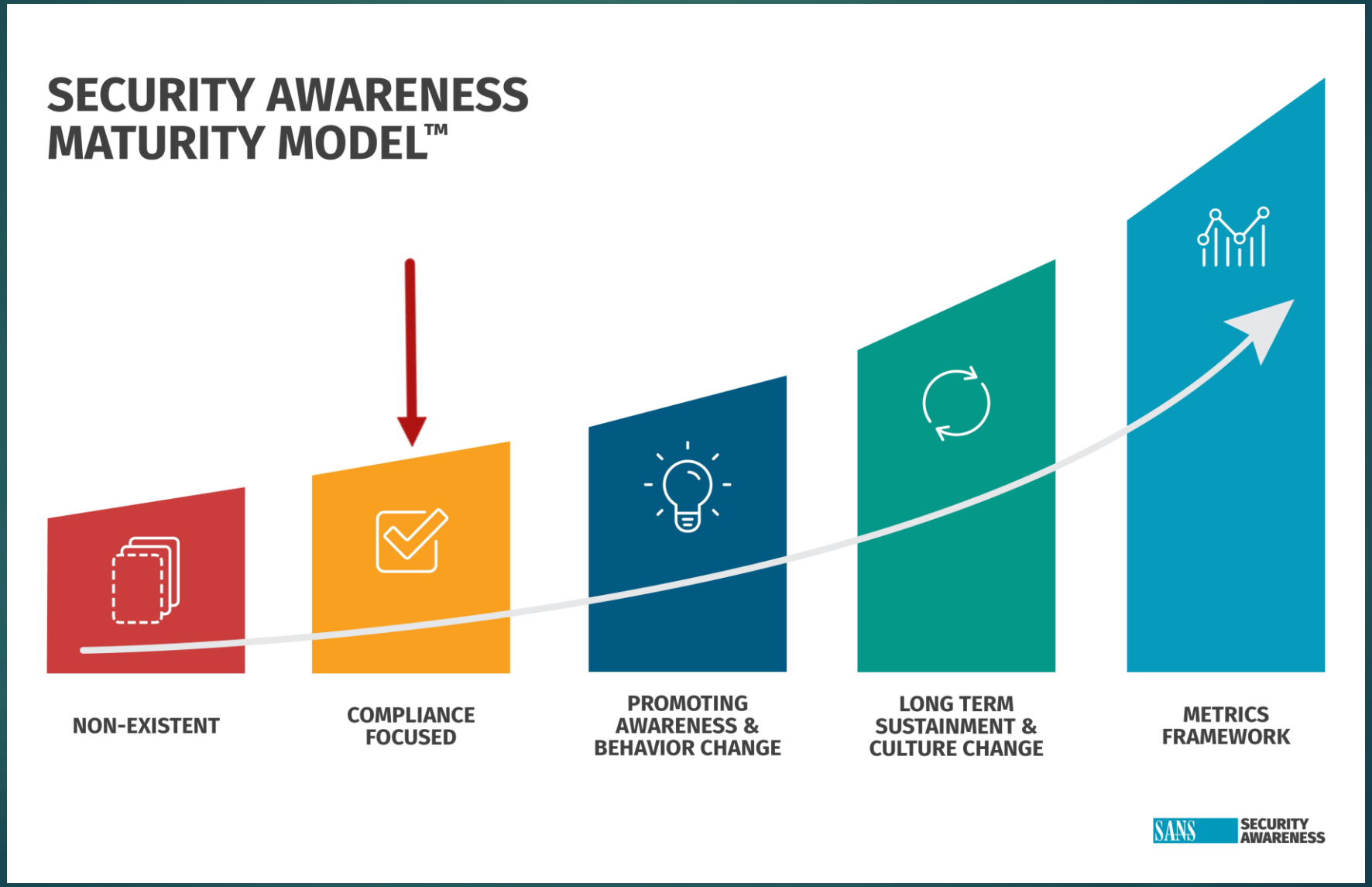
- Everyone encounters at some point in your career.
- Someone thought you could do this job, chances are you can.
- Everyone is figuring it out as they go.
- Don't be afraid to ask that indicator, malware, TTP question in the forum or group.
- You guys have a unique organization, take advantage of it!

Key Terrain

- Affords a marked advantage to either combatant
- Provides a significant advantage to the attacker or defender
- Physical world think hilltop, bridge, valley, gate or tunnel
- Routers, key servers, access points, mission critical infrastructure
- Need to defend these differently, update aggressively, isolate, additional logging, layered defense



Security Awareness Maturity Model



Compliance Focused-Bad

- **Fails to incorporate organizations unique risks, threats, and vulnerabilities.**
  - **Often statically created with minimal changes.**
  - **Lots of videos.**
  - **People aimlessly click through training.**
  - **Phishing training sent monthly, poor metrics.**
  - **Rinse and repeat.**
  - **BEHAVIOR DOESN'T CHANGE!!!**

Start with Phishing

- **Threat actor uses technology to deceive an individual to take a specific action.**

