Federal Information Security Educators (FISSEA)

Fall Forum

Role-Based Training

November 15, 2022

1:00pm – 4:00pm ET

#FISSEA2022 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Welcome and Opening Remarks

Maureen Premo

FISSEA Co-Chair
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2023
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

Keynote

Need for Skills - The Importance of Role-based Training in Tackling the Ever-changing Landscape of Threats

Paula Januszkiewicz

Founder and CEO
Microsoft Regional Director, CQURE

Need for Skills: The Importance of Role-based Training in Tackling the Ever-changing Landscape of Threats

Paula Januszkiewicz

FISSEA Fall Forum, November 15th 2022

CQURE

Need for Skills

The Importance of Role-based Training in Tackling the Ever-changing Landscape of Threats

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

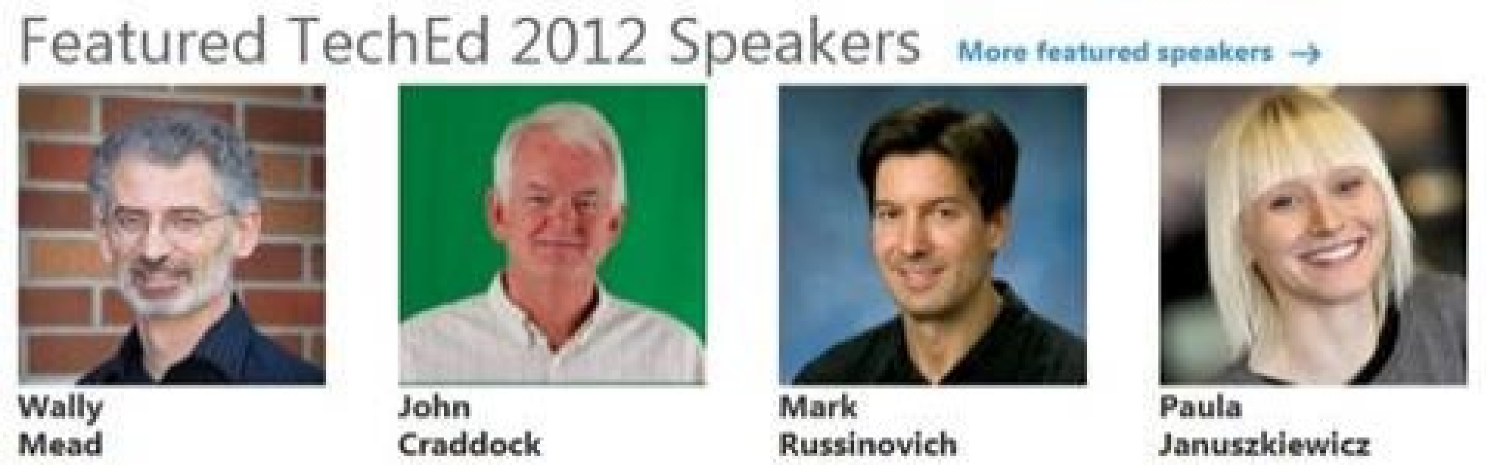
Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com



Featured TechEd 2012 Speakers

More featured speakers →

Wally Mead

John Craddock

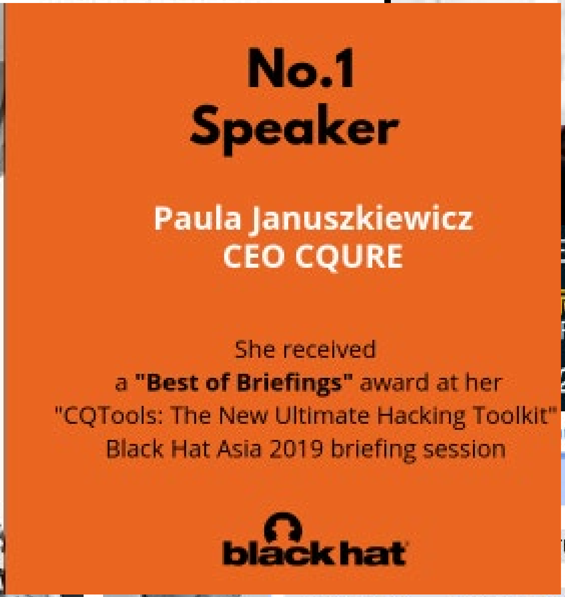
Mark Russinovich

Paula Januszkiewicz

Microsoft CQURE ACADEMY©

We are proud to announce that **Paula Januszkiewicz** was rated as **No 1 Speaker** at Microsoft **Ignite!!!**

May 4-8, 2015
Chicago, IL

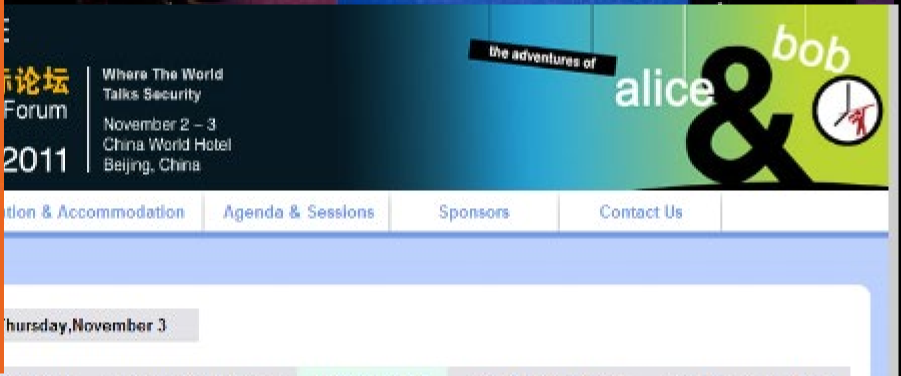


No.1 Speaker

Paula Januszkiewicz
CEO CQURE

She received
a **"Best of Briefings"** award at her
"CQTools: The New Ultimate Hacking Toolkit"
Black Hat Asia 2019 briefing session

black hat



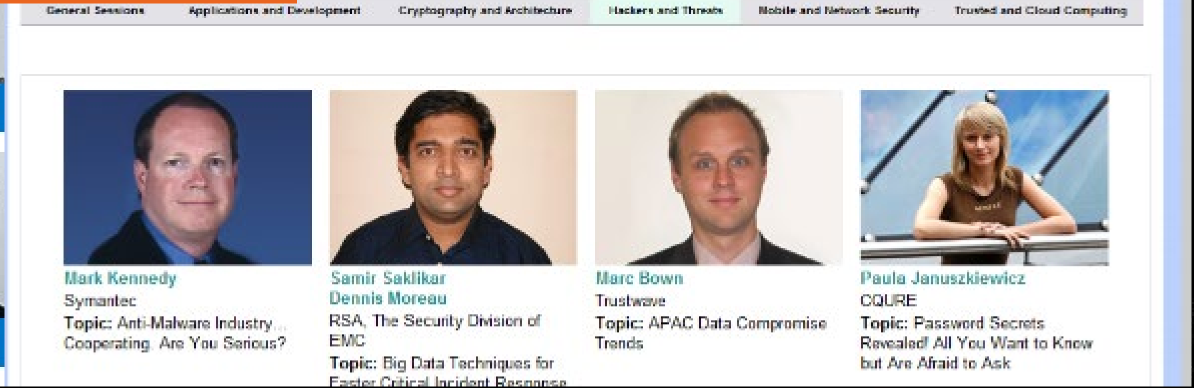
际论坛
Forum
2011

Where The World Talks Security

November 2 – 3
China World Hotel
Beijing, China

tion & Accommodation | Agenda & Sessions | Sponsors | Contact Us

hursday,November 3



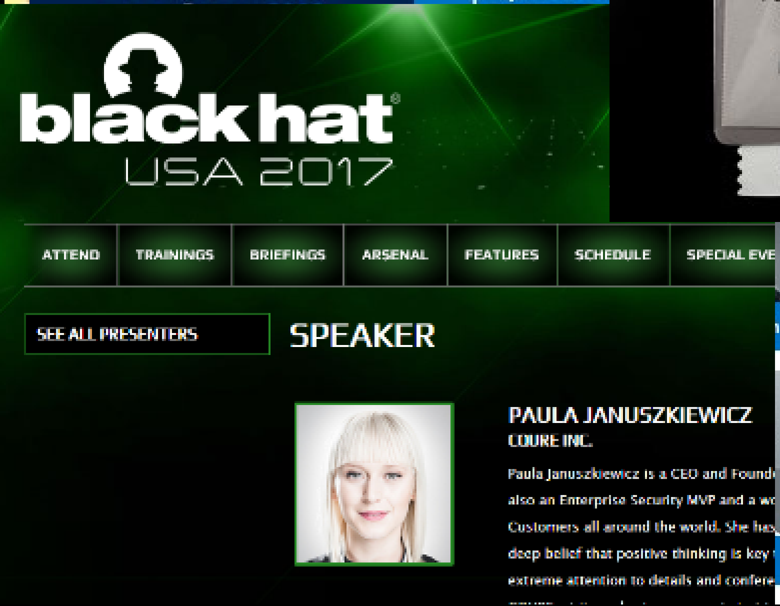
General Sessions | Applications and Development | Cryptography and Architecture | Hackers and Threats | Mobile and Network Security | Trusted and Cloud Computing

Mark Kennedy
Symantec
Topic: Anti-Malware Industry Cooperating. Are You Serious?

Samir Saklikar
Dennis Moreau
RSA, The Security Division of EMC
Topic: Big Data Techniques for Faster Critical Incident Response

Marc Bown
Trustwave
Topic: APAC Data Compromise Trends

Paula Januszkiewicz
CQURE
Topic: Password Secrets Revealed! All You Want to Know but Are Afraid to Ask



black hat®
USA 2017

ATTEND | TRAININGS | BRIEFINGS | ARSENAL | FEATURES | SCHEDULE | SPECIAL EVE

SEE ALL PRESENTERS

SPEAKER

PAULA JANUSZKIEWICZ
CQURE INC.

Paula Januszkiewicz is a CEO and Founde
also an Enterprise Security MVP and a wo
Customers all around the world. She has
deep belief that positive thinking is key
extreme attention to details and confere

Brian Keller | Paula Januszkiewicz | Mark Minasi

John Craddock | Scott Woodgate | Marcus Murray

What does CQURE do?

1. Consulting Services:

Extensive IT Security Audits and Penetration Tests of all kinds,
Configuration Audit and Architecture,
Design Social Engineering Tests,
Advanced Troubleshooting and Debugging,
Emergency Response Services

2. R&D & CQLabs Tools & Hacks Publications

3. Trainings & Seminars:

Offline (mainly in New York or via our partners worldwide),
Online

The Impact of Cybercrime

Impactful Hacking Stats (2022)

50%

Over 50 percent of all cyber attacks are done on SMB’s.

32/65%

Out of all ransomware victims, 32 percent pay the ransom, but they only get 65 percent of their data back.

62%

of incidents in the System Intrusion pattern involved threat actors compromising partners.

77%

of organizations do not have a cyber security incident response plan.

Source: Source: Purplesec (2022), Cloudwards (2022), Data Breach Investigation Report (2022); Trend Micro, IBM, CSO (2021);

"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."

-JAMES COMEY, FORMER FBI DIRECTOR

200+

Median number of days attackers are present on a victims network before detection

80

Days after detection to full recovery

$3Trillion

Impact of lost productivity and growth

$3.9Million

Average cost of a data breach (15% YoY increase)

2023 will be a year of a well-written and well-tested incident response plan (cyber crisis management plan).

Companies should revise goals of penetration tests.

Cybersecurity awareness trainings
should be multi-channeled
& should reference personal life.

Effective cyber defense is a long game that requires continuous strategic investment.

Workstation security and identity security are one of the top priorities now.

Six Techniques to Understand the Landscape of Threats

#1
Well Configured Firewall

#1 Well Configured Firewall

- Key learning points:
  - Windows Firewall is often misconfigured
  - Firewall is a great segmentation tool
  - You can allow only certain processes to communicate with the Internet or locally
  - No need-to-know processes to block them, you can operate on the services list

Demo:
Phishing Little

#1 Well Configured Firewall

Role: Network Engineer

Primary Skill: Network Security

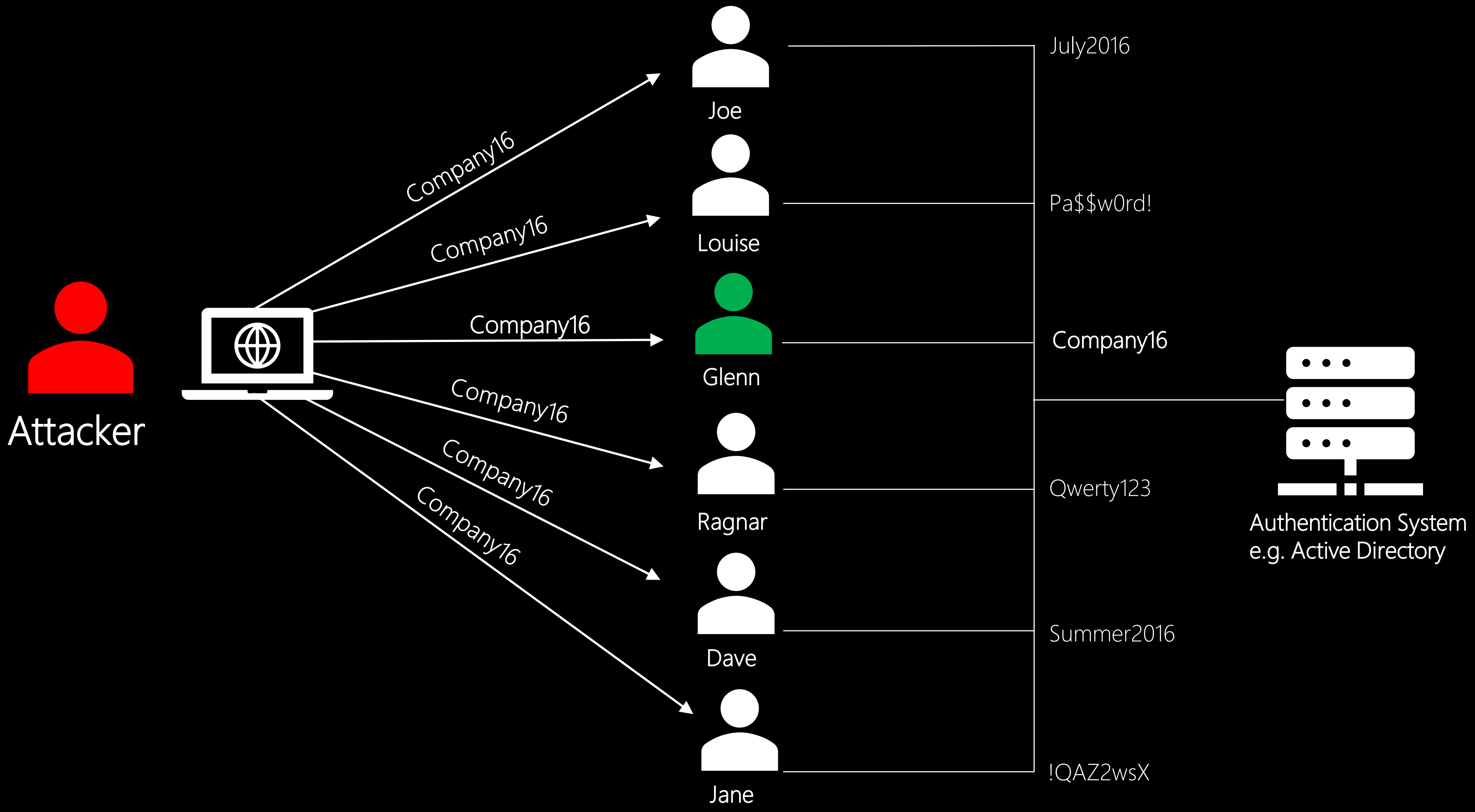
Additional Skills: Computer Network Defense, Cryptography & Encryption, Architecture

#2 Usage of MFA and Conditional Access

#2 Usage of MFA and Conditional Access

- Key learning points:
  - Passwords are almost always re-used
  - There is almost always (ekhm... always) some variant of the company name with some number (year, month etc.)
  - It's highly reasonable to check for obvious passwords and continuously deliver security awareness campaigns

Password Spraying



Demo:
Bypassing MFA

#2 Usage of MFA and Conditional Access

Role: Security Administrator

Primary Skill: Security Configuration Management

Additional Skills: Identity Management, Systems and Application Security, Architecture

#3
Network Segmentation and SMB Signing

#3A Network segmentation

- Key learning points:
  - Network segmentation can be a blessing or a curse
  - Greater control over who has access to what
  - Allows rules to be set to limit traffic
  - Allows exposure to security incidents to be reduced
  - Performance: allows Broadcast Domains to be reduced so that broadcasts do not spread on the entire network

Demo:

SMB Relay

#3B Server Message Block Signing (or alternative)

- Key learning points:
  - Set Service Principal Names (SPN) for services to avoid NT LAN Manager (NTLM):
  - Reconsider using Kerberos authentication all over
  - https://technet.microsoft.com/en-us/library/jj865668.aspx
  - Require SPN target name validation
  - Microsoft network server: Server SPN target name validation level
  - Reconsider turning on SMB Signing
  - Reconsider port filtering
  - Reconsider code execution prevention but do not forget that this attack leverages administrative accounts

#3 Network Segmentation and SMB Signing

Role: Enterprise Security Architect

Primary Skill: Defense in Depth

Additional Skills: Computer Network Defense, Architecture, Data Security

#4 Whitelisting

#4A Disallowing unusual code execution

- Key learning points:
  - Common file formats containing malware are:
  - .exe (Executables, GUI, CUI, and all variants like SCR, CPL etc.)
  - .dll (Dynamic Link Libraries)
  - .vbs (Script files like JS, JSE, VBS, VBE, PS1, PS2, CHM, BAT, COM, CMD etc.)
  - .docm, .xlsm etc. (Office Macro files)
  - .other (LNK, PDF, PIF, etc.)

#4B Whitelisting on board

- Key learning points:
  - Code execution prevention implementation is a must
  - PowerShell is an ultimate hacking tool, possible solutions: block it for users, use Just Enough Administration etc.
  - Verify where users have write access to: accesschk.exe –w .\users c:\windows
  - AppLocker can run in the audit mode
  - AppLocker is great but not with the default configuration

Demo:

Forensics Operations

#4 Whitelisting

Role: Security Administrator

Primary Skill: Configuration Management

Additional Skills: Information Systems, Systems and Applications Security

#5
Configuration Audit

#5A Decommission of old protocols or their default settings

- Key learning points:
  - SNMPv3 addresses: user-based system for access control, a means to properly authenticate users, and a method for encrypting SNMP traffic between agent and host
  - SQL issues – TDS provides by default lack of encryption
  - ODBC Driver – check if it has a secure networking layer built into it

Demo:
Clear Text Queries

#5B Review of the solutions that we trust by default

- Key learning points:
  - The best operators won't use a component until they know how it breaks.
  - Almost each solution has some 'backdoor weakness'
  - Some antivirus solutions can be stopped by SDDL modification for their services
  - Configuration can be monitored by Desired State Configuration (DSC)
  - DSC if not configured properly will not be able to spot internal service configuration changes
  - Example: How do I get to the password management portal?