- **Three actions:**
  - **1. Click a link**
  - **2. Interact with an attachment (open, download, forward)**
  - **3. Provide sensitive information (content like SSN, CC info, invoice data)**

- **Multiple Forms**
  - **1. Email**
  - **2. Voice call (vishing)**
  - **3. SMS (smishing)**

Fix Security Awareness 3 Things

+

From: Pete Bishop <pete@solutionproducts.com>
Sent: Monday, July 15, 2024 2:04 PM
To: [redacted]@mullinscheese.biz>
Subject: Re: Invoice 23005 from Solution Products

WARNING: The sender of this email could not be validated and it may be a phishing attempt. Please send to suspiciousemail@psolit.com.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi, I hope this message finds you well. Kindly acknowledge receipt of the invoice and feel free to reach out if you require any clarification. Thank you.

SOLUTION PRODUCTS LLC INVOICE

Thanks,

Pete Bishop
Owner
Solution Products, LLC
Pete@solutionproducts.com
608-235-9390
www.solutionproducts.com
Solving your Storage, Facilities, Safetynomic, and Material Handling Needs since 2006
SOLUTION PRODUCTS
Creative Storage, Space, Efficiency & Safetynomic Solutions

+

From: Pete Bishop <pete@solutionproducts.com>
Sent: Monday, July 15, 2024 2:04 PM
To: [redacted]cheese.biz>
Subject: Re: Invoice 23005 from Solution Products

WARNING: The sender of this email could not be validated and it may be a phishing attempt. Please send to suspiciousemail@[redacted]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi, I hope this message finds you well. Kindly acknowledge receipt of the invoice and feel free to reach out if you require any clarification. Thank you.

SOLUTION PRODUCTS LLC INVOICE

Thanks,

Pete Bishop
Owner
Solution Products, LLC
Pete@solutionproducts.com
608-235-9390
www.solutionproducts.com
Solving your Storage, Facilities, Safetynomic, and Material Handling Needs since 2006

SOLUTION PRODUCTS
Creative Storage, Space, Efficiency & Safetynomic Solutions

Google

Gmail

Important: Your Password will expire in 1 day(s) Inbox x

MyUniversity 12:18 PM (50 minutes ago)

to me

Dear network user,

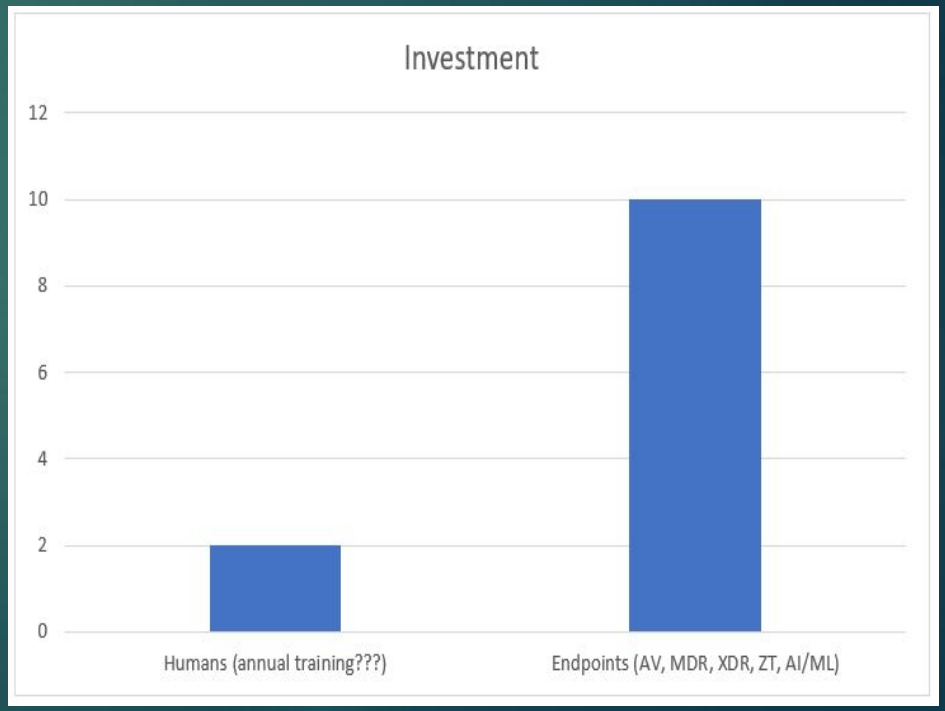
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

MY UNIVERSITY

Thank you
MyUniversity Network Security Staff

Four Tips to Success

1. Patch your stuff.
   - Look at EPSS, or a business impact analysis approach.
     - CISA Stakeholder Specific Vulnerability Scoring System
2. Know your assets.
   - Use a free asset inventory tool, when you've exhausted that pay for a commercial product.
3. Have good policies in place.
   - This isn't sexy work, but its necessary to guide your user behavior.
4. Train users on phishing!!!!
   - Humans aren't the weakest link, they are the biggest attack vector.



Questions

nick@thenetdefender.com