Demo:

Extracting User’s Secrets

# 5C Do not fall for hipster tools

- Key learning points:
  - Personal data was involved in 58% of breaches in 2020 (Verizon)
  - The average time to identify a breach in 2020 was 207 days (IBM)
  - With increasing budget the risk of possessing hipster tools increases too – do we know where these tools come from and what are their security practices?
  - Lots of solutions where not created according to the good security practices (backup software running as Domain Admin etc.)
  - Each app running in the user's context has access to secrets

#5 Configuration Audit

Role: System/Network Administrator

Primary Skill: Systems and Application Security

Additional Skills: Computer Network Defense, Database security

#6
Connecting the dots (monitoring identity etc.)

#6 Monitoring privileged accounts and identity misuse

- Key learning points:
  - gMSA can also be used for the attack
  - Service accounts’ passwords are in the registry, available online and offline
  - A privileged user is someone who has administrative access to critical systems
  - Privileged users have sometimes more access than we think (see: SeBackupRead privilege or SeDebugPrivilege)
  - Privileged users have possibility to read SYSTEM and SECURITY hives from the registry

Demo:

Accounts with Issues

Demo:
DPAPI Beauty

#6 Connecting the dots (monitoring identity etc.)

Role: Cybersecurity Analyst

Primary Skill: Identity Management & Monitoring

Additional Skills: Incident Management, Digital Forensics, Cyber Threat Intelligence

Why human factor is so important?

Summary

#1
Well Configured Firewall

#2
Usage of MFA and Conditional Access

#3
Network Segmentation and SMB Signing

#4
Whitelisting

#5
Configuration Audit

#6
Connecting the Dots (monitoring identity etc.)

Summary

Every employee in the organization is the first line of defense when it comes to protecting your organization from cyber threats.

Remote workers will continue to be a target for cybercriminals. As a side effect of remote workforces, cloud breaches will increase.

The cybersecurity skills gap will remain an issue. It's time to act – now!

Be cautious of links and attachments in emails – double check with the sender if you feel uneasy.

Never leave your devices unlocked and unattended.

Prevention is the key to success: How can we know what to prevent if we do not know what is the threat?

Thank you!

CQURE

DOWNLOAD THE TOOLS

https://resources.cqureacademy.com/tools/

Username: student
Password: CQUREAcademy#123!

Visit our BLOG and discover more about cybersecurity solutions & tools:

https://cqureacademy.com/blog

Need for Skills

The Importance of Role-based Training in Tackling the Ever-changing Landscape of Threats

Paula Januszkiewicz

CQURE: CEO, Cybersecurity Expert, Penetration Tester

CQURE Academy: Trainer

Microsoft MVP on Cloud and Datacenter Management

Microsoft Regional Director

paula@cqure.us

@PaulaCqure @CQUREAcademy

www.cqureacademy.com

CQURE

Q&A

Are There Any Questions?

Featured Presentation

Cyber Work Roles Assigned…Now What? Let’s Talk Resources

Susan Hansche

Cybersecurity & Infrastructure Security Agency
Department of Homeland Security

Stacey Wise

IT Specialist
Pension Benefit Guaranty Corporation

Cyber Work Roles Assigned… Now What? Let's Talk Resources

Stacey Wise, PBGC
Susan Hansche, DHS CISA

HELLO!

I am Susan Hansche

CISA Cybersecurity Division

HELLO!

I am Stacey Wise

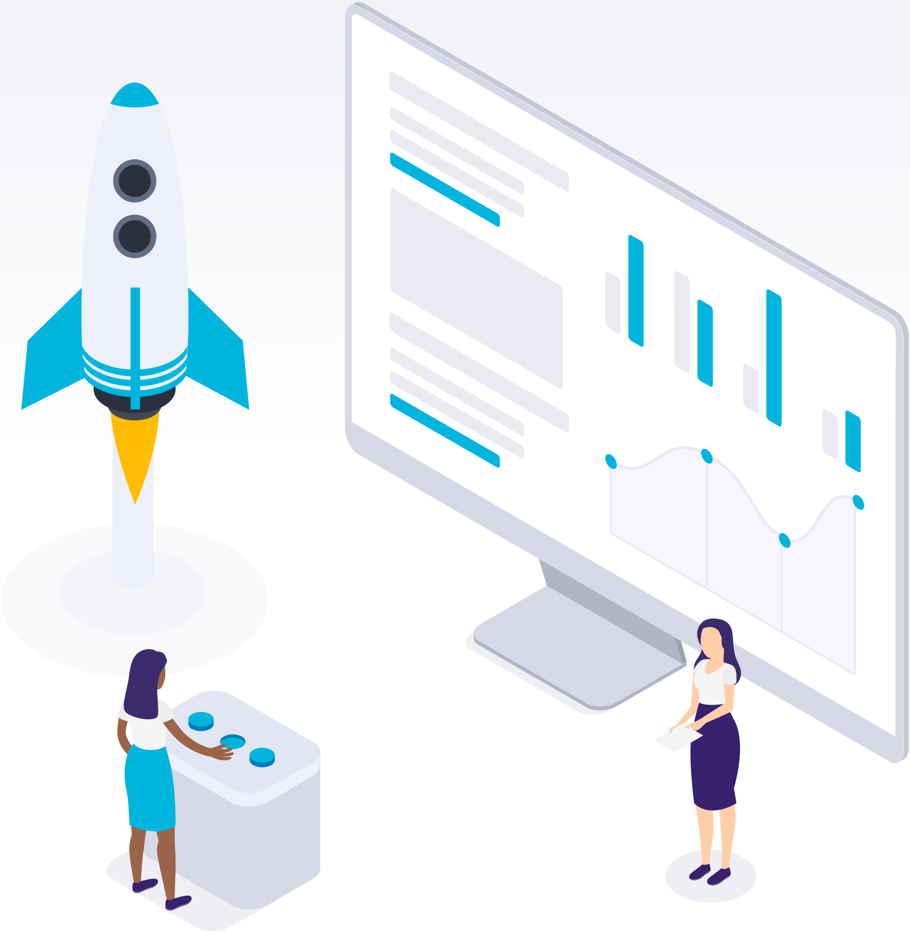
Pension Benefit Guaranty Corporation

(ECD – Enterprise Cybersecurity Department)

Role Based Training Program Lead

1

Process for Identifying and Maintaining Roles



“

- Implement NIST Cybersecurity Workforce Framework based on PGBC policies
- Initial Goal: Identify who has “significant security responsibilities”
- Process: Survey hiring managers to: identify if a work role was identified in their department, how many, and a point of contact
- Feedback loop: Review, edit, review, edit and review, edit

Process for Identifying and Maintaining Roles (continued)

- Introduce 1-2 new roles every year as a deliberate thoughtful part of the process
- Internal "master" list and from that we developed Role Based Training (RBT) policy (Bulletin 13 which outlines all role-based training requirements) in addition to training policies and procedures
- Work role "title" is not the same as the hiring/job "title" (IT Specialist, etc.)

The Work Roles…so far

Defined in Bulletin 13

Reference NIST SP 800-181 NICE Framework

The work roles that are trained on an annual basis:

- *Risk Executives*
  - Chief Information Officer (CIO)
  - Chief Information Security Officer (CISO)
  - Risk Management Officer (RMO)
- *Authorizing Officials* (AOs)
- *Common Control Providers* (CCPs)
- *Security Control Assessors* (SCAs)*
- *Information Owners* (IOs) and *Information System Owners* (ISOs)
- *Information System Security and Privacy Officers and Managers* (ISSPOs and ISSMs)
- *Incident Response Handlers* (IRHs) **
- *Privacy Executives*
  - Senior Agency Official for Privacy (SAOP)
  - Chief Privacy Officer (CPO)
- *Cyber Policy & Planning (CPP)*
- *Cyber Training Educator (CTE)*
- *Threat & Warning Analysts (TWA)*

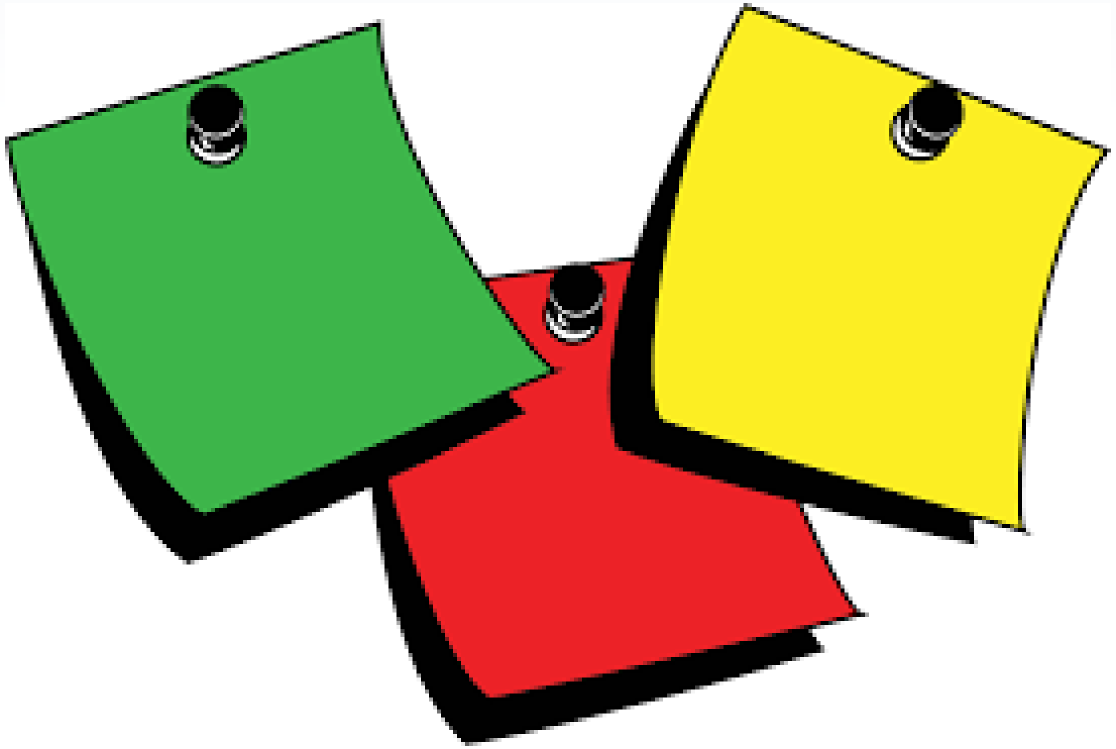
What Training is needed and where do you find it……..

- Everyone identified in a significant cyber work role is required to take one hour of training relevant to their role each year
- Work with the POC to identify the training that is appropriate for the role

Challenge:
Find training that is significant to each role

- How do we find free resources?
- What platforms are available?
- How do we find courses with valuable content?
- Do we look at on demand course or instructor lead?

Interactive Session



Interactive Session

- What to look for when choosing RBT?
- Where do you get your training from?
  - External Speakers (if so, where from?)
  - COTS Training on Internal LMS (i.e., Skillsoft, Precipio)
  - Design and Develop Internally/Post on Internal LMS
  - Industry Training (i.e., AWS, Palo Alto, SANS)
  - Certificate Training (i.e., ISC2, ISACA, PMP)
  - Federal / MS-ISAC resources?
  - Academic?
- How do provide variety each year?

All options are important – this is anonymous posting, so please share!

Interactive Session

- What challenges are you having for Role-Based Training?
- What has worked for you?
- What hasn’t worked for you?
- What would you like to know more about?

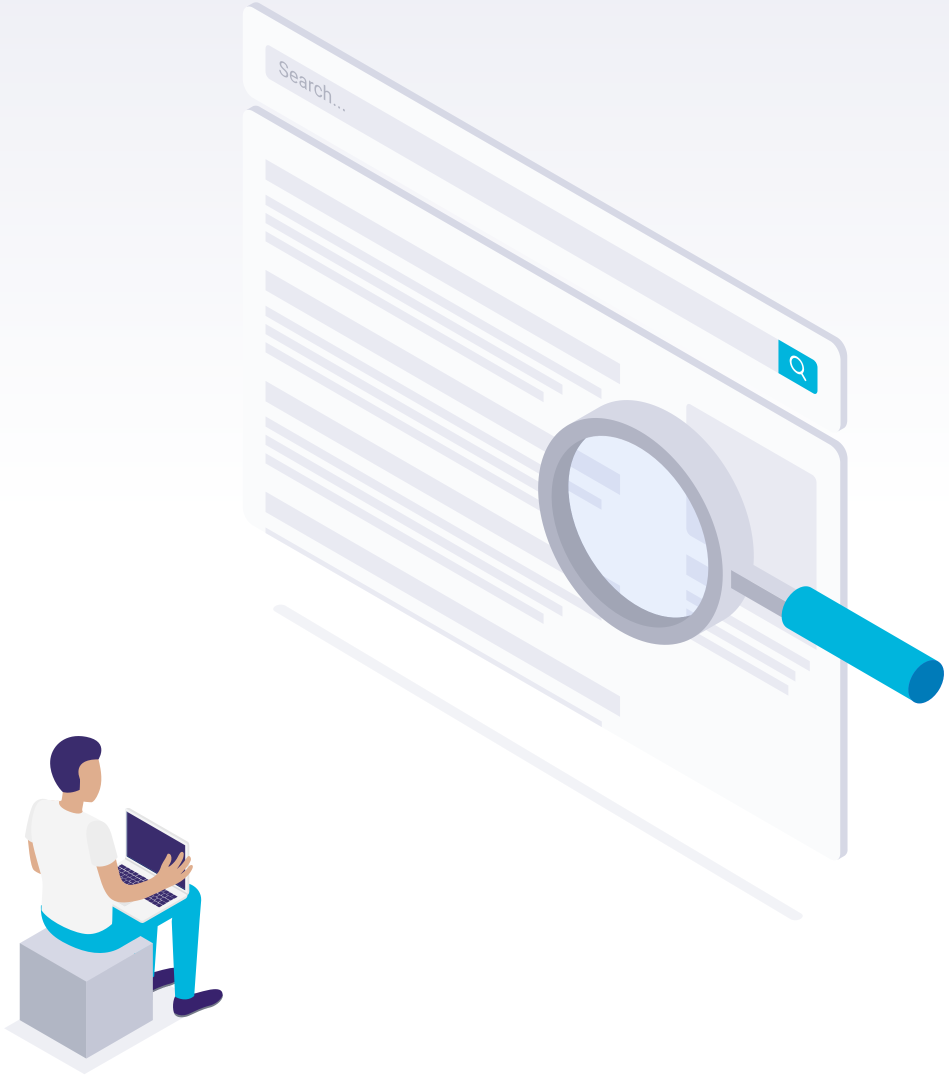
All options are important – this is anonymous posting, so please share!

THANKS!

Any questions?

You can contact us:

- wise.Stacey@pbgc.gov
- susan.hansche@cisa.dhs.gov



Featured Presentation

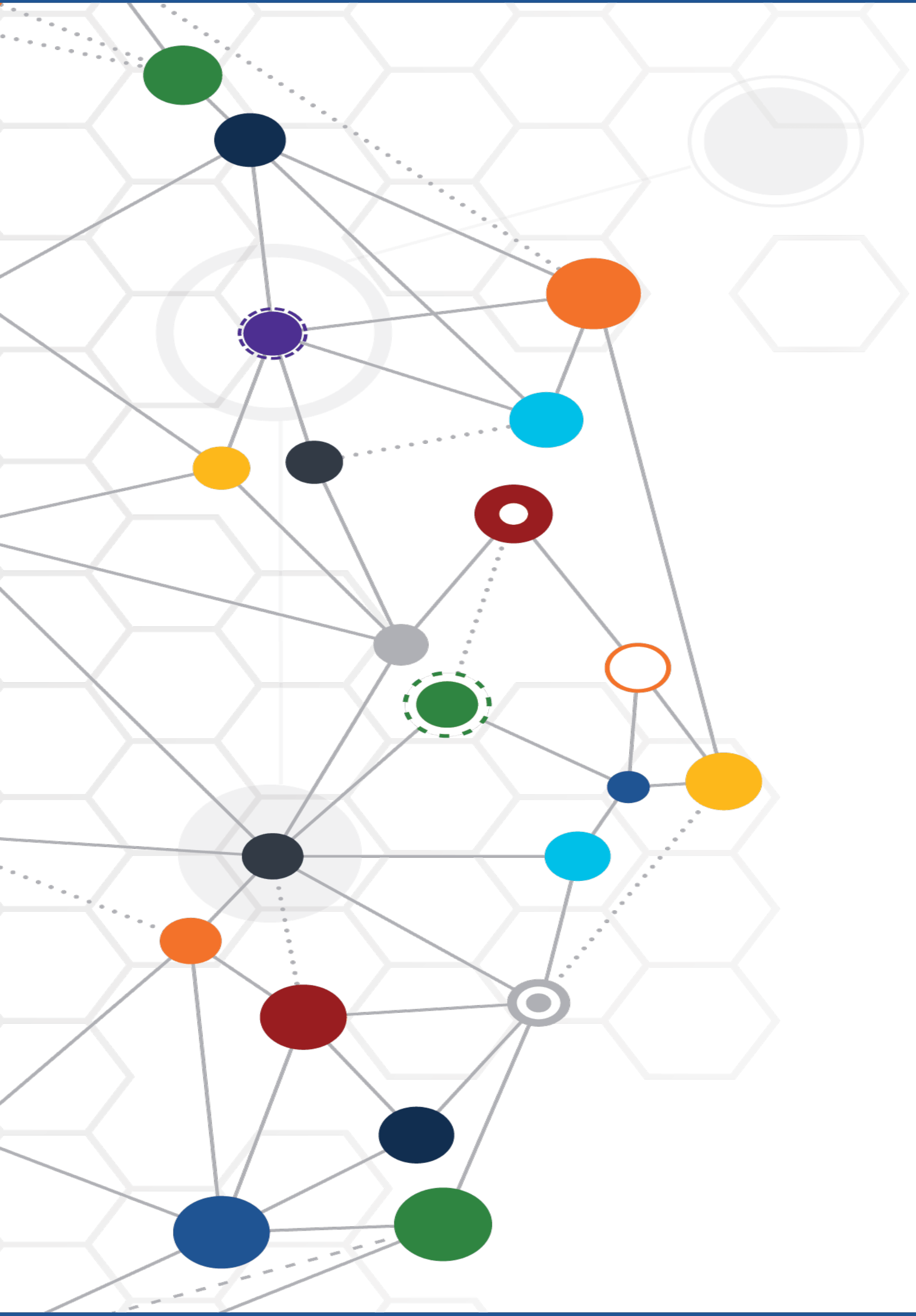
A Tailored Approach to Workforce Training

Scott Anderson

Department of Veteran Affairs

Sharon McPherson

Senior Cybersecurity Specialist for Policy, Training & Awareness
Cyber Workforce Management
Department of Veteran Affairs



A TAILORED APPROACH TO WORKFORCE TRAINING

Sharon McPherson and Scott Anderson

Office of Information and Technology

Department of Veteran Affairs

FISSEA Presentation

November 15, 2022

FOR INTERNAL USE ONLY

VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Current Landscape

71% of organizations report a **shortage of cyber skills** that significantly damaged their ability to function (Lewis, 2019)

North American cybersecurity professionals are significantly more concerned about **skill shortages** than others, with **69%** of respondents saying that this will be a future challenge (ISC^2 Study, 2022)

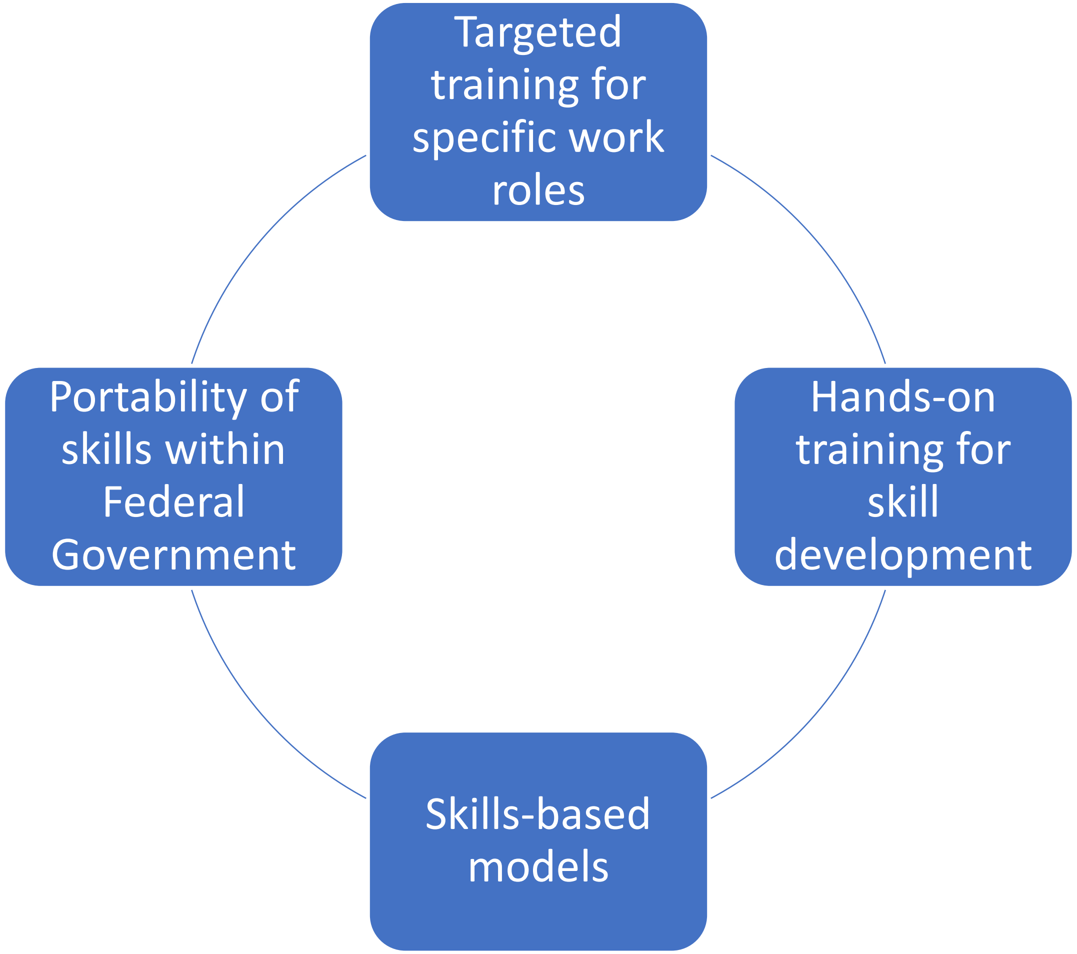
The primary cause for workforce shortages is the **absence of programs** that produce the necessary volume of trained cybersecurity workers. (Lewis, 2022).

Challenges

- Lack of targeted training for specific work roles
- Existing training is too broad
- Limited hands-on training for skill development
- No portability of skills across the Federal Government

What We Need

Tailored approaches that provide more relevant and practical training to support the execution of tech work.



Targeted training for specific work roles

Hands-on training for skill development

Skills-based models

Portability of skills within Federal Government

VA's Approach to Training

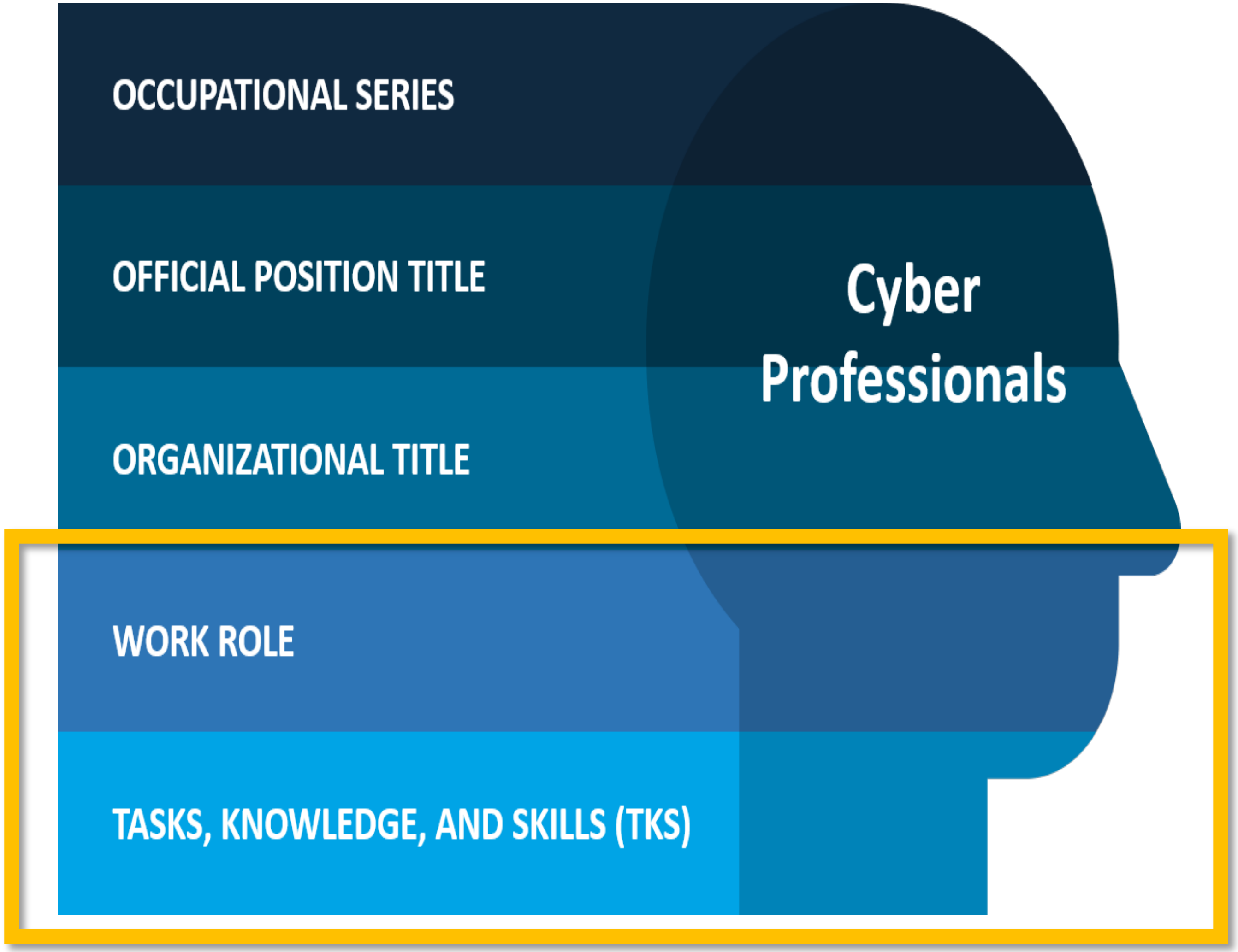
What We're Doing

- **Work Role Skills-Based Profiles (SBP)**
  - Targeted training for OIT Competencies and technical work
- **Self-assessments / Skills Maturity Assessments (SMAs)**
- **Role-Based Training (CTA)**
- **Experience-Based Learning**
  - On the Job Training (OJT)
  - Hands-on Learning
  - Skills Execution

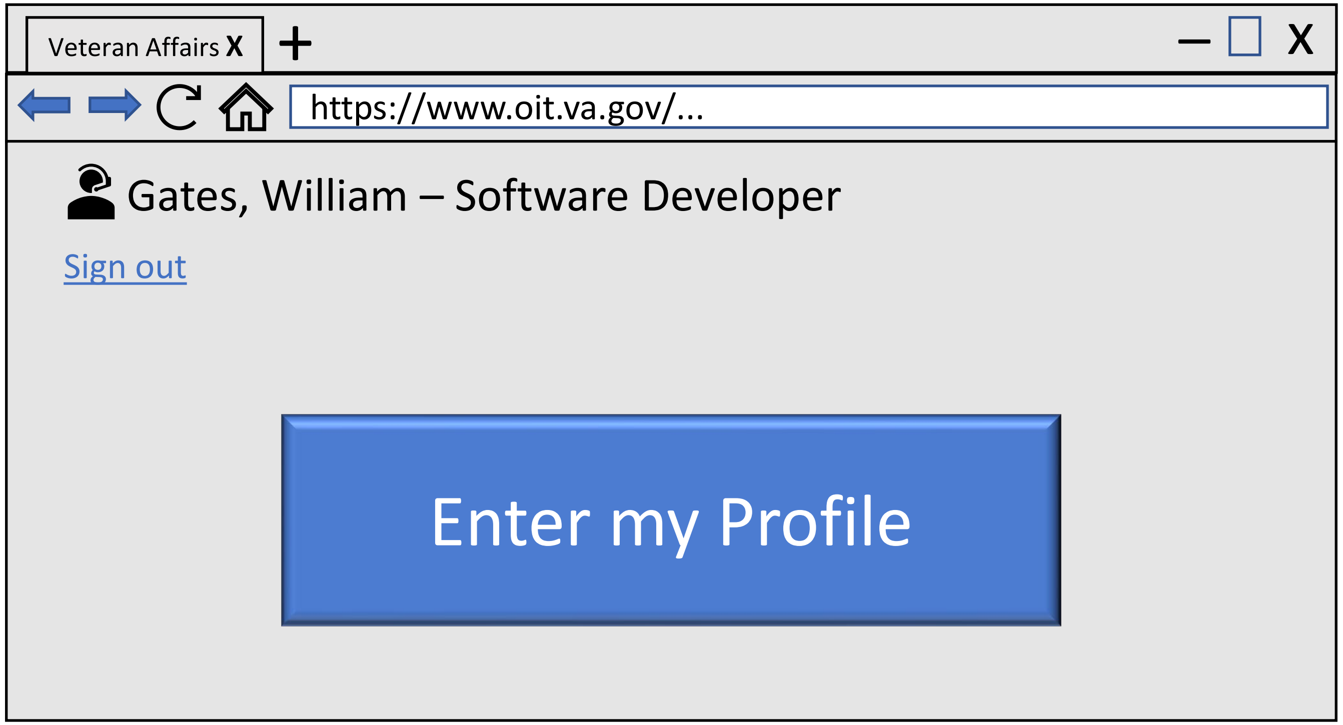
What We're Using

- **Career Pathway tool available on NICCS site**
  - Career Pathways roadmap offers a digitalized experience on how to explore and build personalized career roadmaps across the 52 work roles

Cyber Workforce Training (CWT) for Career Development



Skill-Based Profiles



Gates, William – Software Developer

Skills Maturity Assessment

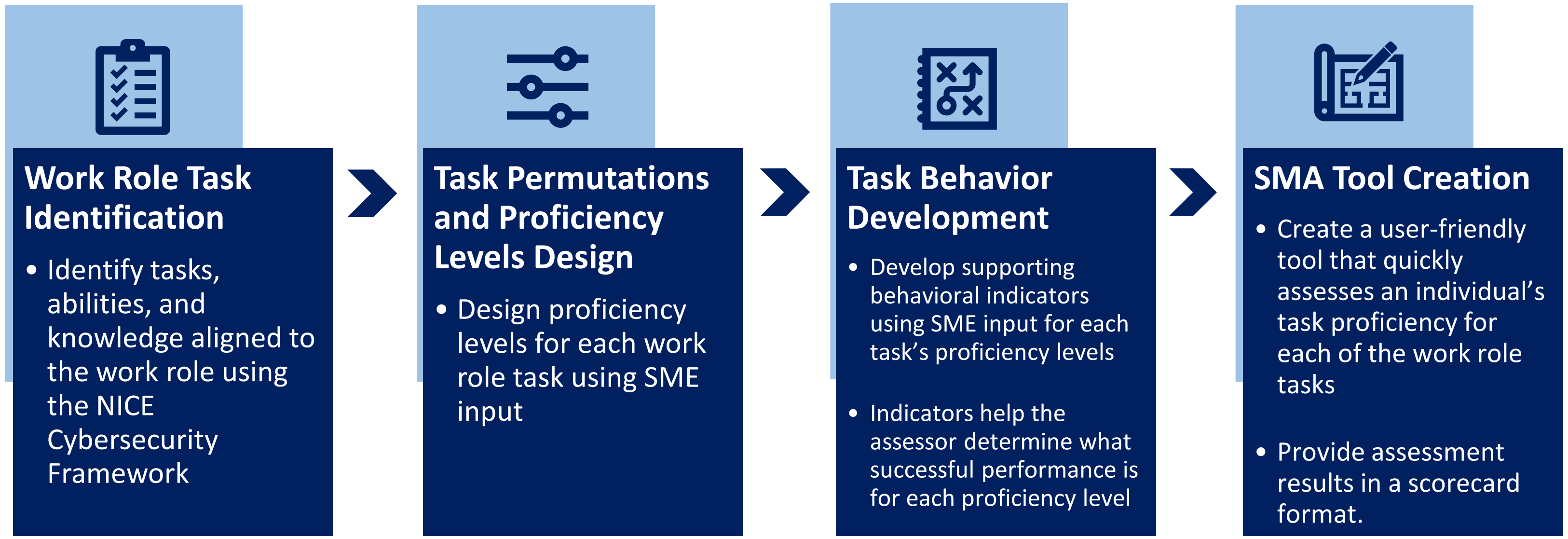
Skills Maturity Assessment is a tool designed to support programs focused on learning and development of skill proficiency.

The **goals** of the assessment are:

- To measure an individual's demonstration of the skills needed to perform tasks in a given work role (as defined by the NICE Framework for Cybersecurity)
- Identify skill gaps to support development
- Determine skill maturity over a period of time
- Provide an opportunity to highlight developmental opportunities

Methodology for Developing a Skills Maturity Assessment (SMA) Tool

- The Skills Maturity Assessments tool measures an individual's development, identifies areas of strength, and determines possible skill gaps to building maturity in a cyber role.



Work Role Task Identification

- Identify tasks, abilities, and knowledge aligned to the work role using the NICE Cybersecurity Framework

Task Permutations and Proficiency Levels Design

- Design proficiency levels for each work role task using SME input

Task Behavior Development

- Develop supporting behavioral indicators using SME input for each task’s proficiency levels
- Indicators help the assessor determine what successful performance is for each proficiency level

SMA Tool Creation

- Create a user-friendly tool that quickly assesses an individual’s task proficiency for each of the work role tasks
- Provide assessment results in a scorecard format.

What is the Cyber Training Academy?

Cyber Training Academy

- The Cyber Training Academy (CTA) provides learning activities for all VA staff to support them in fulfilling the tasks associated with their cyber work roles.

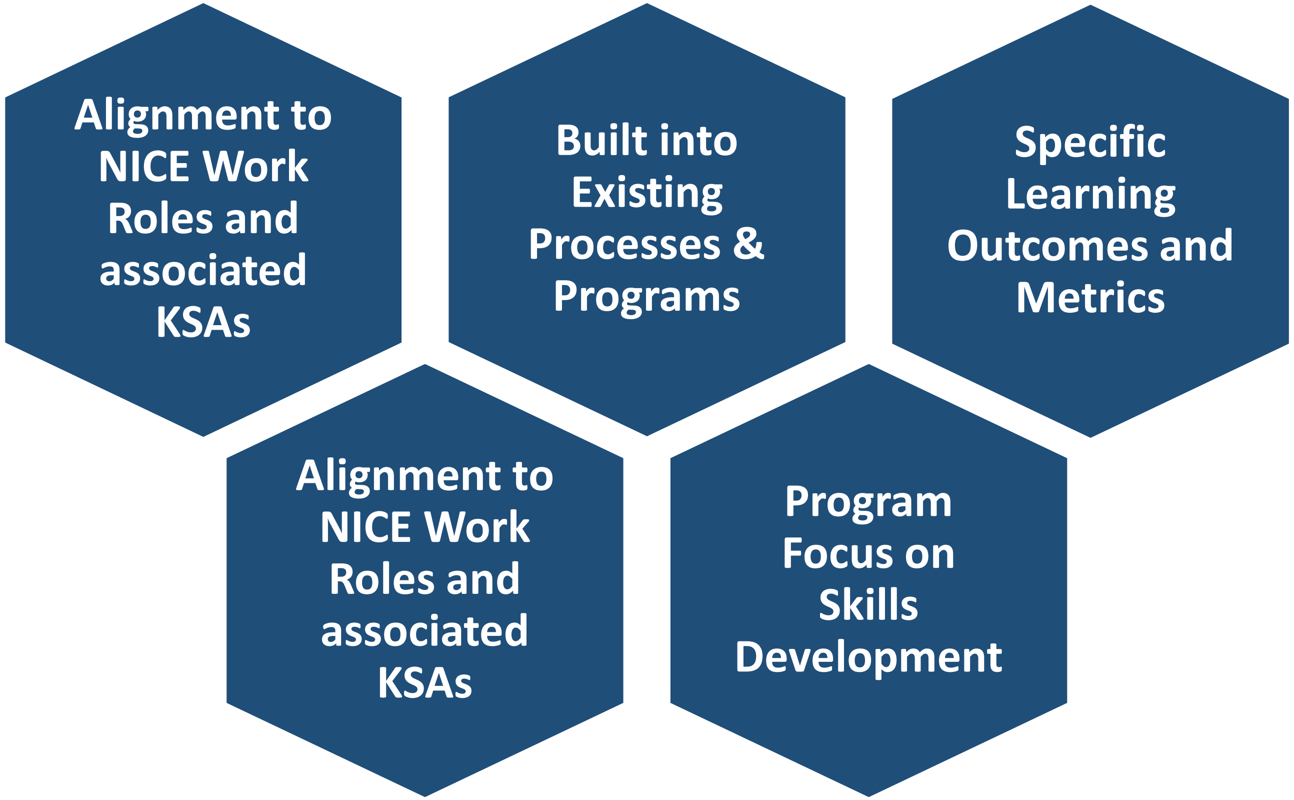
Address the development of **practicable and portable skills** by create consistent learning opportunities for the cyber workforce and adopt an integrated learning approach that incorporates a variety of training types, such as **skill-based training**, **individual** and **collective training**, virtual training, hands-on laboratories, mission-based activities, and exercises based on real-world scenarios.

Ensure all staff **has and maintains the requisite knowledge, skills, abilities, and technical execution of tasks** that align to the cyber work roles within the NICE workforce framework.

Promote employee development and growth will not only create a skilled workforce that is equipped to handle future cyber needs and vulnerabilities but will also **position VA as a cyber employer of choice** in today's highly competitive recruiting environment.

Experiential Learning

- What is Needed for a Successful Experiential Learning Program?



Alignment to NICE Work Roles and associated KSAs

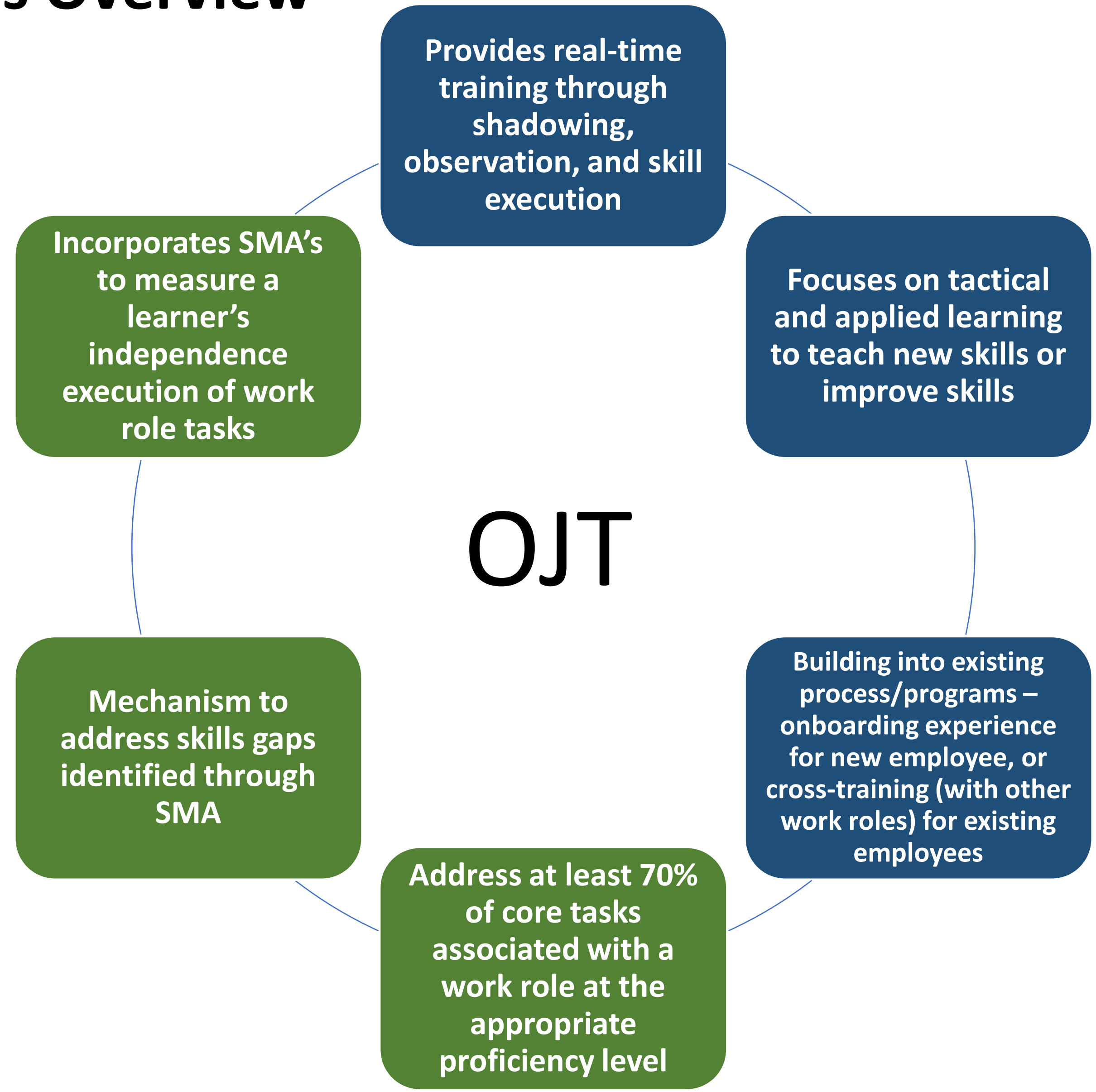
Built into Existing Processes & Programs

Specific Learning Outcomes and Metrics

Alignment to NICE Work Roles and associated KSAs

Program Focus on Skills Development

OJT Process Overview



OJT

Provides real-time training through shadowing, observation, and skill execution

Focuses on tactical and applied learning to teach new skills or improve skills

Building into existing process/programs – onboarding experience for new employee, or cross-training (with other work roles) for existing employees

Address at least 70% of core tasks associated with a work role at the appropriate proficiency level

Mechanism to address skills gaps identified through SMA

Incorporates SMA's to measure a learner's independence execution of work role tasks

Summary

A constantly evolving cyber landscape requires organization to take a more proactive role in the learning and development of their workforce by:

- Targeted training for specific work roles
- Hands-on training for skill development
- Skills-based models
- Support portability of skills within Federal Government

QUESTIONS?

Federal Information Security Educators (FISSEA) Fall Forum

BREAK

The Forum will resume at 2:45pm EDT

#FISSEA2022 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Welcome Back!

Menachem Goldstein

FISSEA Co-Chair
Cybersecurity Specialist, Enterprise Cybersecurity Department
Pension Benefit Guaranty Corporation

FISSEA Ignite!

Lightning Fast View of Supply Chain Defense and Offense

Donald Costello
Associate Professor
University of Nebraska-Lincoln

Lightning Fast View of Supply Chain Defense and Offense

FISSEA TALK NOVEMBER 15 2022

Integrate Supply Chain Management with Cybersecurity

- Know SC Management well
- Recognize without denial or minimization that SC's are under attack.
- Despite the fact the Cybersecurity itself involves a lot of Math it still has to be managed
- One aspect of SCM is the organization of the enterprise

What is Change Management ?

- ***Change management :the process of taking an individual or a group of people from a current state to a more desired state. It Is LARGELY due to new technology and globalization.***
  Through 2024, 50% of supply chain organizations will invest in
  applications that support artificial intelligence and advanced analytics capabilities organizations WILL seek tools that help them make better and more informed decisions faster.

Rapid Technology Changes greatly Impact SCD

Supply Chain Digitization. ...

□ Supply Chain Solutions Will Continue to Move to the Cloud. ...

□ **Omnichannel** Supply Chains Become the Norm. ...

□ ***Sustainability*** Is Becoming Essential. ...

□ Growth in ***Circular*** Supply Chains. ...

□ ***Agile Supply*** Chains. ...

□ Internet of Things.

□ ***New technology => New Ideas => New Terminology***

Supply Chain attacks & Ransomware

- *A supply chain attack breaks into the victim's network by taking advantage of vulnerabilities in the computer systems of the company's supply chain partners. The attacks are an attempt to infiltrate an organization's computers to gain access to the networks of its many suppliers and partners. Supply chains are perceived as especially vulnerable to ransomware attacks due to the broad targets they represent and the opportunity to cause large-scale damage via a single exploited vulnerability*.

Look and see that

- Supply Chain Management is a complex and fascinating field
- The rate of technological change is so large
- You, we have to study and learn about Change Management
- Recognize that we are in a Technology War
- Know that ***NIST*** exists and it is an essential tool in understanding SC and their defense,
- Know that there is something called a Cybersecure attack to match Supply Chain attacks.

Lightning Fast Key Points made

Environment

- Systems view essential
- Supply Chain Management Basics Change
- Understanding Change Management Key
- We are in a Technology War
- The Art of War

You

- Do a YouTube on a Systems View and Change Management
- Keep Instagram of how your organization is using Supply Chain Management
- Allocate time each week to study Cybersecurity

The Art of War

- ***Sun Tzu is traditionally credited as the author of The Art of War, an influential work of military strategy that has affected both Western and East Asian philosophy and military thinking. It focuses much more on alternatives to battle and even to war than on war itself, such as stratagem, delay, the use of spies, the making and keeping of alliances, the uses of deceit, and a willingness to submit, at least temporarily, to more powerful foes.[***
- ***Google and You Tube art of WAR***

Contact

- *dcostello2@unl.edu*

Security Awareness and Training Contest Recognition

Tamara Kravitz

FISSEA Contest Lead

FISSEA

Security Awareness and Training Contest

Contest Winners

Tamara Kravitz, PMP
FISSEA Working Group Member
November 2022

Contest

Categories

1. Awareness Poster
2. Awareness Video
3. Awareness Website
4. Innovative Solutions
5. Awareness Newsletter
6. Training Awareness
7. Cybersecurity Podcast
8. Cybersecurity Blog

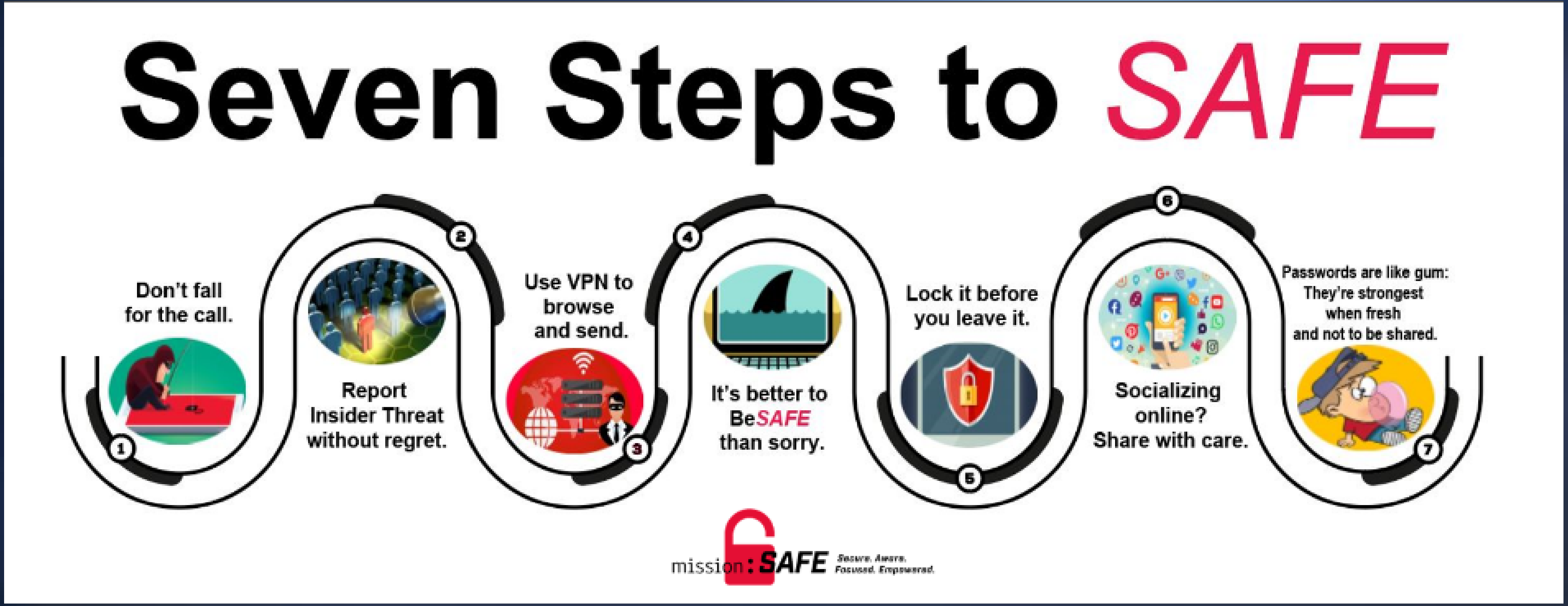
Judges

- Not affiliated with any of the groups that submitted entries
- From various positions, industries, and academics.

Poster Entries (6)

1. Cofense
2. Labcorp
3. KnowBe4
4. Department of State
5. Federal Retirement Thrift Investment Board
6. United States Postal Service

Best Poster



Seven Steps to *SAFE*

1. Don't fall for the call.
2. Report Insider Threat without regret.
3. Use VPN to browse and send.
4. It's better to Be*SAFE* than sorry.
5. Lock it before you leave it.
6. Socializing online? Share with care.
7. Passwords are like gum: They're strongest when fresh and not to be shared.

mission:SAFE Secure. Aware. Focused. Empowered.

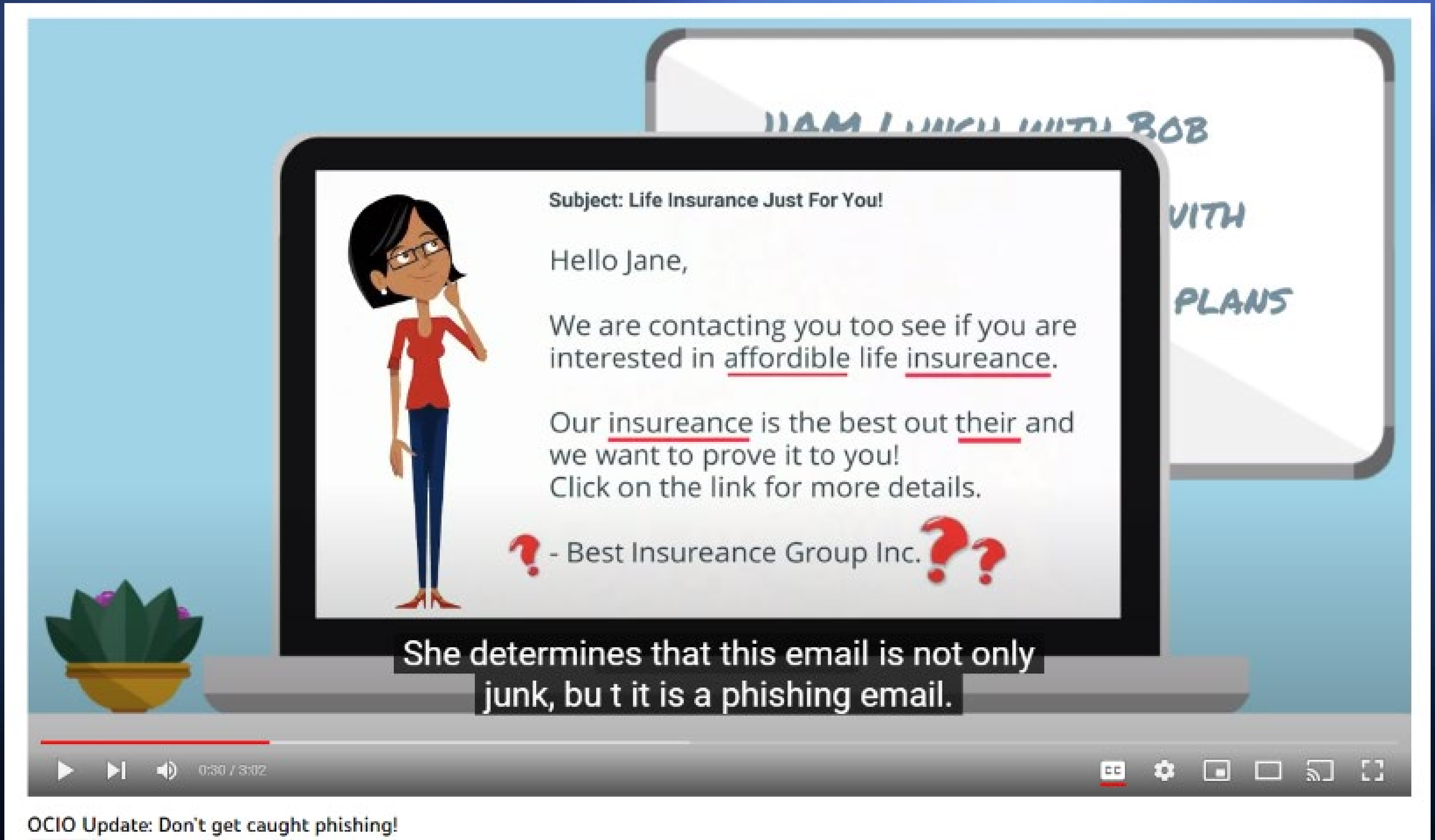
Organization: Labcorp

Video Entries (6)

1. **Cofense**
2. **Federal Retirement Thrift Investment Board (FRTIB)**
3. **Dept. of State (DOS)**
4. **Labcorp**
5. **Indian Health Service (IHS)**
6. **U.S. Office of Personnel Management (OPM)**

Video Winner!

Office of Personnel Management, Office of the Chief Information Security Officer, Cybersecurity Program



Subject: Life Insurance Just For You!

Hello Jane,

We are contacting you too see if you are interested in affordible life insureance.

Our insureance is the best out their and we want to prove it to you!
Click on the link for more details.

- Best Insureance Group Inc.

She determines that this email is not only junk, bu t it is a phishing email.

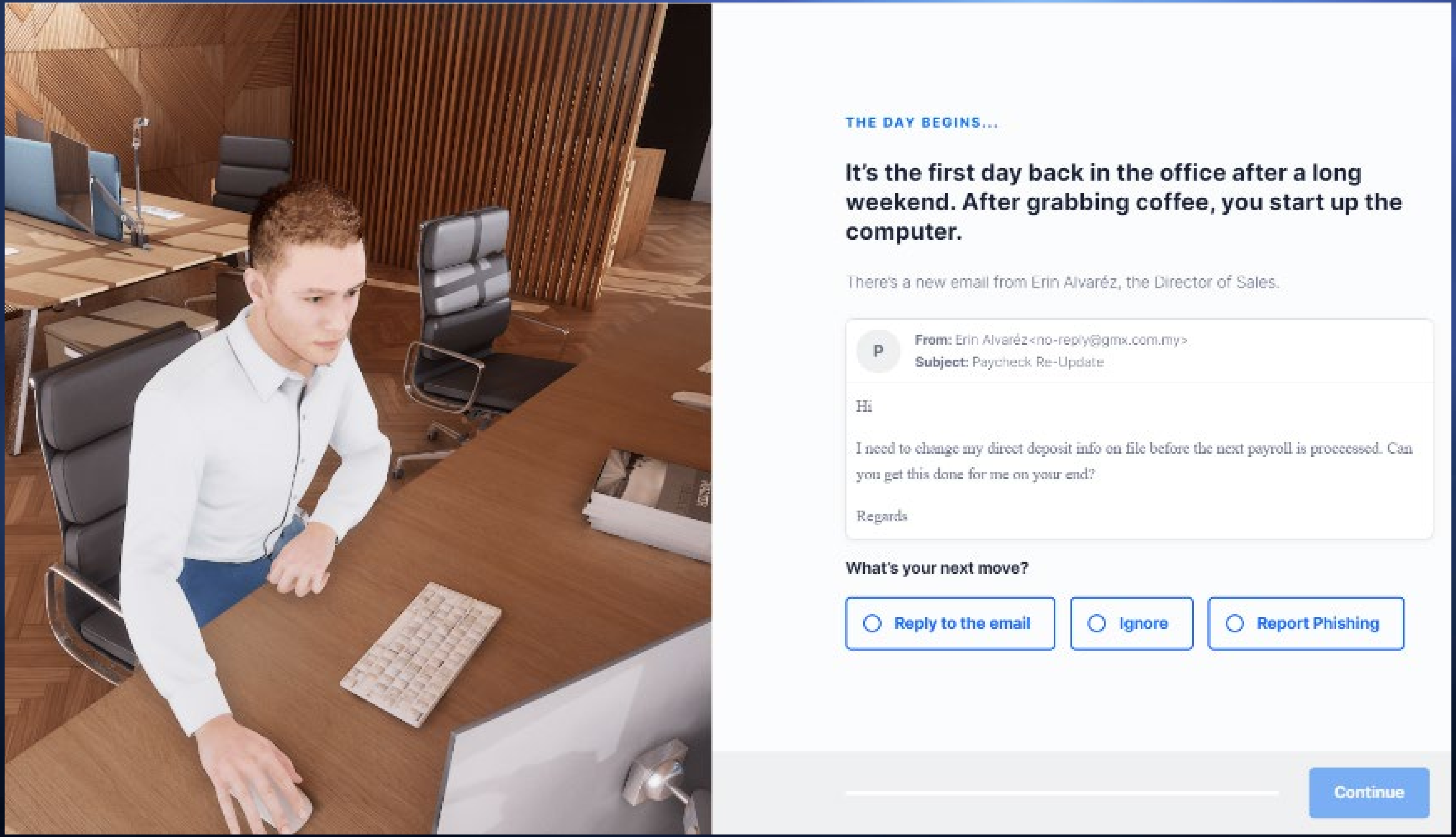
OCIO Update: Don't get caught phishing!

Website Entries (4)

1. **Indian Health Service (IHS)**
2. **Cofense**
3. **U.S. General Services Administration (GSA)**
4. **KnowBe4**

Website Winner!

Cofense



THE DAY BEGINS...

It's the first day back in the office after a long weekend. After grabbing coffee, you start up the computer.

There's a new email from Erin Alvaréz, the Director of Sales.

P **From:** Erin Alvaréz<no-reply@gmx.com.my>
Subject: Paycheck Re-Update

Hi

I need to change my direct deposit info on file before the next payroll is processed. Can you get this done for me on your end?

Regards

What's your next move?

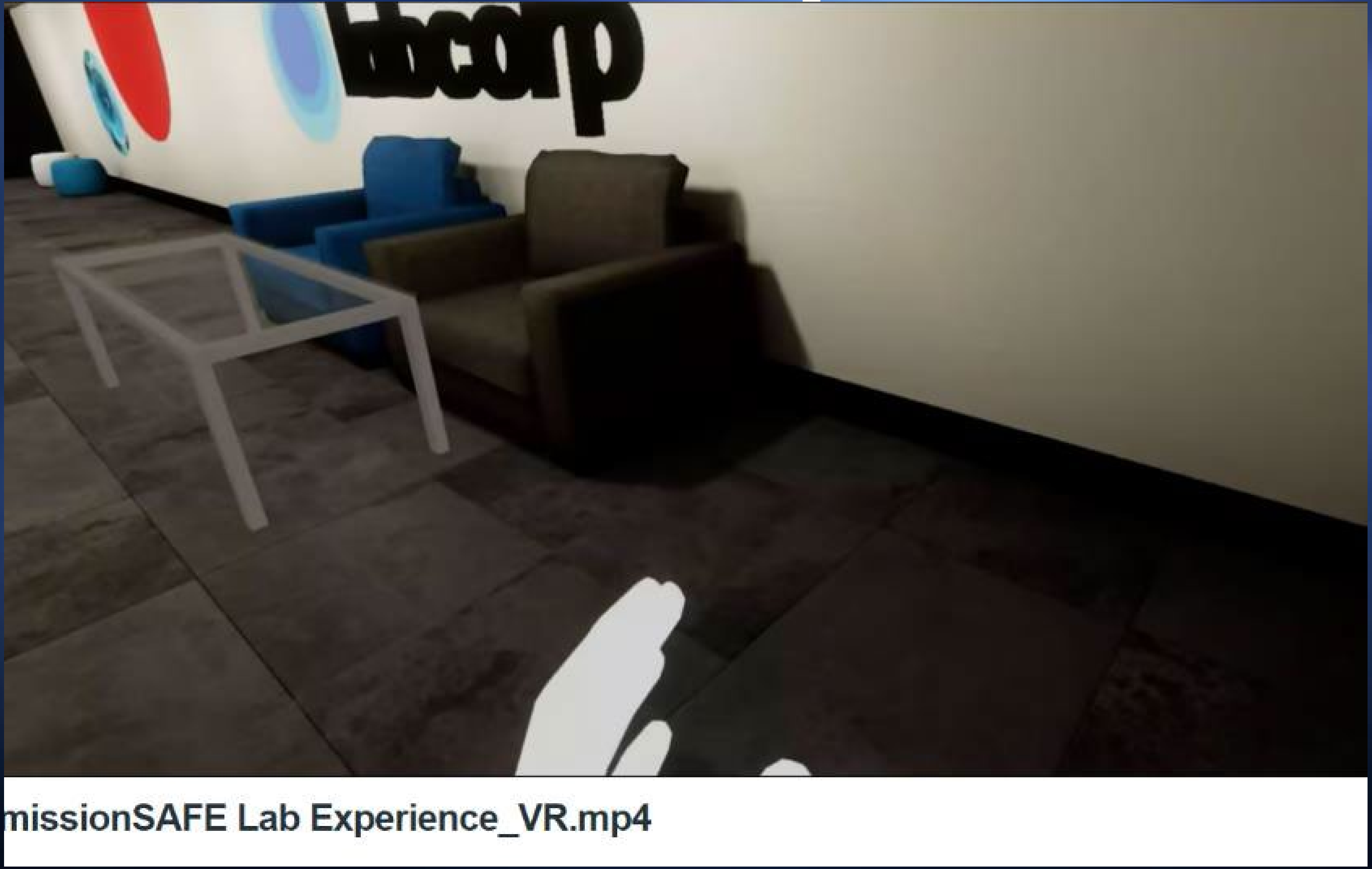
○ Reply to the email ○ Ignore ○ Report Phishing

Innovative Solutions Entries (8)

1. ECS
2. United States Postal Service (USPS)
3. Centers for Medicare & Medicaid Services (CMS)
4. Labcorp
5. U.S. Department of Education
6. Idaho National Lab
7. Cofense
8. Indian Health Service (IHS)

Innovative Solutions Winner!

Labcorp



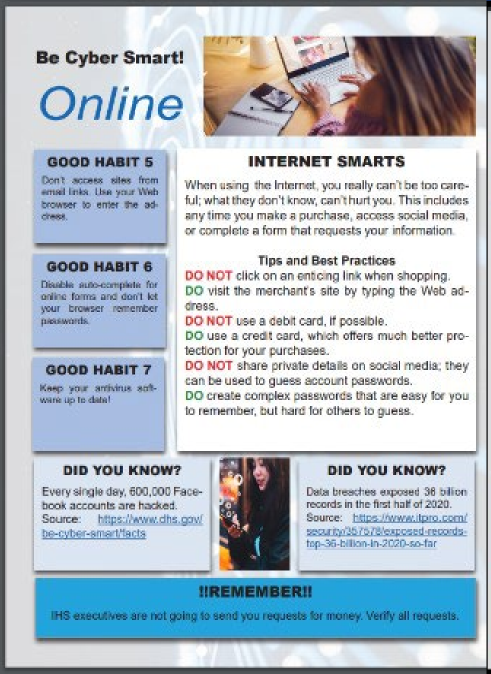
missionSAFE Lab Experience_VR.mp4

Newsletter Entries (6)

1. **Centers for Medicare & Medicaid Services (CMS)**
2. **Indian Health Service (HIS)**
3. **Labcorp**
4. **Cofense**
5. **U.S. Department of Education**
6. **Department of State (DOS)**

Innovative Solutions Winner!

Indian Health Service



Be Cyber Smart!

Online

GOOD HABIT 5

Don't access sites from email links. Use your Web browser to enter the address.

GOOD HABIT 6

Disable auto-complete for online forms and don't let your browser remember passwords.

GOOD HABIT 7

Keep your antivirus software up to date!

INTERNET SMARTS

When using the Internet, you really can't be too careful; what they don't know, can't hurt you. This includes any time you make a purchase, access social media, or complete a form that requests your information.

Tips and Best Practices

DO NOT click on an enticing link when shopping.
DO visit the merchant's site by typing the Web address.
DO NOT use a debit card, if possible.
DO use a credit card, which offers much better protection for your purchases.
DO NOT share private details on social media; they can be used to guess account passwords.
DO create complex passwords that are easy for you to remember, but hard for others to guess.

DID YOU KNOW?

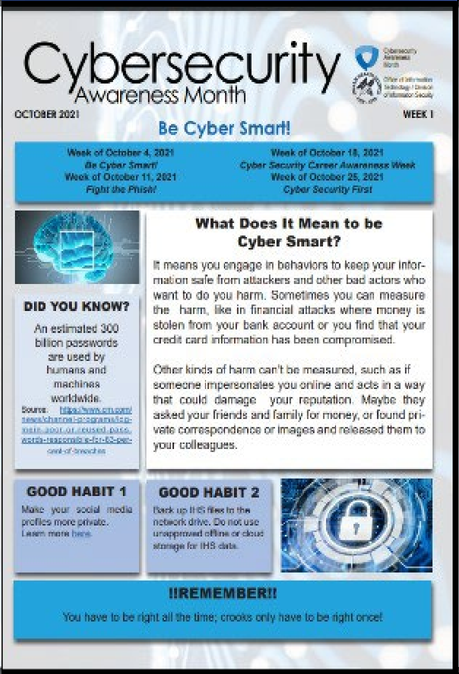
Every single day, 600,000 Facebook accounts are hacked.
Source: https://www.dhs.gov/be-cyber-smart/facts

DID YOU KNOW?

Data breaches exposed 36 billion records in the first half of 2020.
Source: https://www.itpro.com/security/357578/exposed-records-top-36-billion-in-2020-so-far

!!REMEMBER!!

IHS executives are not going to send you requests for money. Verify all requests.



Cybersecurity Awareness Month

Cybersecurity Awareness Month
Office of Information Technology / Division of Information Security

OCTOBER 2021

WEEK 1

Be Cyber Smart!

Week of October 4, 2021
Be Cyber Smart!
Week of October 11, 2021
Fight the Phish!

Week of October 18, 2021
Cyber Security Career Awareness Week
Week of October 25, 2021
Cyber Security First

DID YOU KNOW?

An estimated 300 billion passwords are used by humans and machines worldwide.
Source: https://www.crn.com/news/channel-programs/lp-main-poor-or-reused-passwords-responsible-for-63-percent-of-breaches

What Does It Mean to be Cyber Smart?

It means you engage in behaviors to keep your information safe from attackers and other bad actors who want to do you harm. Sometimes you can measure the harm, like in financial attacks where money is stolen from your bank account or you find that your credit card information has been compromised.

Other kinds of harm can't be measured, such as if someone impersonates you online and acts in a way that could damage your reputation. Maybe they asked your friends and family for money, or found private correspondence or images and released them to your colleagues.

GOOD HABIT 1

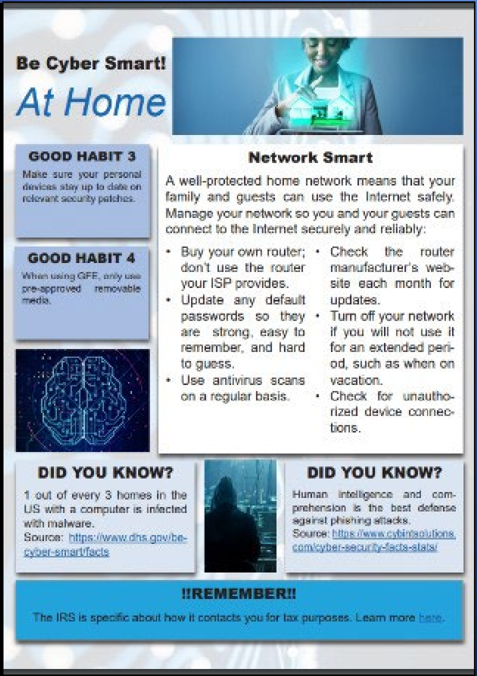
Make your social media profiles more private. Learn more here.

GOOD HABIT 2

Back up IHS files to the network drive. Do not use unapproved offline or cloud storage for IHS data.

!!REMEMBER!!

You have to be right all the time; crooks only have to be right once!



Be Cyber Smart!

At Home

GOOD HABIT 3

Make sure your personal devices stay up to date on relevant security patches.

GOOD HABIT 4

When using GFE, only use pre-approved removable media.

Network Smart

A well-protected home network means that your family and guests can use the Internet safely. Manage your network so you and your guests can connect to the Internet securely and reliably:

- Buy your own router; don't use the router your ISP provides.
- Update any default passwords so they are strong, easy to remember, and hard to guess.
- Use antivirus scans on a regular basis.
- Check the router manufacturer's website each month for updates.
- Turn off your network if you will not use it for an extended period, such as when on vacation.
- Check for unauthorized device connections.

DID YOU KNOW?

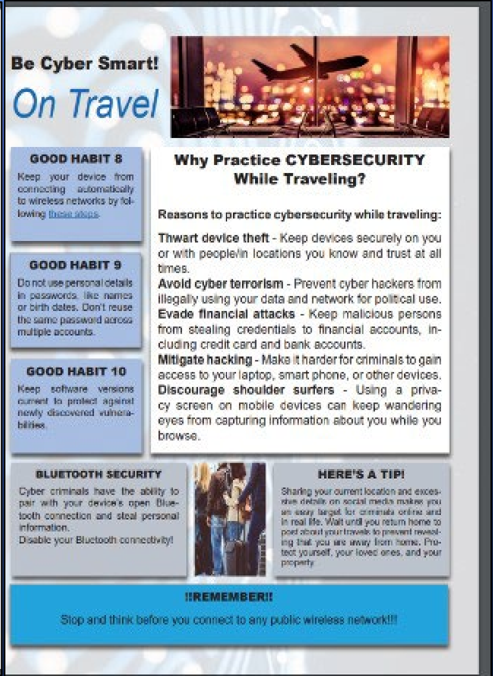
1 out of every 3 homes in the US with a computer is infected with malware.
Source: https://www.dhs.gov/be-cyber-smart/facts

DID YOU KNOW?

Human intelligence and comprehension is the best defense against phishing attacks.
Source: https://www.cybintsolutions.com/cyber-security-facts-stats/

!!REMEMBER!!

The IRS is specific about how it contacts you for tax purposes. Learn more here.



Be Cyber Smart!

On Travel

GOOD HABIT 8

Keep your device from connecting automatically to wireless networks by following these steps.

GOOD HABIT 9

Do not use personal details in passwords, like names or birth dates. Don't reuse the same password across multiple accounts.

GOOD HABIT 10

Keep software versions current to protect against newly discovered vulnerabilities.

Why Practice CYBERSECURITY While Traveling?

Reasons to practice cybersecurity while traveling:

Thwart device theft - Keep devices securely on you or with people/in locations you know and trust at all times.
Avoid cyber terrorism - Prevent cyber hackers from illegally using your data and network for political use.
Evade financial attacks - Keep malicious persons from stealing credentials to financial accounts, including credit card and bank accounts.
Mitigate hacking - Make it harder for criminals to gain access to your laptop, smart phone, or other devices.
Discourage shoulder surfers - Using a privacy screen on mobile devices can keep wandering eyes from capturing information about you while you browse.

BLUETOOTH SECURITY

Cyber criminals have the ability to pair with your device's open Bluetooth connection and steal personal information.
Disable your Bluetooth connectivity!

HERE'S A TIP!

Sharing your current location and excessive details on social media makes you an easy target for criminals online and in real life. Wait until you return home to post about your travels to prevent revealing that you are away from home. Protect yourself, your loved ones, and your property.

!!REMEMBER!!

Stop and think before you connect to any public wireless network!!!

Training Entries (8)

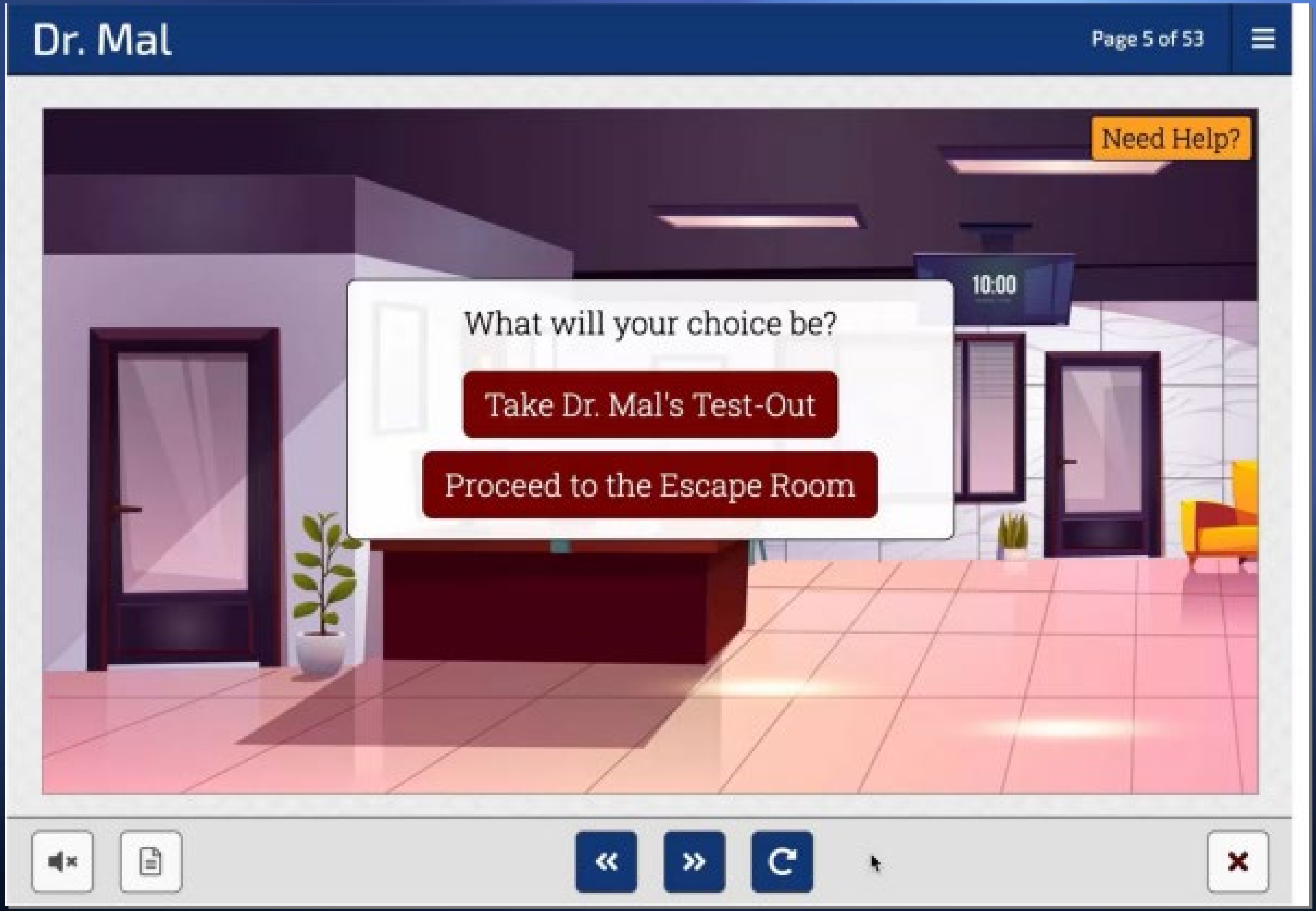
1. Cofense
2. Centers for Medicare & Medicaid Services
3. KnowBe4
4. Labcorp
5. Social Security Administration
6. Indian Health Service
7. U.S. Department of Education
8. DHS CISA

Training Winner(s)!

Cofense

Training Winner(s)!

U.S. Department of Education



What will your choice be?

Podcast Entries (2)

1. **Centers for Medicare & Medicaid Services**
2. **KnowBe4**

Podcast Winner

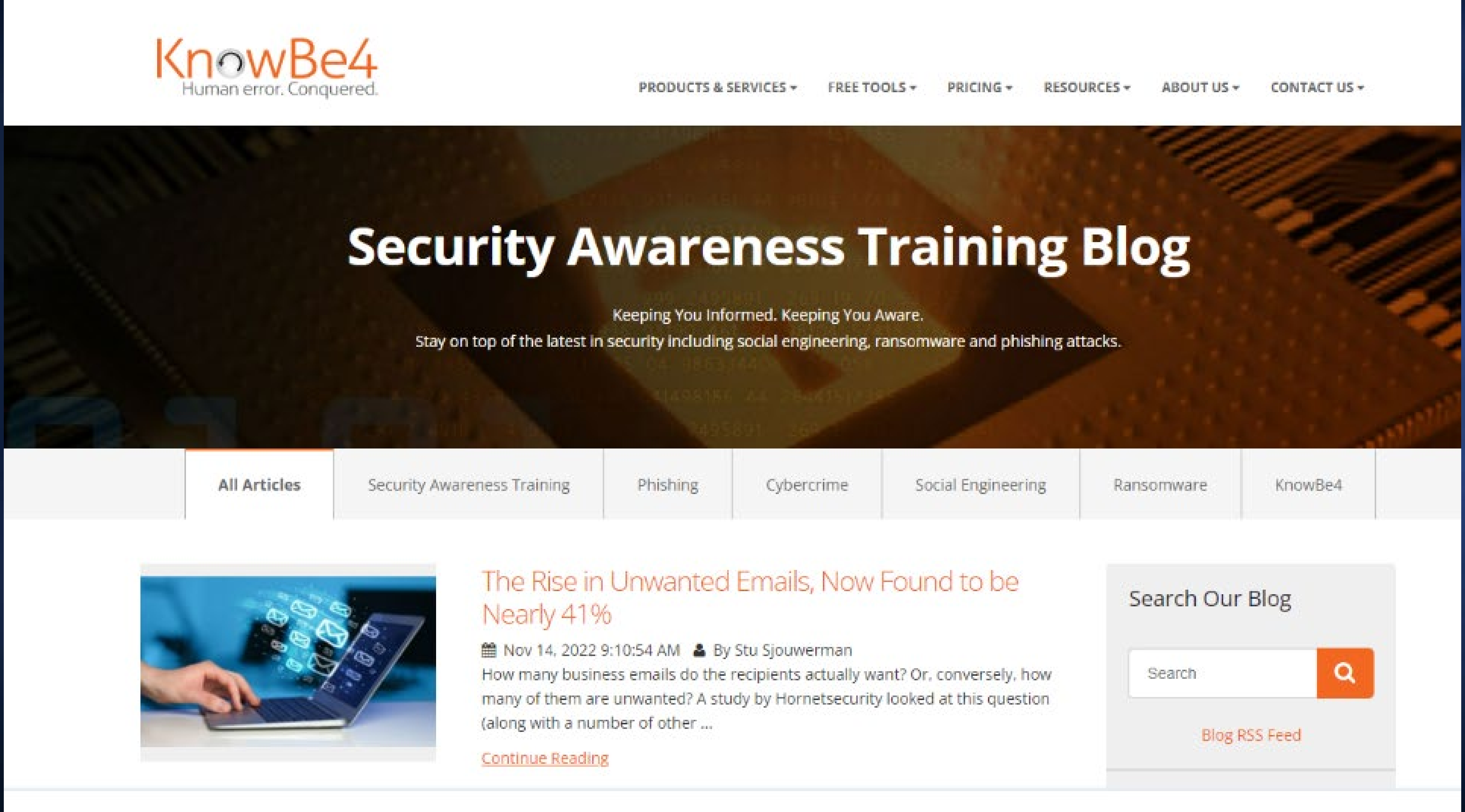
KnowBe4

The Security Masterminds Podcast takes a deep dive into cybersecurity topics with engaging and thought-provoking discussions. Hosts Erich Kron and Jelle Wieringa take a deep dive into cybersecurity topics, trends, and challenges with industry leaders and experts from around the world. Guests have included chief information security officers (CISOs), social engineers, industry leaders, experts on emerging technologies and movie directors. The monthly podcast has rapidly grown a loyal fan base who appreciate the depth of discussions and the 'no filler' approach the podcast takes. Security Masterminds brings the best in all things cybersecurity, taking an in-depth look at the industry's most pressing issues and trends.

Blog Entries (2)

1. **Indian Health Service**
2. **KnowBe4**

Blog Winner



KnowBe4
Human error. Conquered.

Security Awareness Training Blog

Keeping You Informed. Keeping You Aware.
Stay on top of the latest in security including social engineering, ransomware and phishing attacks.

The Rise in Unwanted Emails, Now Found to be Nearly 41%

Nov 14, 2022 9:10:54 AM By Stu Sjouwerman

How many business emails do the recipients actually want? Or, conversely, how many of them are unwanted? A study by Hornetsecurity looked at this question (along with a number of other ...

Continue Reading

Search Our Blog

Thanks to all
who submitted entries!

Thanks to our judges!

Security Awareness and Training People’s Choice Results

Tamara Kravitz

FISSEA Contest Lead

PEOPLE'S CHOICE AWARDS

CATEGORY (Votes)	WINNER (Top Percentage of Votes)
Awareness Poster (57)	COFENSE (47.11%)
Awareness Video (50)	COFENSE (44.64%)
Awareness Website (72)	COFENSE (60.50%)
Innovative Solutions (64)	US Department of Education (44.03%)
Awareness Newsletter (74)	US Department of Education (51.03%)
Training Awareness (64)	US Department of Education (36.57%)
Cybersecurity Podcast (50)	Centers for Medicare and Medicaid Services (56.82%)
Cybersecurity Blog (51)	Indian Health Service (54.04%)

“Choose Your Own Misadventure”

Mark Henderson

Internal Revenue Service

FISSEA Fall Forum “Choose your own misadventure”

Mark Henderson

Internal Revenue Service

Online Fraud Detection and Prevention

OS:CTO:C:O:OFDP

Disclaimer

Any views or opinions are my own and do not necessarily reflect the official views of the U.S. Treasury.

Overview

- present select findings from NIST 8420A
- review potential actions of phishing exercise recipients
- provide reasons why exercises typically cause issues
- describe operational impacts of phishing exercises
- compare data from observed phishing exercises
- review prohibitions against using agencies or brands
- demonstrate ways to reduce the likelihood of issues with phishing exercises

Perform phishing exercises (85%)

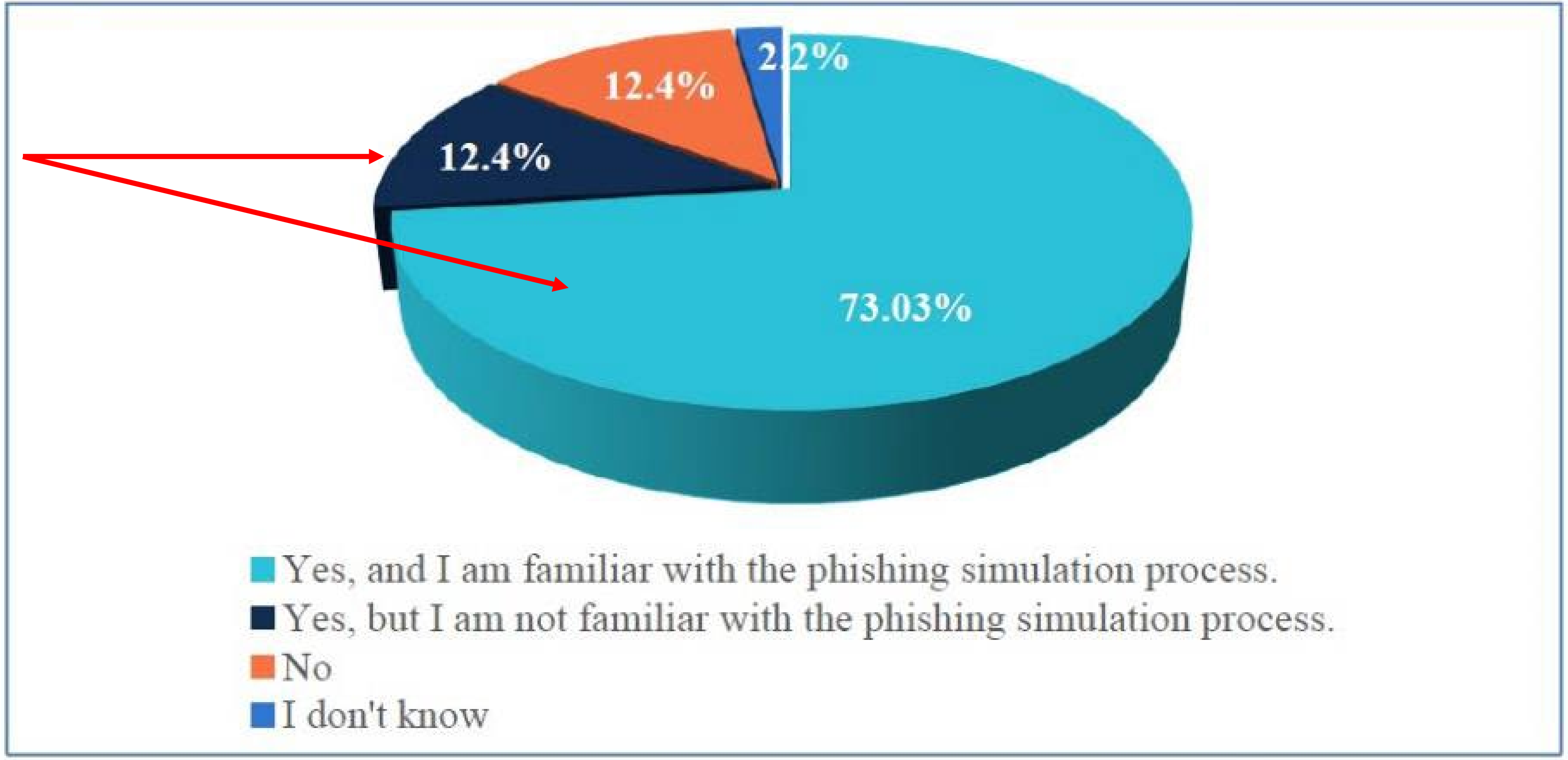


Figure 11: Organizations performing phishing simulations (n=89)

Phishing click rates (#2) and employee reporting of simulated phishing (#4)

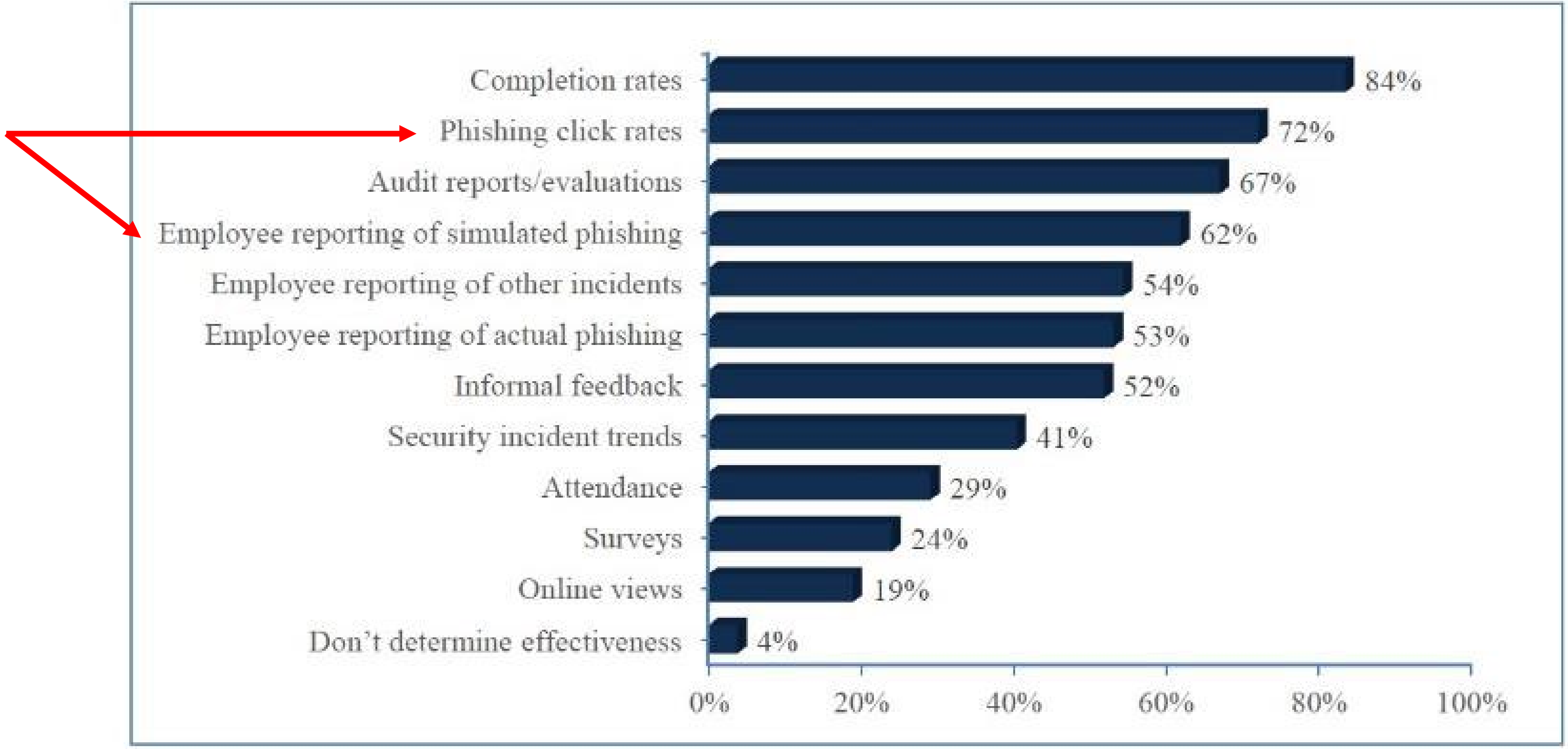


Figure 24: Measures of effectiveness (n=79)

If 40% consult HR/Legal … then 60% don’t

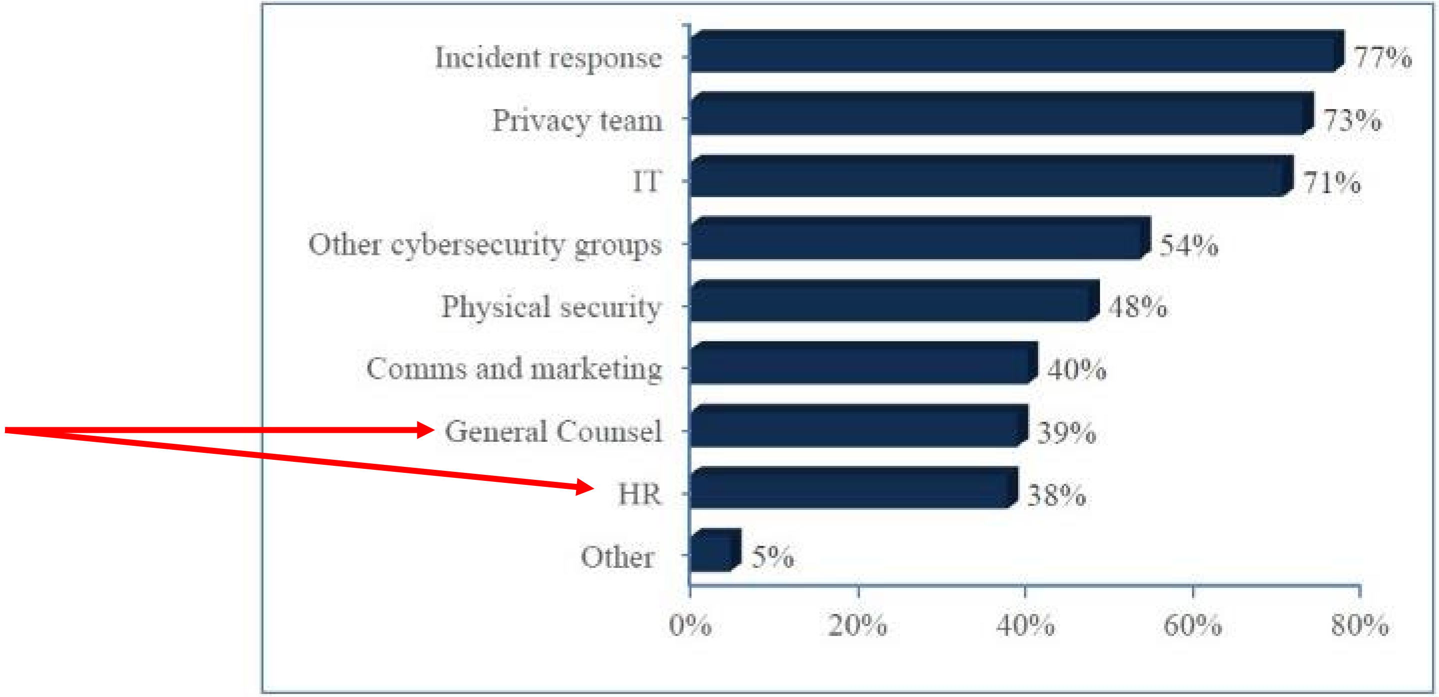


Figure 18: Internal groups collaborating with security awareness programs (n=81)

Additional findings from NIST 8420A

- “Ninety percent of survey participants are part-time” [p. 9]
- “fairly equally distributed between Departments (32.3%), sub-components (31.3%), and independent agencies (35.4%)” [p. 10]
- “Organizations with between 1,000 and 4,999 federal employees made up the largest subset (29.2% of organizations), followed by organizations with 50,000 or more employees (21.9%)” [p. 11]
- “32% of the 28 organizations had programs of less than 10,000 federal employees and contractors (none less than 1,000)” [p. 12]
- “… (n=24, 86%) have a mix of federal employees and contractors working together on the program.” [p. 15]

What is a “controversial” lure?

If you don’t know, please ask your Human Resources and/or Legal department

Recent examples [not meant to be exhaustive]:

- Fake bonuses
  - GoDaddy, National Institutes of Health study (large Italian hospital), OSHU (oshu.edu), Tribune, West Midlands Trains
- Fake employee appreciation awards
  - Tacoma Public Schools in Washington
- Use of COVID-19

Simplified actions of exercise recipients

“Click” = Fail

- Receive the exercise landing page

“Don’t click” = Pass

- Do **<u>not</u>** receive the exercise landing page

“Clickers”

open email and click attachment (or URL)

- deliberately [“clickers”]
- by mistake (e.g., trying to report the email) [the “accidental” clicker]
- by analysis (e.g., use a URL analysis engine) [the “curious” clicker]

“Non-clickers”

- open email, don’t click and report internally
- open email, don’t click, don’t report (e.g., delete)
- don’t open email but delete by accident (e.g., cleaning Inbox)
- **don’t open email (e.g., sick, vacation, etc.) … but might later**
- **open email, don’t click and report externally**

Why some phishing exercises cause issues

- Some cybersecurity professionals are **<u>not</u>** familiar with relevant laws
- Some organizations:
  - do **<u>not</u>** consult counsel or HR before conducting a phishing exercise
  - do **<u>not</u>** notify and do **<u>not</u>** obtain permission to use an agency or brand
- “Non-clickers” are unpredictable
- When contact information is **<u>not</u>** available, external organizations will have difficulty contacting the responsible parties

Prohibition against USG agencies

“Copyright Exceptions for U.S. Government Works,” https://www.usa.gov/government-works#item-206099 (“You cannot use government trademarks or government agencies' logos without permission.”)

IRS-specific prohibitions

- 15 U.S.C. § 1051 (“irs” is a registered servicemark)
- 31 U.S.C. § 333 (“any colorable imitation”)
- IRS.gov “Report Phishing” https://www.irs.gov/privacy-disclosure/report-phishing (“What if I want to train my employees on IRS or tax-related phishing emails by conducting a tax-related phishing exercise?”)

Department of Education

- https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2021-12-15/guidance-about-use-protected-brands-and-official-government-names-logos-or-insignia
- https://fsapartners.ed.gov/knowledge-center/topics/fsa-cybersecurity-announcements-and-guidance (FSA Cybersecurity Topics)

Prohibition against use of brands

- Trademark law(s)
  - “Throughout the life of the registration, you must police and enforce your rights.” [USPTO]
- Domain Name Disputes (dndisputes.com) [Uniform Domain-Name Dispute-Resolution Policy]
  - Facebook UDRP against Proofpoint
  - Belfius Bank UDRP against Phished
- “Stop Phishing with Bad Fake Bait” (EDUCAUSE) [see comments from Shane McGee CPO/GC at Cofense]

What if “non-clickers” reported externally to a USG agency?

“Anti-Phishing Testers Put Themselves on the Hook” [August 2020]

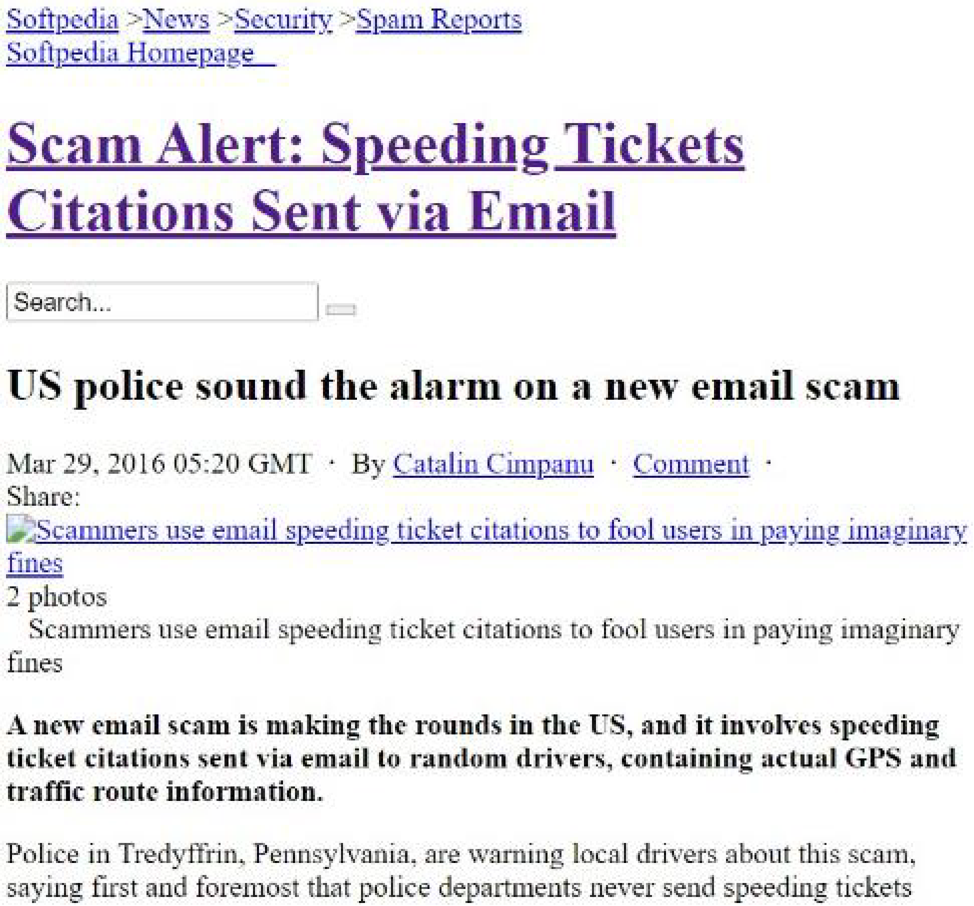
Anti-Phishing Testers Put Themselves on the Hook › Pretending to be the IRS, even in self-defense, turns out to be a bad idea

BY ROBERT N. CHARETTE

26 AUG 2020 | 5 MIN READ

What if “non-clickers” reported externally to local law enforcement?

Tredyffrin Police Department [03/22/2016?]



Softpedia >News >Security >Spam Reports
Softpedia Homepage

Scam Alert: Speeding Tickets Citations Sent via Email

Search...

US police sound the alarm on a new email scam

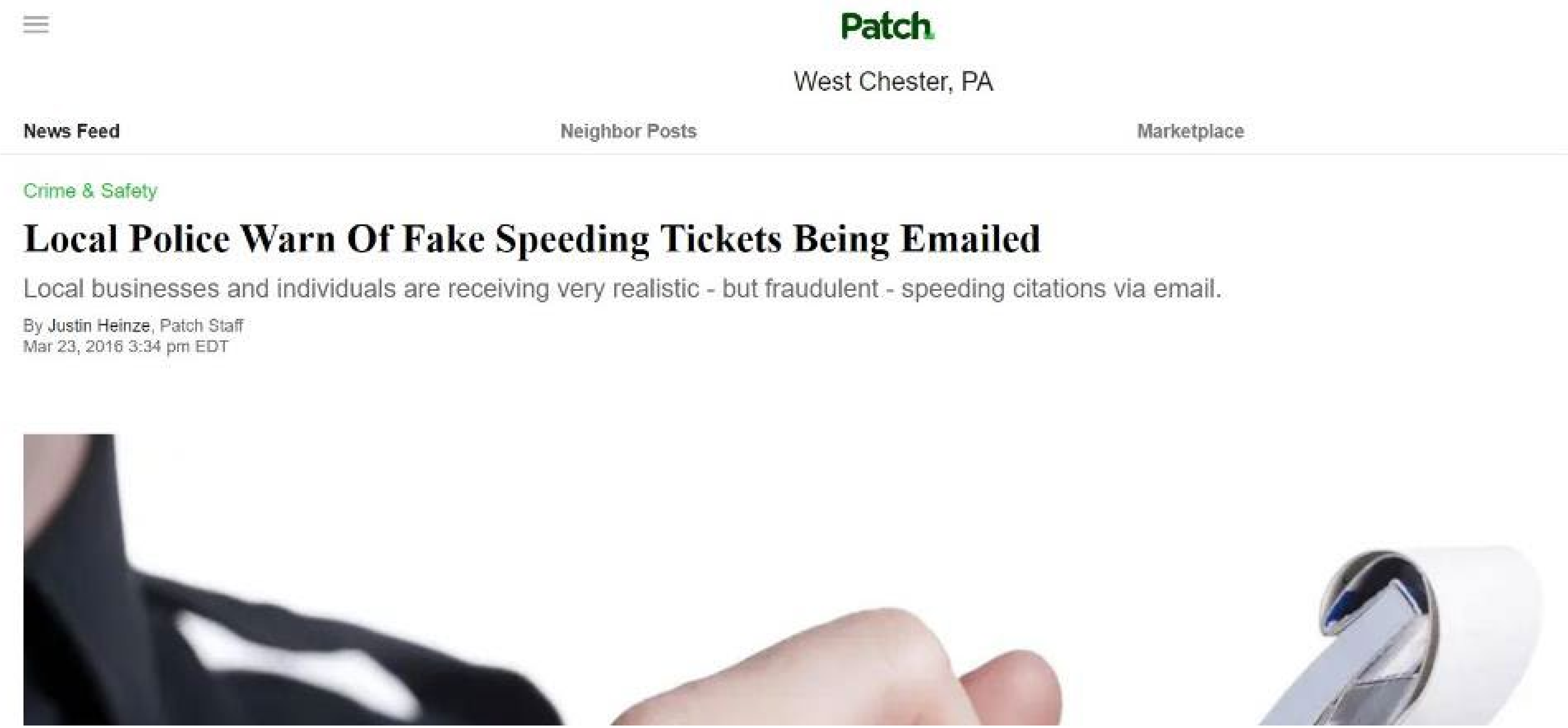
Mar 29, 2016 05:20 GMT · By Catalin Cimpanu · Comment ·
Share:
Scammers use email speeding ticket citations to fool users in paying imaginary fines
2 photos
Scammers use email speeding ticket citations to fool users in paying imaginary fines

A new email scam is making the rounds in the US, and it involves speeding ticket citations sent via email to random drivers, containing actual GPS and traffic route information.

Police in Tredyffrin, Pennsylvania, are warning local drivers about this scam, saying first and foremost that police departments never send speeding tickets

"This scam was brought to their attention last week, when a local business' employee received one such alert via email."

Community coverage [03/23/2016]



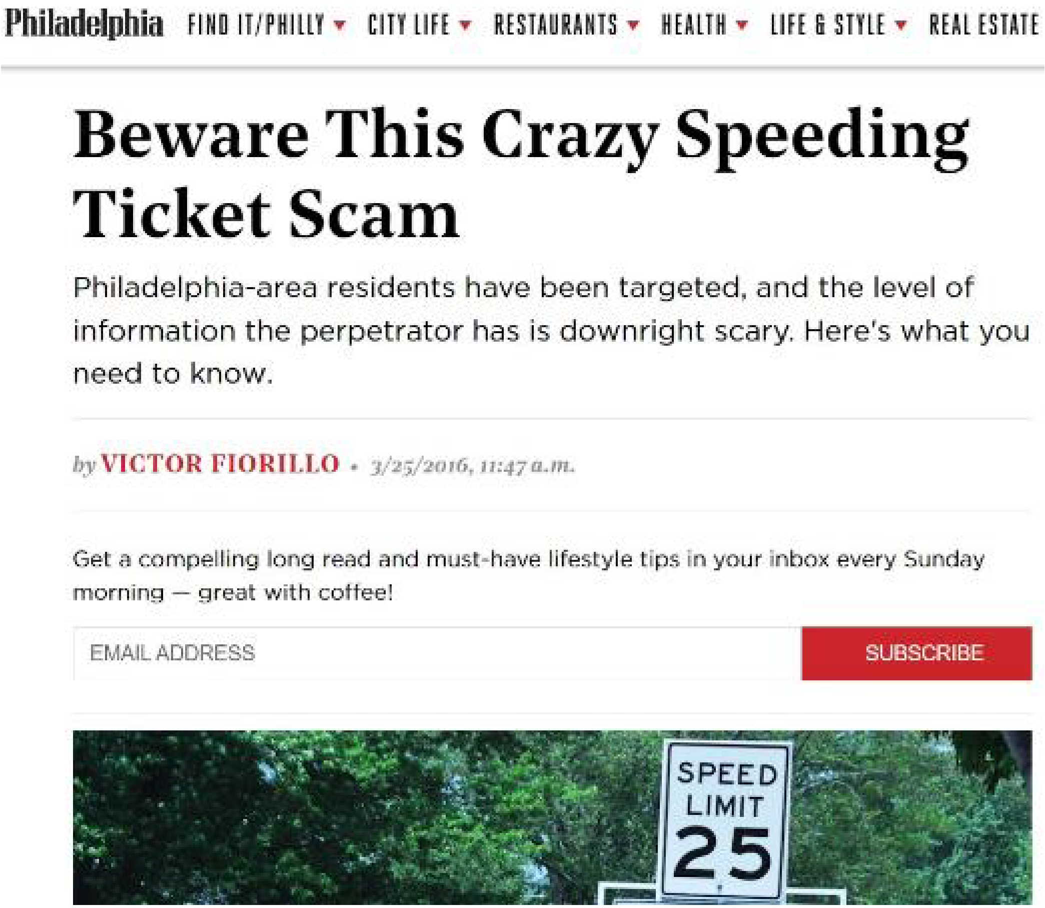
Crime & Safety

Local Police Warn Of Fake Speeding Tickets Being Emailed

Local businesses and individuals are receiving very realistic - but fraudulent - speeding citations via email.

By Justin Heinze, Patch Staff
Mar 23, 2016 3:34 pm EDT

Local media coverage [3/25/2016]



Beware This Crazy Speeding Ticket Scam

Philadelphia-area residents have been targeted, and the level of information the perpetrator has is downright scary. Here's what you need to know.

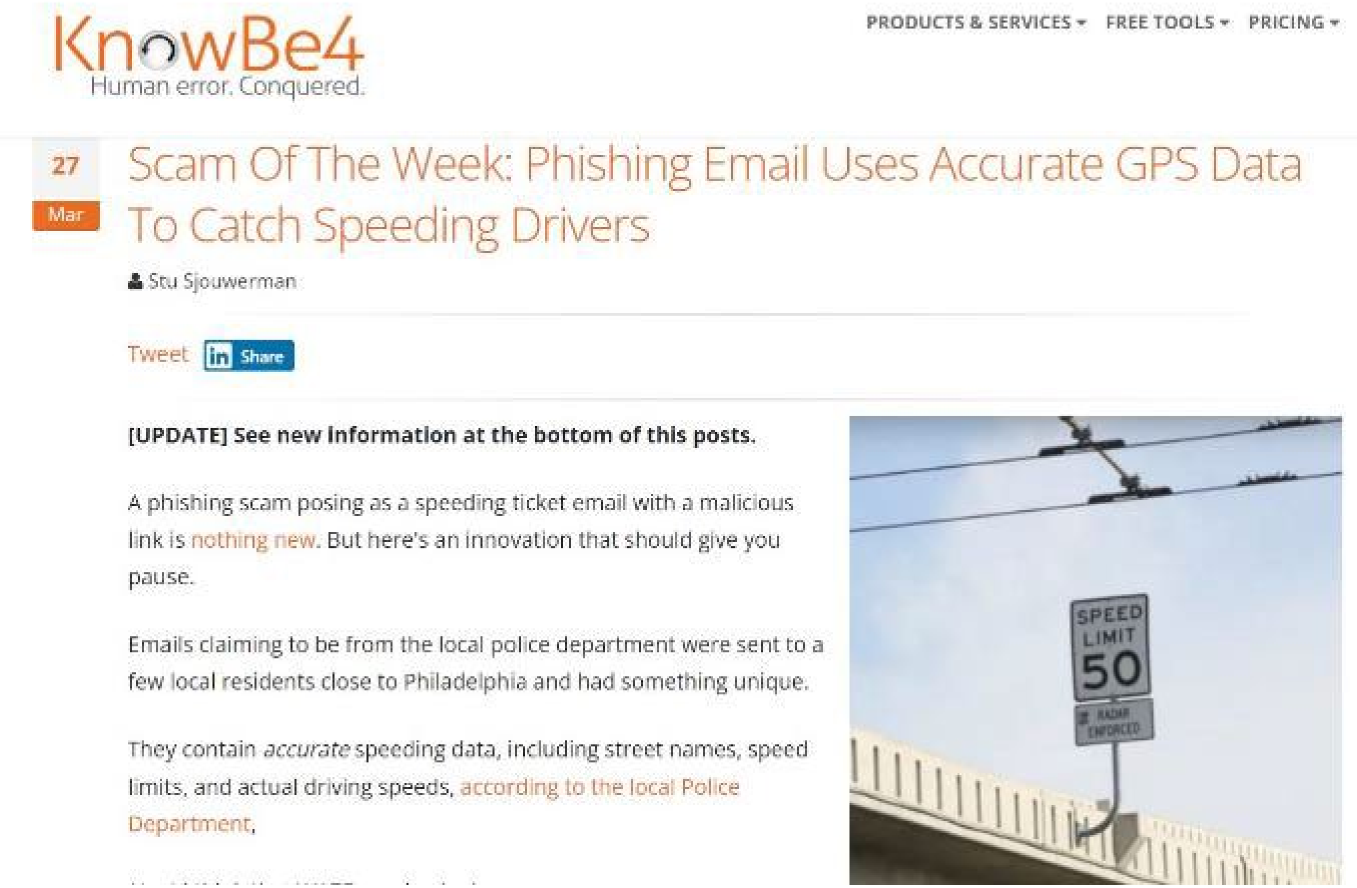
by VICTOR FIORILLO • 3/25/2016, 11:47 a.m.

Get a compelling long read and must-have lifestyle tips in your inbox every Sunday morning — great with coffee!

EMAIL ADDRESS | SUBSCRIBE

- “Philadelphia-area residents have been targeted, and the level of information the perpetrator has is downright scary”
- “The Tredyffrin Police Department in Chester County [explained] that three local residents reported receiving emails notifying them of speeding infractions”

KnowBe4 blog [03/27/2016]



KnowBe4
Human error. Conquered.

PRODUCTS & SERVICES ▾ FREE TOOLS ▾ PRICING ▾

27
Mar

Scam Of The Week: Phishing Email Uses Accurate GPS Data To Catch Speeding Drivers

Stu Sjouwerman

Tweet Share

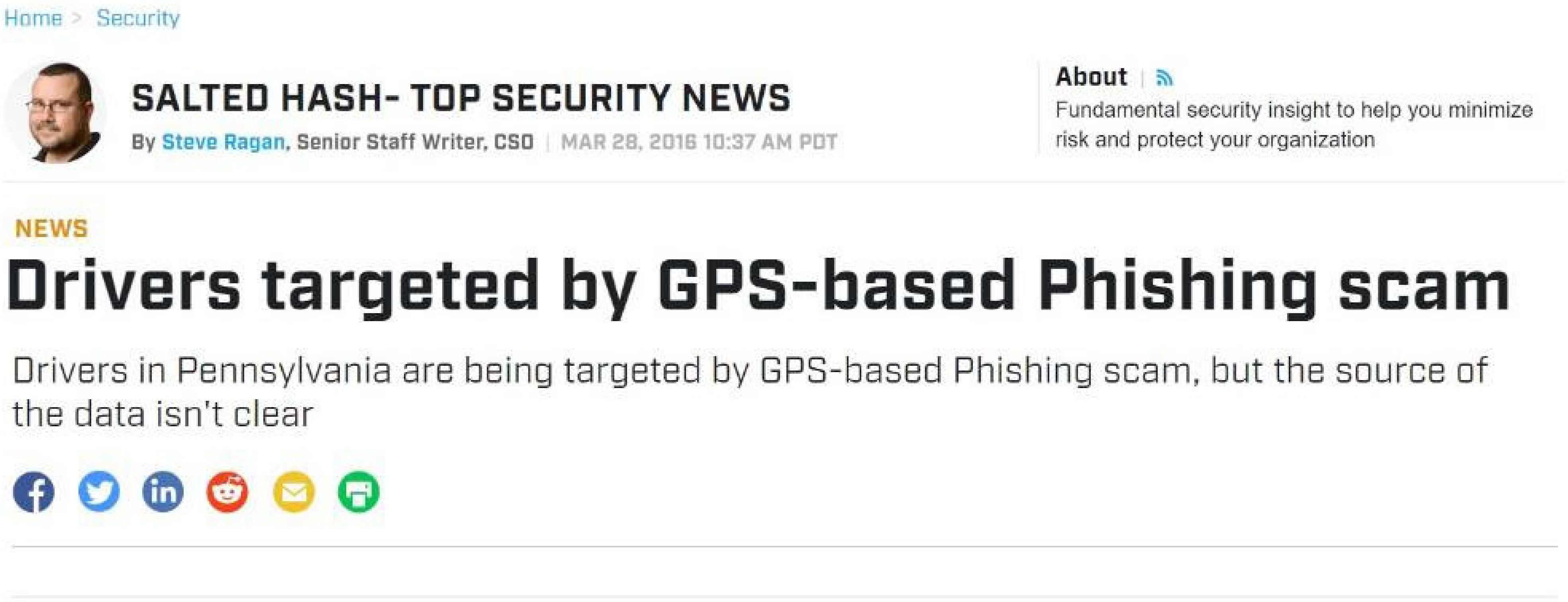
[UPDATE] See new information at the bottom of this posts.

A phishing scam posing as a speeding ticket email with a malicious link is nothing new. But here's an innovation that should give you pause.

Emails claiming to be from the local police department were sent to a few local residents close to Philadelphia and had something unique.

They contain *accurate* speeding data, including street names, speed limits, and actual driving speeds, according to the local Police Department,

CSO (“Salted Hash”) coverage [03/28/2016]



Home > Security

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO | MAR 28, 2016 10:37 AM PDT

About |

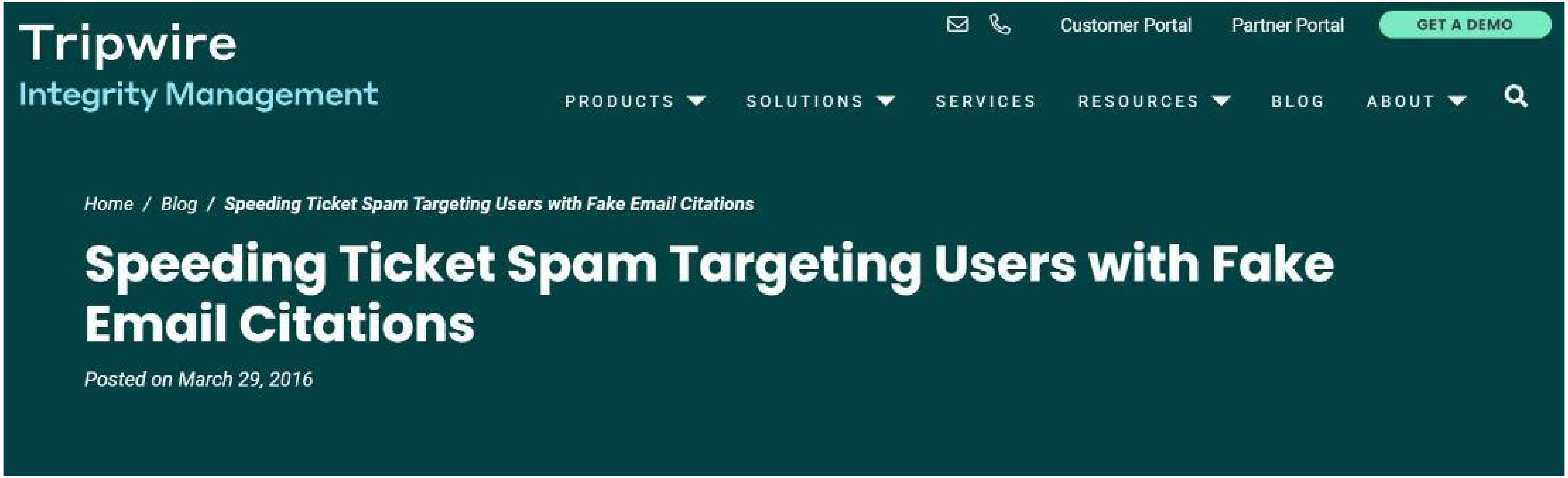
Fundamental security insight to help you minimize risk and protect your organization

NEWS

Drivers targeted by GPS-based Phishing scam

Drivers in Pennsylvania are being targeted by GPS-based Phishing scam, but the source of the data isn't clear

Tripwire article [03/29/2016]

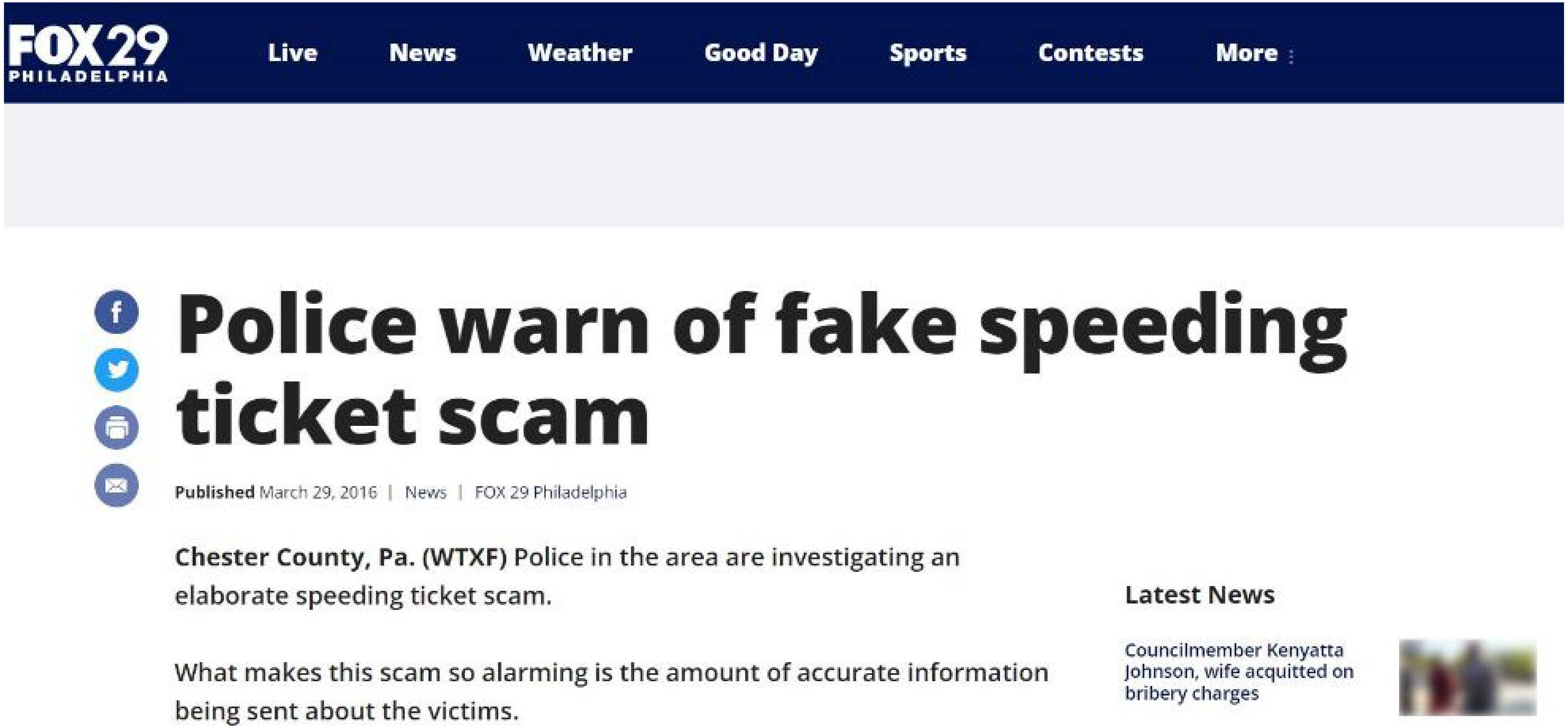


Home / Blog / **Speeding Ticket Spam Targeting Users with Fake Email Citations**

Speeding Ticket Spam Targeting Users with Fake Email Citations

Posted on March 29, 2016

TV coverage [3/29/2016]



Police warn of fake speeding ticket scam

Published March 29, 2016 | News | FOX 29 Philadelphia

Chester County, Pa. (WTXF) Police in the area are investigating an elaborate speeding ticket scam.

What makes this scam so alarming is the amount of accurate information being sent about the victims.

Latest News

Councilmember Kenyatta Johnson, wife acquitted on bribery charges

What if “non-clickers” at a USG agency reported externally to other USG agencies?

DOJ TSP-themed phishing exercise [2009]

The “email had circulated quickly to other agencies …” including:

- the National Oceanic and Atmospheric Administration (NOAA)
- the Economic Development Administration at the Commerce Department
- the Federal Aviation Administration (FAA)
- National Highway Traffic Safety Administration at the Transportation Department (NHTSA)
- the Government Accountability Office (GAO)
- the General Services Administration (GSA) alerted the TSP board to the e-mail”

DOJ “… modified our protocols to make sure that doesn't happen in the future.”

Army TSP-themed phishing exercise [2014]

Exercise recipients “… forwarded the e-mail to thousands of friends and colleagues at the:

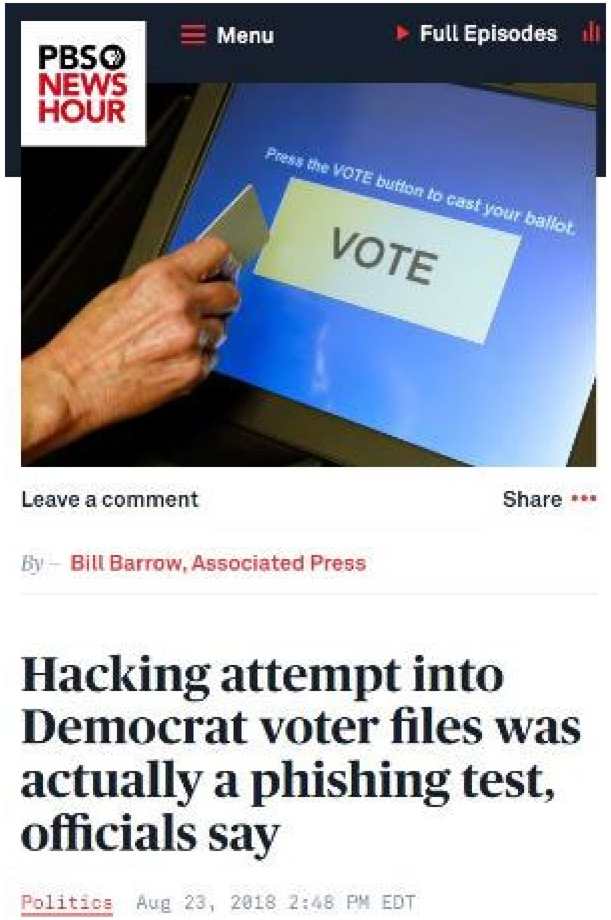
- Defense Department (DoD)
- the FBI
- Customs and Border Protection (CBP)
- the Labor Department (DoL) and other agencies.”

A Washington Post article highlighted:

“Defense officials say they will require more oversight of security tests that try to trip up employees”

What if “non-clickers” reported externally to federal law enforcement?

Phishing Exercise at the DNC [08/2018]



By – Bill Barrow, Associated Press

Hacking attempt into Democrat voter files was actually a phishing test, officials say

Politics Aug 23, 2018 2:48 PM EDT

“discovered after national party officials already had contacted federal law enforcement fearing a malicious hacking attempt”

“But cybersecurity protocols, Lord said, require that an entity conducting phishing tests notify other relevant parties so they don’t see red flags.”

Likelihood of external notifications

Number of employees	Click rate (10%)	“Non-clickers” (90%)	External notifications (1% of non-clickers)
10	1	9	N/A
100	10	90	**1**
1,000	100	900	9
10,000	1,000	9,000	90
100,000	10,000	90,000	900

Avoiding issues with phishing exercises

1. consider an alternative (e.g., tabletop exercises)
2. conduct agency-neutral/brand-neutral exercises unless you have the explicit permission of the agency/brand
3. have counsel and/or HR review potential exercise lures for potential issues before launching your campaign
4. provide “honest signals” or identifiers within the phishing exercise campaign (e.g., email headers, landing page, RFC 9116, etc.) [see Notes]

Green = “Go” (Likelihood of issues very low)

- The phishing exercise does not reference an agency and/or brand
- Controversial phishing exercise lures have been reviewed and approved by Legal and Human Resources (HR)
- “Honest Signals” are present throughout the phishing exercise construction and/or delivery

Yellow = “Proceed with Caution”

- Agency indirectly referenced (e.g., W2, 1099, etc.)
- Brand indirectly referenced
- Partial review of controversial phishing exercise lures by Legal and Human Resources (HR)
- Partial or no “Honest Signals” present throughout phishing exercise construction and/or delivery

Red = STOP!

- The phishing exercise references an agency or brand directly
- Controversial phishing exercise lures were not checked by Legal or Human Resources (HR)
- Few if any “Honest Signals” present throughout phishing exercise construction and/or delivery

Questions?

Thank you!

Closing Remarks

Menachem Goldstein

FISSEA Co-Chair
Cybersecurity Specialist, Enterprise Cybersecurity Department
Pension Benefit Guaranty Corporation

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2023
Email fissea@list.nist.gov

Submit a presentation proposal for a future FISSEA Forum
https://www.surveymonkey.com/r/fisseacallforpresentations

THANK YOU

We look forward to receiving your feedback via the post-event survey!

https://www.surveymonkey.com/r/2022fisseafallforum

#FISSEA2022 | nist.gov/fissea

FISSEA Winter Forum

February 14, 2023

1:00pm – 4:00pm EDT

REGISTER TODAY: nist.gov/fissea

SAVE THE DATE

Federal Information Security Educators (FISSEA) Conference

April 19, 2023

#FISSEA2022 | nist.gov/fissea

fissea

FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

NIST

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE