NIST CYBER

NIST National Institute of Standards and Technology U.S. Department of Commerce

fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

2020 Vision:

Bringing the Future of Cybersecurity Awareness and Training Into Focus

33rd Annual FISSEA Conference 2020 Summer Webinar Series

#FISSEA2020 | nist.gov/fissea

fissea
FEDERAL
2020

Summer Series

August 17, 2020

Adaptive Learning:

Utilizing AI and Social Collaboration for User-Centric Training Results

Federal Information Security Educators (FISSEA)

About FISSEA

FISSEA, founded in 1987, is an organization run by and for Federal government information security professionals to assist Federal agencies in strengthening their employee cybersecurity awareness and training programs.

Purpose

- Elevate the general level of information security knowledge for the federal government and federally-related workforce.
- Serve as a professional forum for the exchange of information and improvement of information systems security awareness and training programs throughout the federal government.
- Provide for the professional development of community members.

Organization

- FISSEA seeks to bring together information security professionals.
- Each year, an award is presented to a candidate selected as Awareness and Training Innovator of the Year, honoring distinguished accomplishments in information security training programs.

The Learning Continuum

Awareness

- Campaigns: Cybersecurity Awareness Month; Stop.Think.Connect
- Building a Security Awareness and Training Program (NIST SP 800-50)
- Federal Information Security Educators (FISSEA)

Training

- Learning Experiences and Credentials (e.g., Certification, Certificate, Badge, etc.)
- Role-Based Training (NIST SP 800-16)
- FISSEA and National Initiative for Cybersecurity Education (NICE)

Education

- K12: Elementary, Middle, and High School
- Higher Education: Community Colleges, Colleges and Universities, and Professional Schools
- NICE – Education and Workforce

Engagement Opportunities

Awareness and Training ~ FISSEA (federal environments)

- FISSEA Community of Interest
- FISSEA Summer Series
- Annual FISSEA Conference and Exhibitor Showcase

Training and Education ~ NICE (education and workforce for the nation)

- Federal Cybersecurity Workforce Summit & Webinar Series
- Annual NICE Conference and Expo
- NICE K12 Cybersecurity Education Conference
- NICE Webinar Series

JOIN US FOR THE NEXT WEBINAR

Storytelling in Cybersecurity: Your Ace in the Hole
September 21, 2020 1:00PM-2:30PM

We know that storytelling is one of the most effective strategies to engage people. We are accustomed to using storytelling, experiential learning, and competitions in training and education because they engage the emotion system of the brain (hippocampus) – and produce excitement, anxiety, confidence, joy – which transfers information into memory, and information into action. Join #FISSEA2020 and Sarah Moffat for a workshop on storytelling in business, specifically, cybersecurity. During this 70-minute session (plus time for the big FISSEA Innovator of the Year award!) you'll get a chance to practice your storytelling skills while getting tips from Sarah Moffat, a graduate from the TED® Masterclass. Sarah's TED Talk, "How to Develop a Round Table as Legendary as King Arthurs" was delivered on the TED® HQ stage in NYC and is now in the TED Masterclass app! Sarah's going to share what she's learned from working in cybersecurity education, training, and awareness for 15 years, plus her TED training, and help us all tap our creative side to communicate important cybersecurity concepts to a variety of audiences -- from teaching children in kindergarten to enlisting the support of the non-technical C-suite.

Featuring: Presentation of the Annual Innovator of the Year Award

REGISTER
https://csrc.nist.gov/Projects/fissea/2020-summer-series

NIST CYBER

Next Webinar
September 21, 2020| 1pm– 2:30pm EST
"Storytelling in Cybersecurity: Your Ace in the Hole"

fissea FEDERAL

Save the date
34th Annual FISSEA Conference
June 16-17, 2021 | NIST Gaithersburg, MD

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Save the Date

FISSEA 2021

June 16-17, 2021
NIST Campus
Gaithersburg, Maryland

Presenters

Tapio Kymäläinen *President, Howspace*

Digital facilitation evangelist. Tapio is a seasoned expert in mixing the soup of learning, change and digital tools. Sometimes enough to feed 10 people and other times enough for 30,000 people, but always spiced with passion, creativity and love for learning.

Joe Barrow, *Enterprise Solutions Architect, Area9*

Joe is an Enterprise Solutions Architect at Area9 Lyceum - bringing employee, channel, and customer learning into the 21st century to drive productivity and performance through learning science, computer science and neuroscience.

Brian Simms *Director of Learning, Learning Tree International*

As Director of Digital Content and Learning Services, Brian is leading Learning Tree's effort to modernize blended learning and create an ecosystem of learning that empowers careers and supports organizations.

WHAT IFs?

Questions we will answer:

- What if your workforce had instant digital **access to the expert help they needed while they were working**?
- What if your workforce had an eLearning experience that **tailored itself to what each learner needed, right when they needed it?**
- What if instructor time could then be **focused on exactly what each student needs the most practice with?**

Problem:

One-on-one tutoring is the learning gold standard. But how is that possible today?

Learning Innovation In a Blended Model:

- **Over 100 organizations** in need of ITIL Foundation training amid COVID-19 Pandemic
- Average time to content mastery: **6.5 hours**
- Annual one-click access for **continued project support and implementation** needs
- Custom, targeted **virtual sessions weekly** for those who need it

CASE STUDY:
ITIL® 4 Foundation

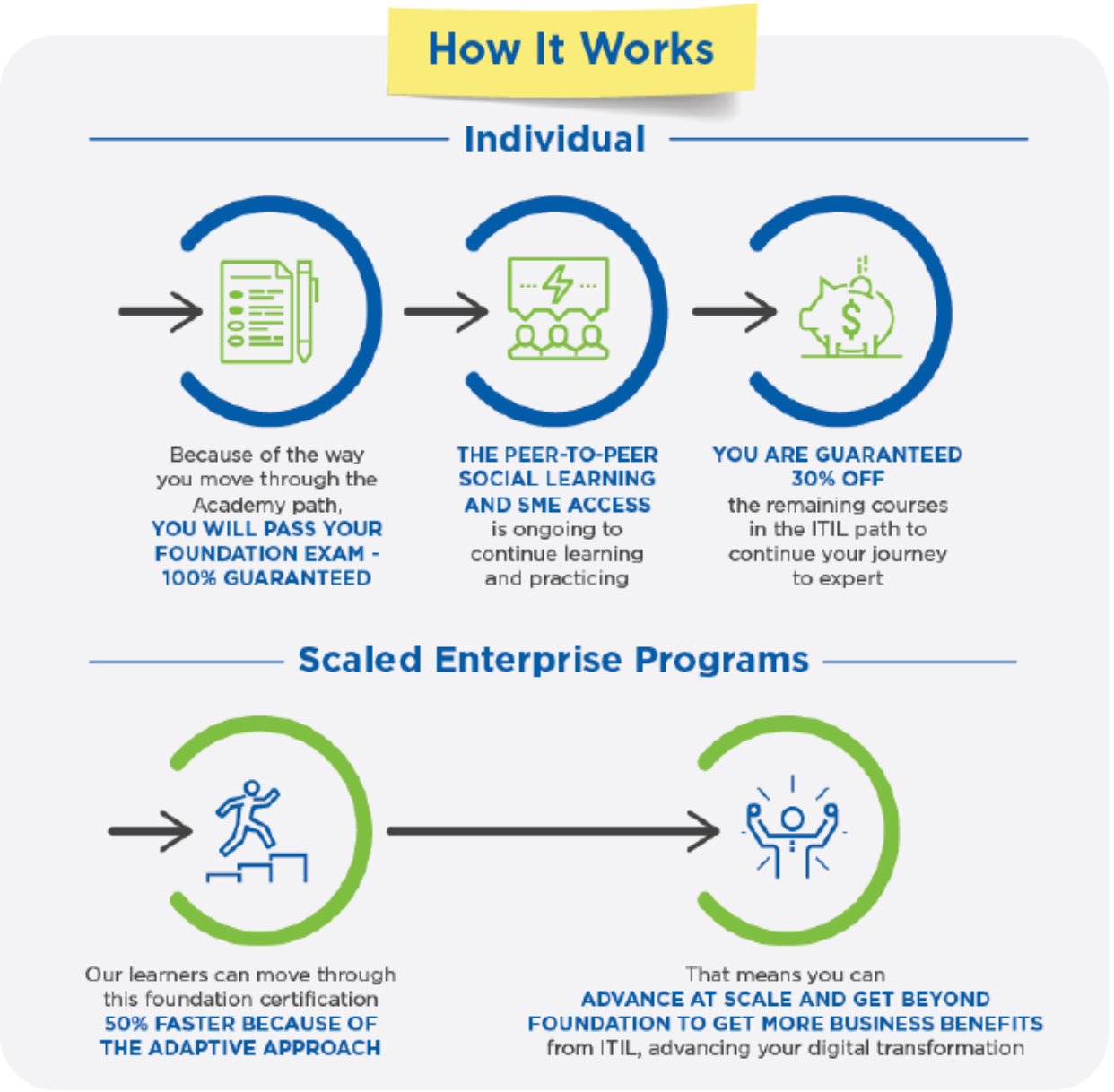
A personalized, blended learning environment that provides each learner all the resources needed to pass the ITIL 4 Foundation exam and get them practicing ITIL in meaningful ways **suited to their specific needs**

The Virtual Academy includes annual access to:

- Online collaboration space
- Accredited adaptive online course
- Official digital book, official mobile app, and exam voucher
- Individual/group virtual workshops, as needed
- Options for discounted VILT/ILT events, as needed

Insights from the moderator of the academy:

"With insight into where learners are struggling – (even when they can do so completely at their own pace) and visibility into the nature of their problems and the application of their solutions, we can make best use of our in-person learning time."



NIST CYBER

NIST National Institute of Standards and Technology U.S. Department of Commerce

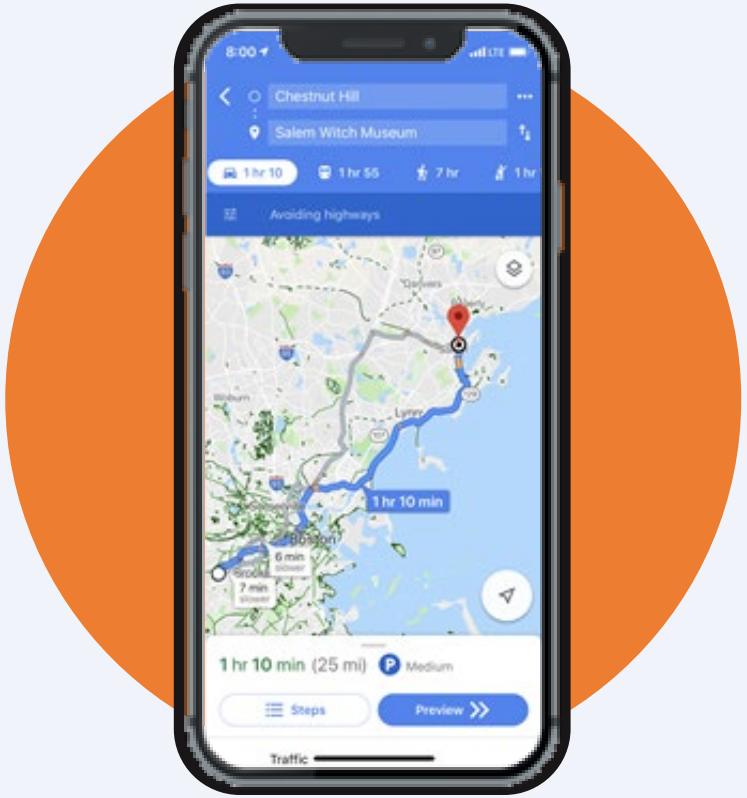
fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Adaptive Learning

Work Smarter Not Harder

Traditional e-Learning

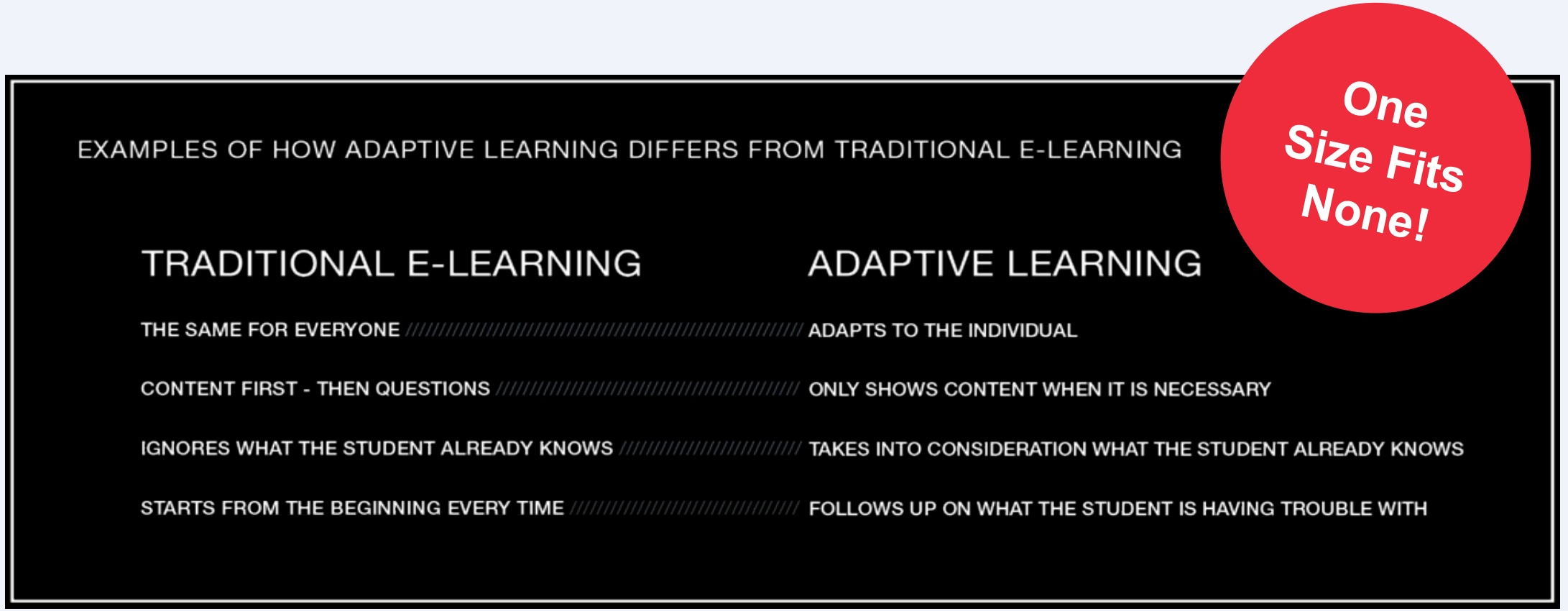


Adaptive Learning

What Is Adaptive Learning?

- An online delivery method that automatically adjusts to the needs of each learner.
- Recreates at scale the optimal teaching approach of a one-on-one personal tutor.
- Uses proven data analytics and intelligent technologies to adjust in real-time to deliver an optimal experience.

How It Differs



Why Is This Different?

+20 Years Of Research
In Human Factors, Learning Science And Computer Science

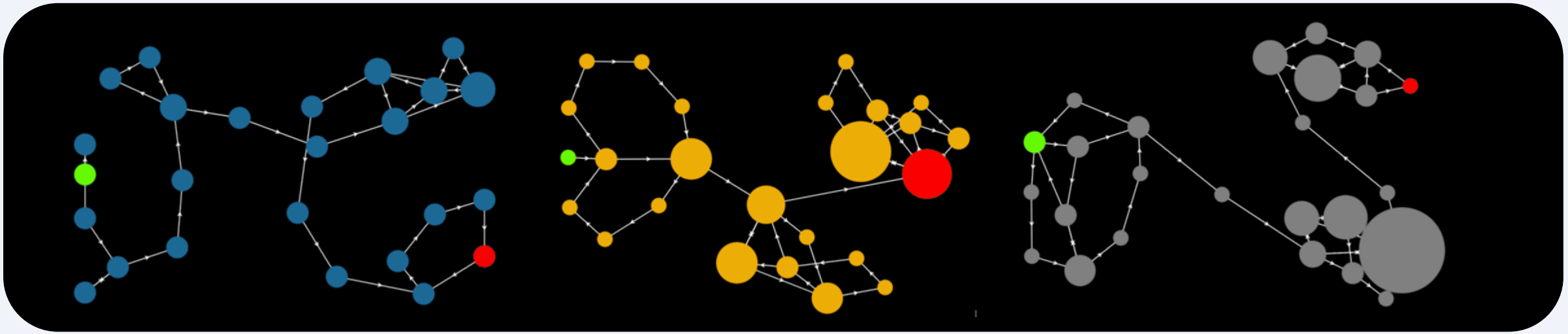
Powered Learning Of
Over 30Million Students In Over 2,000 Products - Exit In 2014 & Area9 Lyceum Re-launched In 2018 With $32M Investment

Collected
Billions Of Learning Data-Points

and most importantly…

The Expertise In What Really Impacts Learning

Unique Paths To Proficiency



	Learner 1	Learner 2	LEARNER 3
Final	100% proficient 8m 25s	100% proficient 19m 39s	100% proficient 33m 40s
Initial	88% correct 9% consciously incompetent 3% unconsciously incompetent	52% correct 7% consciously incompetent 41% unconsciously incompetent	47% correct 29% consciously incompetent 24% unconsciously incompetent

Data from Feb 2019 from telecommunications company, technical training course

The Same, But Different

Outcomes: Learning Objective

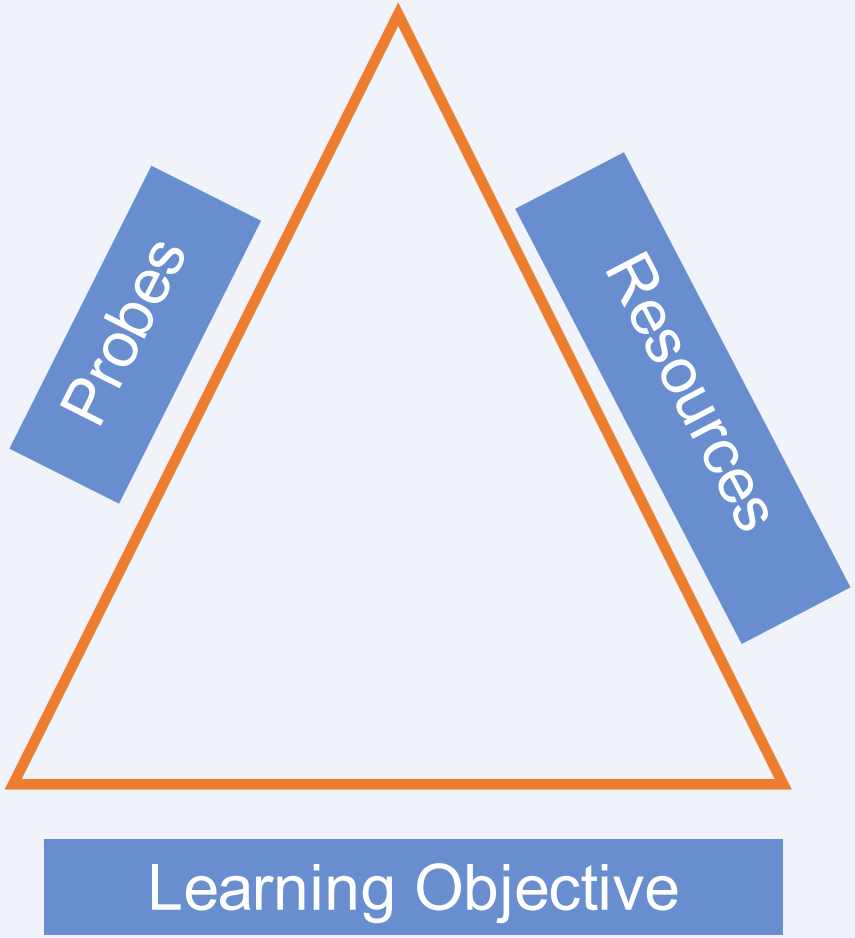
Statement that defines the expected outcome in terms of demonstrable skills or knowledge.

Content: Learning Resources

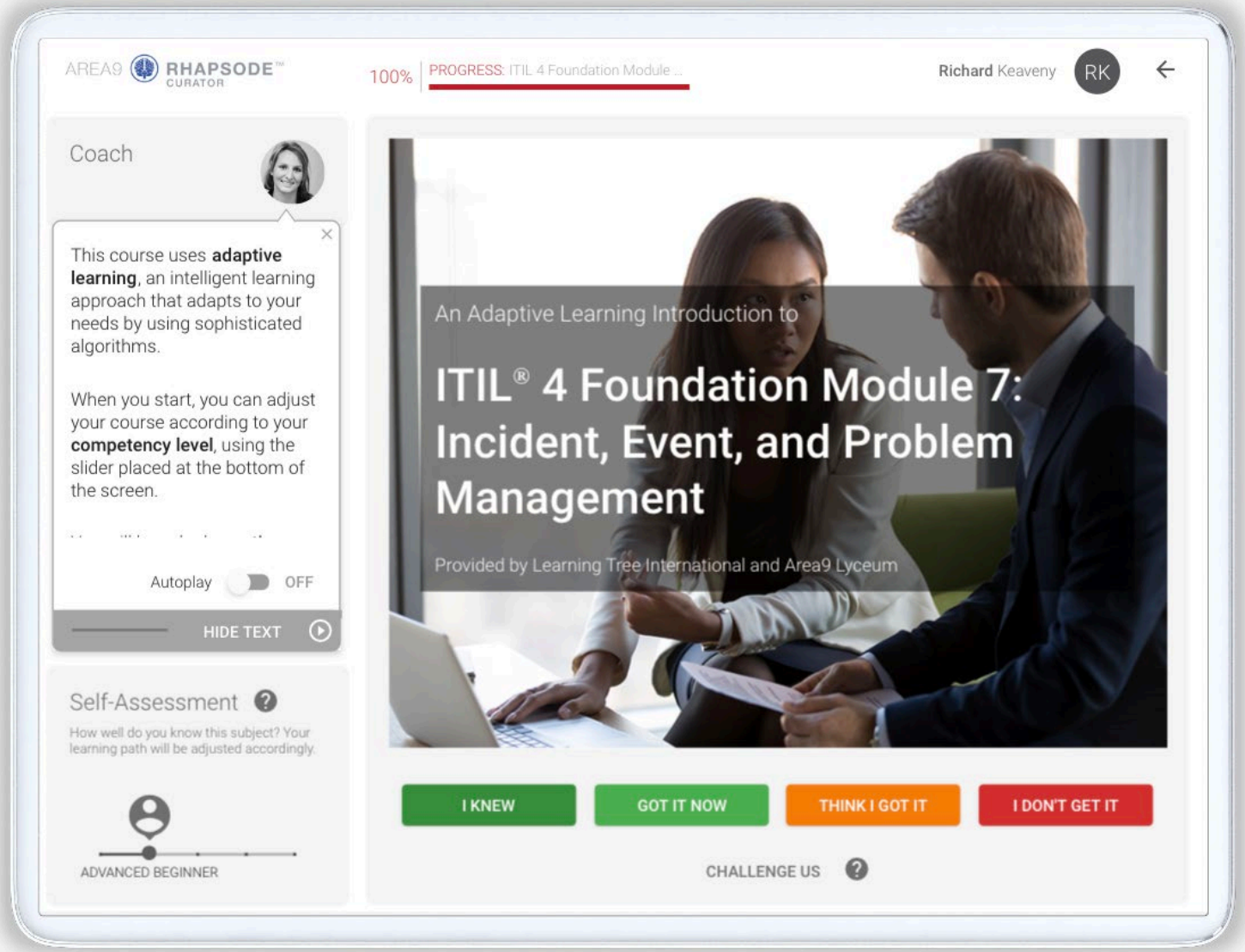
To help learn something new or hard.

Assessment: Probes

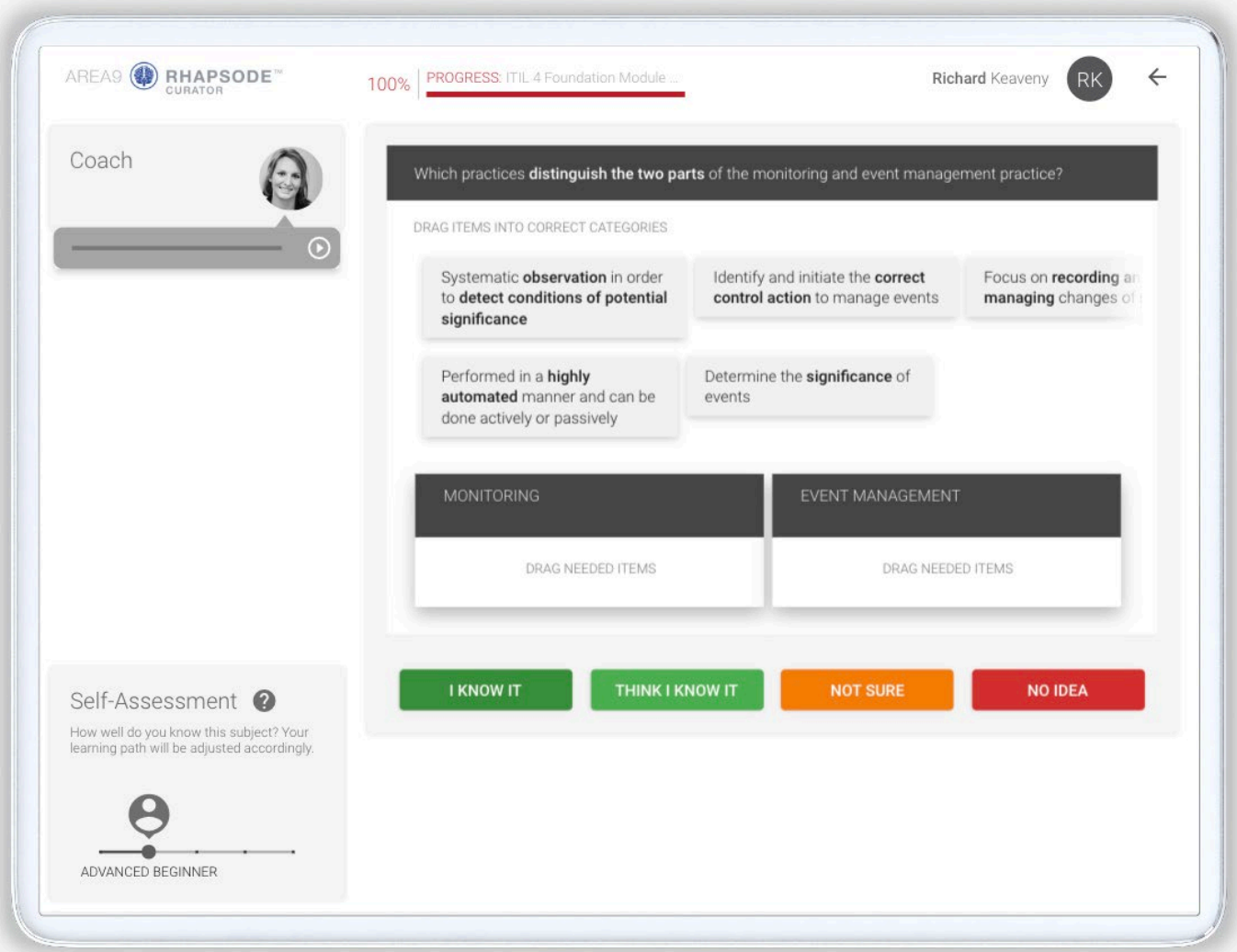
Questions, problems or exercises measure the student's level of proficiency as well as what type of Learning Resource is most helpful for each individual.



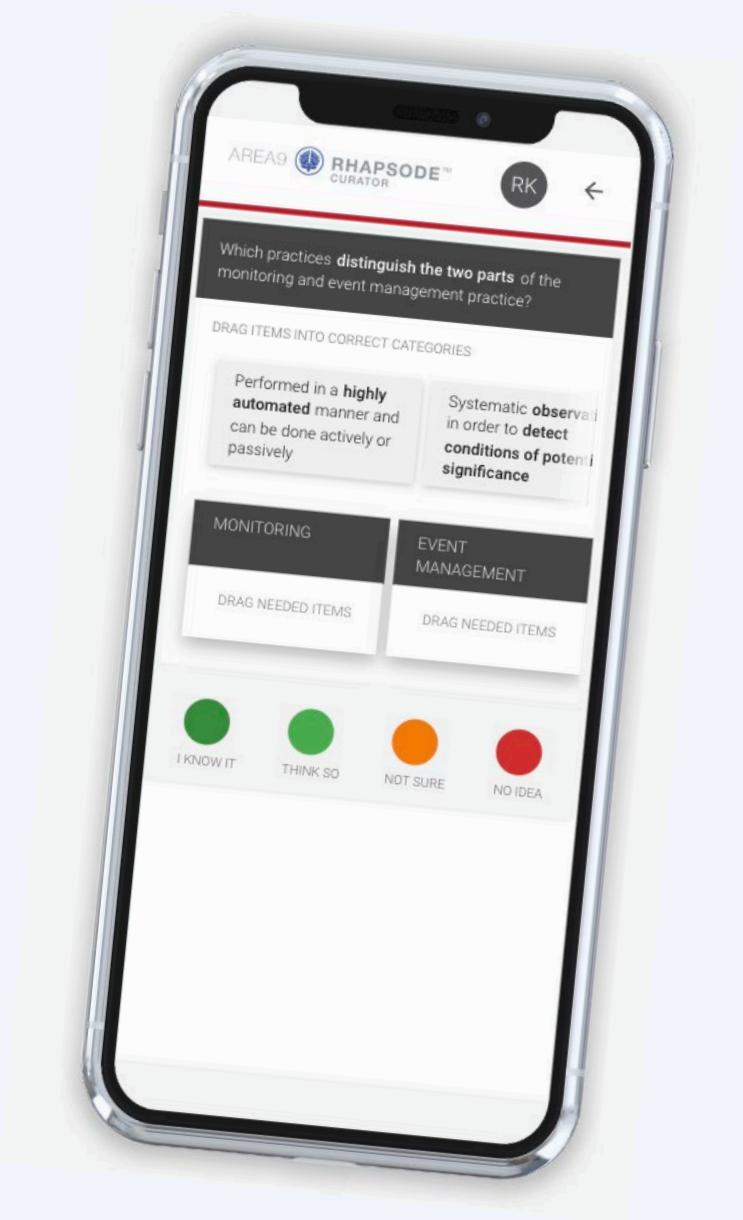
Learning Objectives



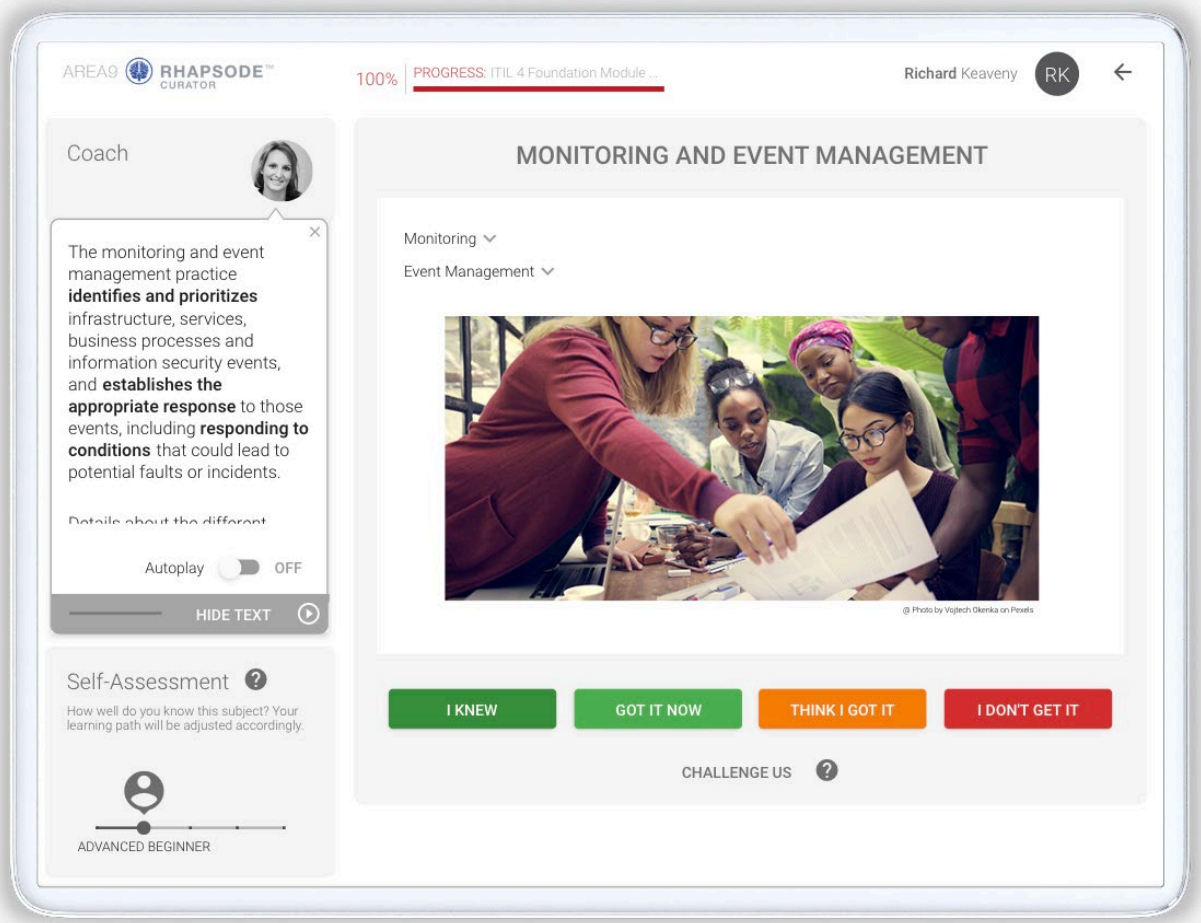
Probes


AREA9 RHAPSODE CURATOR
100% PROGRESS: ITIL 4 Foundation Module ...
Richard Keaveny RK
Coach
Which practices distinguish the two parts of the monitoring and event management practice?
DRAG ITEMS INTO CORRECT CATEGORIES
Systematic observation in order to detect conditions of potential significance
Identify and initiate the correct control action to manage events
Focus on recording ar managing changes of
Performed in a highly automated manner and can be done actively or passively
Determine the significance of events
MONITORING
EVENT MANAGEMENT
DRAG NEEDED ITEMS
DRAG NEEDED ITEMS
I KNOW IT
THINK I KNOW IT
NOT SURE
NO IDEA
Self-Assessment
How well do you know this subject? Your learning path will be adjusted accordingly.
ADVANCED BEGINNER

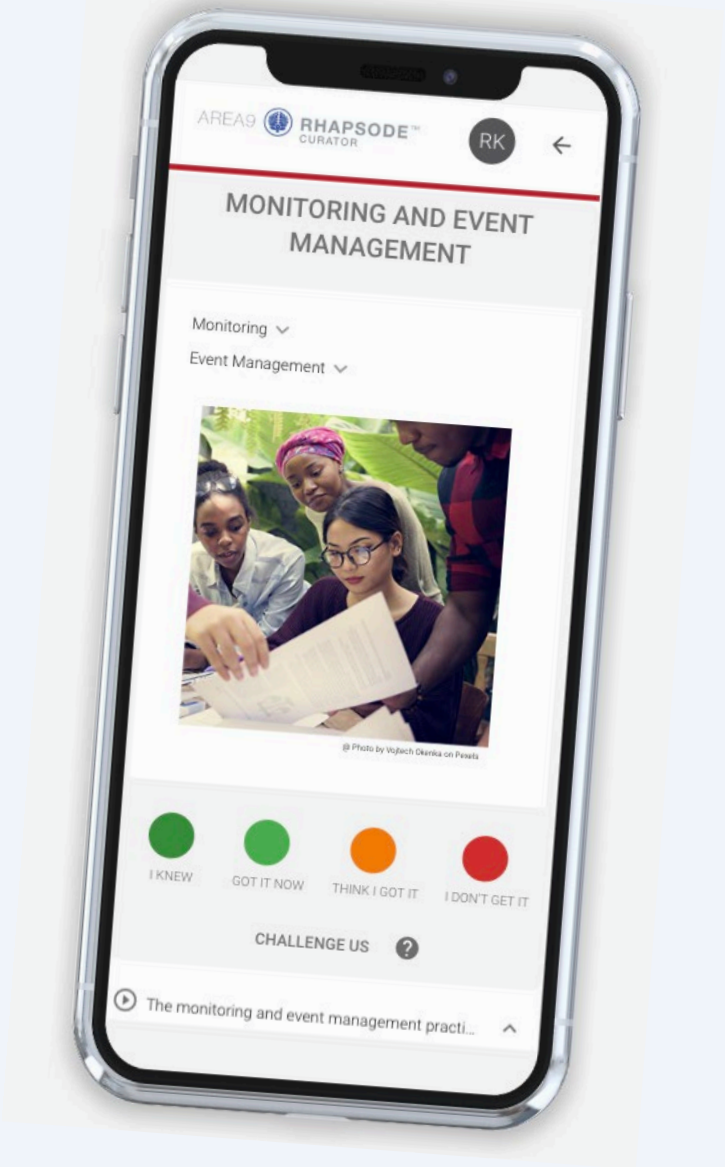
Probes


AREA9
RHAPSODE
CURATOR
RK
Which practices distinguish the two parts of the monitoring and event management practice?
DRAG ITEMS INTO CORRECT CATEGORIES
Performed in a highly automated manner and can be done actively or passively
Systematic observa
in order to detect
conditions of poten
significance
MONITORING
EVENT MANAGEMENT
DRAG NEEDED ITEMS
DRAG NEEDED ITEMS
I KNOW IT
THINK SO
NOT SURE
NO IDEA

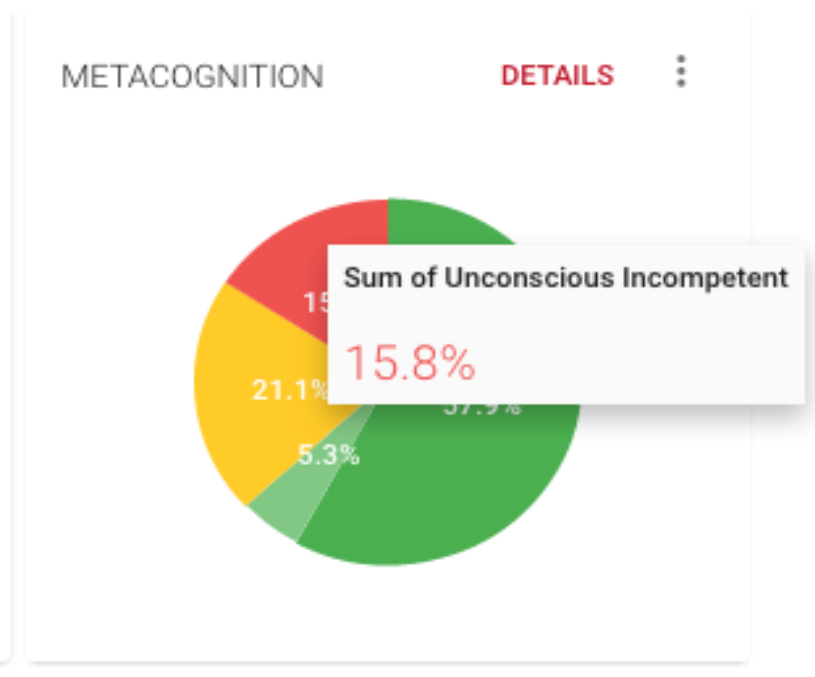
Learning Resources

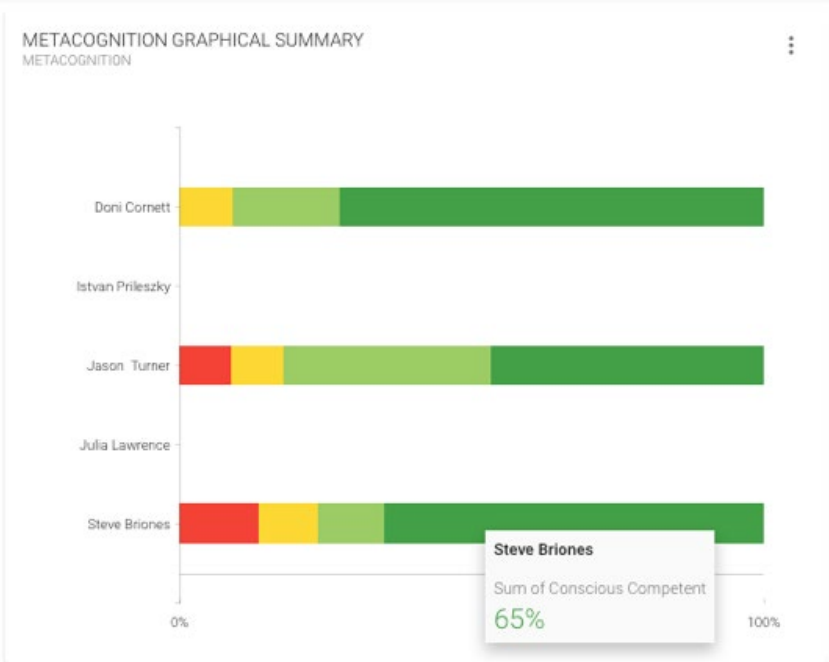


Learning Resources



Actionable Data



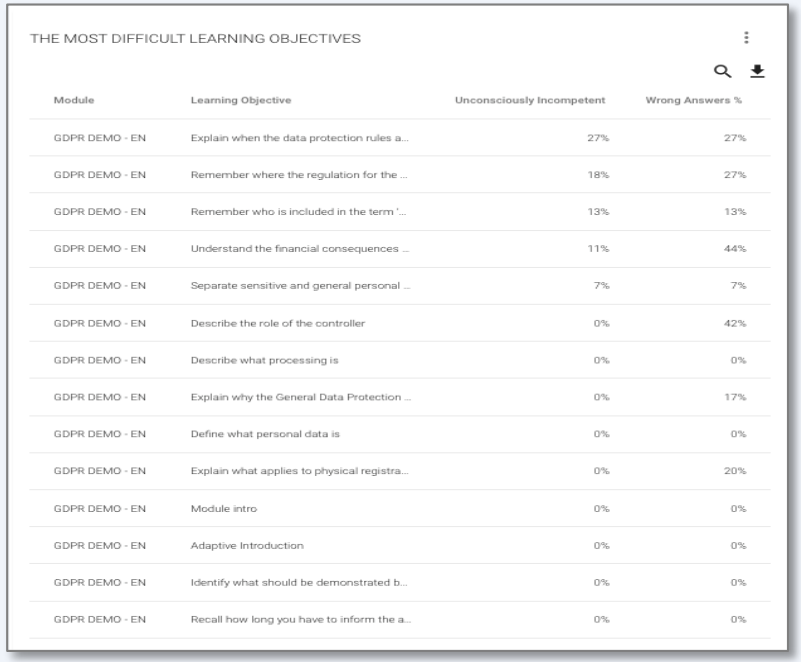


A Personalized Learning Experience that applies science and technology to improve learning

Each Person Learns Differently – one size training fits no one

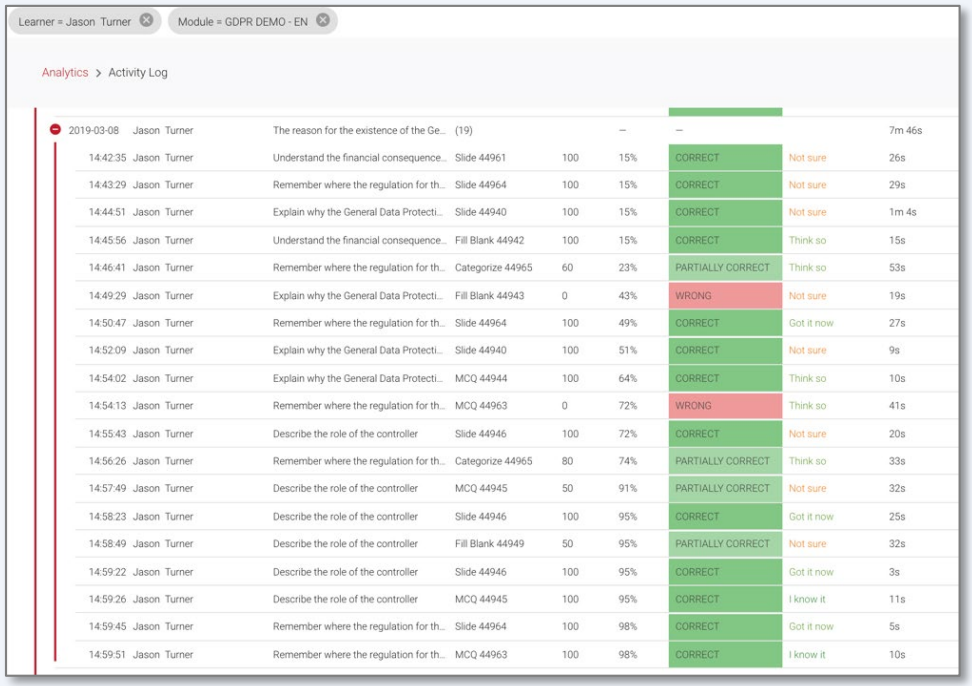
Get To Proficiency Faster

Actionable Data



THE MOST DIFFICULT LEARNING OBJECTIVES

Module	Learning Objective	Unconsciously Incompetent	Wrong Answers %
GDPR DEMO - EN	Explain when the data protection rules a...	27%	27%
GDPR DEMO - EN	Remember where the regulation for the ...	18%	27%
GDPR DEMO - EN	Remember who is included in the term '...	13%	13%
GDPR DEMO - EN	Understand the financial consequences ...	11%	44%
GDPR DEMO - EN	Separate sensitive and general personal ...	7%	7%
GDPR DEMO - EN	Describe the role of the controller	0%	42%
GDPR DEMO - EN	Describe what processing is	0%	0%
GDPR DEMO - EN	Explain why the General Data Protection ...	0%	17%
GDPR DEMO - EN	Define what personal data is	0%	0%
GDPR DEMO - EN	Explain what applies to physical registra...	0%	20%
GDPR DEMO - EN	Module intro	0%	0%
GDPR DEMO - EN	Adaptive Introduction	0%	0%
GDPR DEMO - EN	Identify what should be demonstrated b...	0%	0%
GDPR DEMO - EN	Recall how long you have to inform the a...	0%	0%



Learner = Jason Turner | Module = GDPR DEMO - EN

Analytics > Activity Log

2019-03-08	Jason Turner	The reason for the existence of the Ge...	(19)		–	–			7m 46s
14:42:35	Jason Turner	Understand the financial consequence...	Slide 44961	100	15%	CORRECT	Not sure		26s
14:43:29	Jason Turner	Remember where the regulation for th...	Slide 44964	100	15%	CORRECT	Not sure		29s
14:44:51	Jason Turner	Explain why the General Data Protecti...	Slide 44940	100	15%	CORRECT	Not sure		1m 4s
14:45:56	Jason Turner	Understand the financial consequence...	Fill Blank 44942	100	15%	CORRECT	Think so		15s
14:46:41	Jason Turner	Remember where the regulation for th...	Categorize 44965	60	23%	PARTIALLY CORRECT	Think so		53s
14:49:29	Jason Turner	Explain why the General Data Protecti...	Fill Blank 44943	0	43%	WRONG	Not sure		19s
14:50:47	Jason Turner	Remember where the regulation for th...	Slide 44964	100	49%	CORRECT	Got it now		27s
14:52:09	Jason Turner	Explain why the General Data Protecti...	Slide 44940	100	51%	CORRECT	Not sure		9s
14:54:02	Jason Turner	Explain why the General Data Protecti...	MCQ 44944	100	64%	CORRECT	Think so		10s
14:54:13	Jason Turner	Remember where the regulation for th...	MCQ 44963	0	72%	WRONG	Think so		41s
14:55:43	Jason Turner	Describe the role of the controller	Slide 44946	100	72%	CORRECT	Not sure		20s
14:56:26	Jason Turner	Remember where the regulation for th...	Categorize 44965	80	74%	PARTIALLY CORRECT	Think so		33s
14:57:49	Jason Turner	Describe the role of the controller	MCQ 44945	50	91%	PARTIALLY CORRECT	Not sure		32s
14:58:23	Jason Turner	Describe the role of the controller	Slide 44946	100	95%	CORRECT	Got it now		25s
14:58:49	Jason Turner	Describe the role of the controller	Fill Blank 44949	50	95%	PARTIALLY CORRECT	Not sure		32s
14:59:22	Jason Turner	Describe the role of the controller	Slide 44946	100	95%	CORRECT	Got it now		3s
14:59:26	Jason Turner	Describe the role of the controller	MCQ 44945	100	95%	CORRECT	I know it		11s
14:59:45	Jason Turner	Remember where the regulation for th...	Slide 44964	100	98%	CORRECT	Got it now		5s
14:59:51	Jason Turner	Remember where the regulation for th...	MCQ 44963	100	98%	CORRECT	I know it		10s

A Personalized Learning Experience that applies science and technology to improve learning

Each Person Learns Differently – one size training fits no one

Get To Proficiency Faster

NIST CYBER

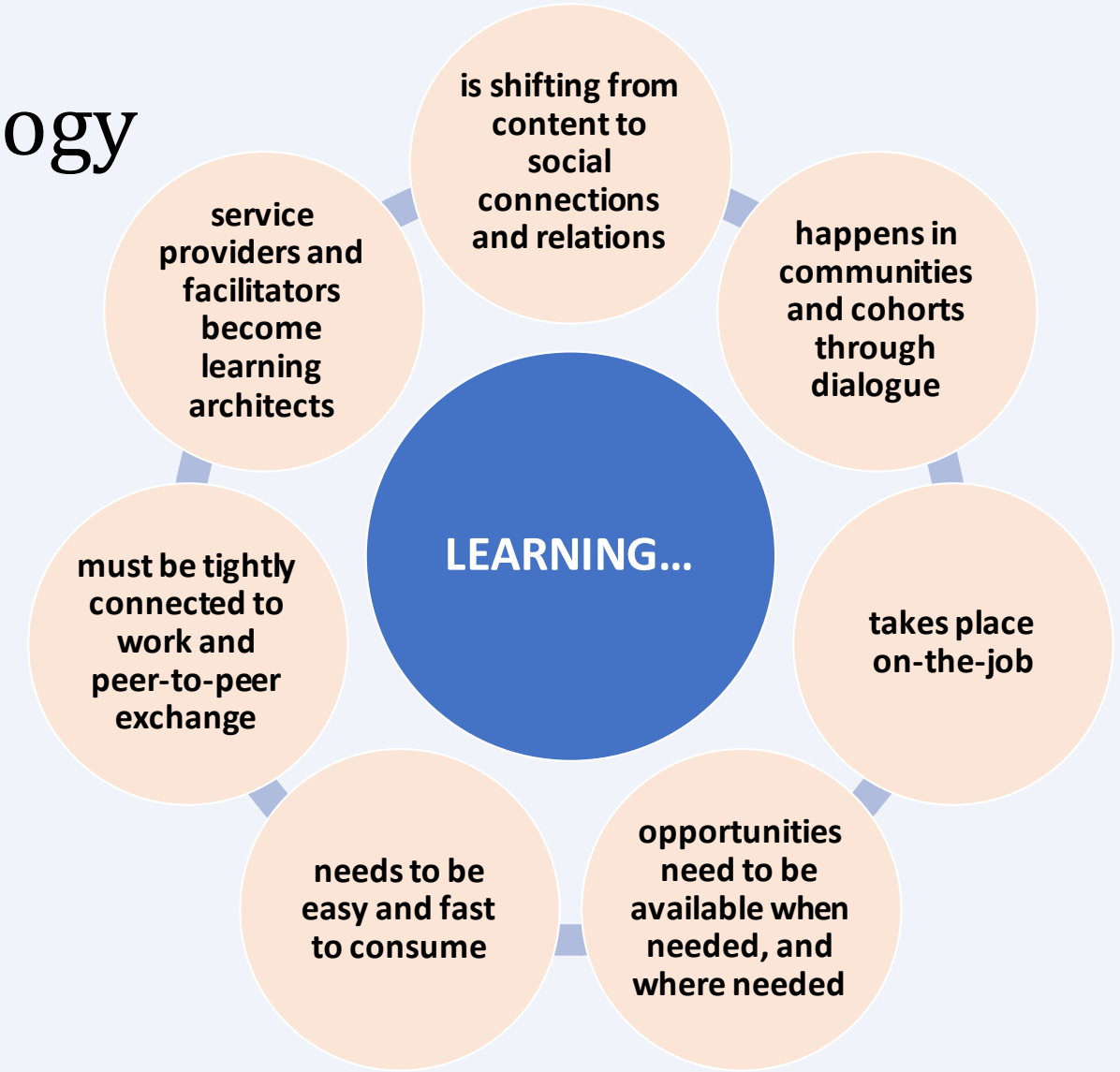
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

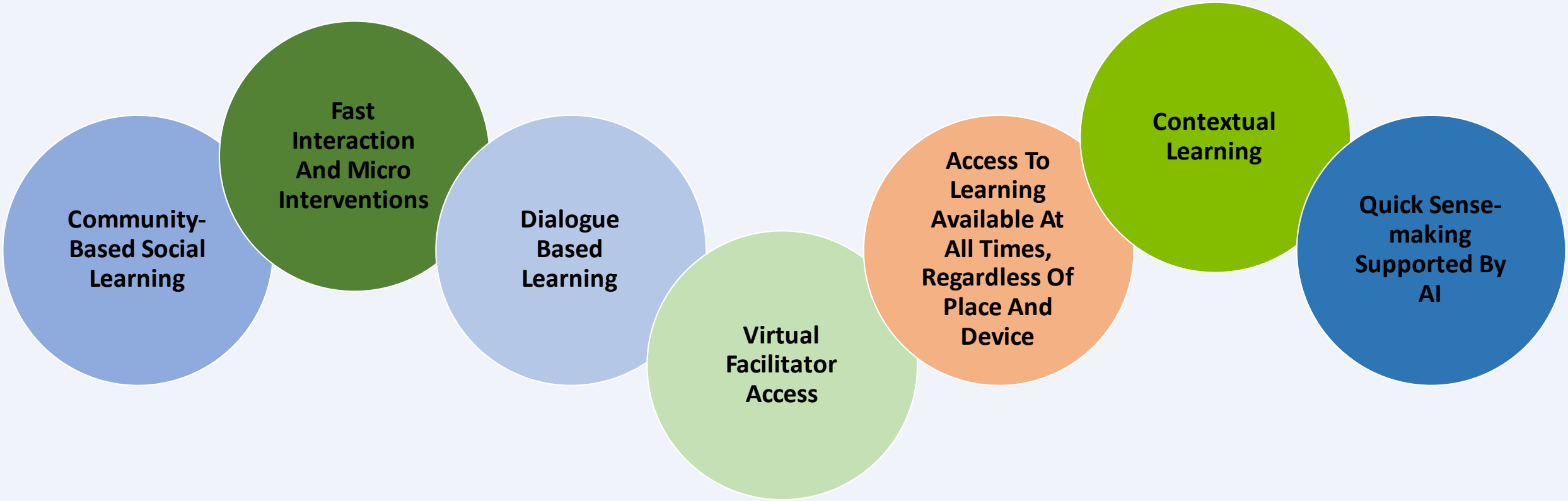
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Social Collaboration

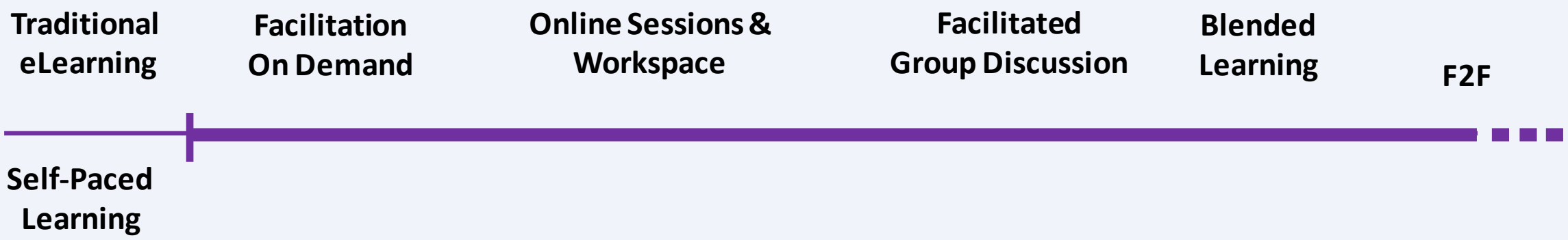
Learning Ideology



Response To Learning Trends



Learning Focus



Howspace supports facilitated learning processes and enhances learner to learner exchange. Facilitated dialogue and contextual learning. Supported by AI, also available to learners.

70-20-10 Learning

Howspace Learning

Traditional Learning

70 On-the-job Learning Through Experiences And Reflections, Dialogue

20 Mutual Learning – Peer Learning – Collaboration And Dialogue

10 Formal Learning, Content Focus, Courseware

True 70-20-10 blended learning experience resulting in enhanced learning experience, improved dialogue, learner engagement and sustained learning impact.

How Does it Work?

The three key elements for sustained learning impact

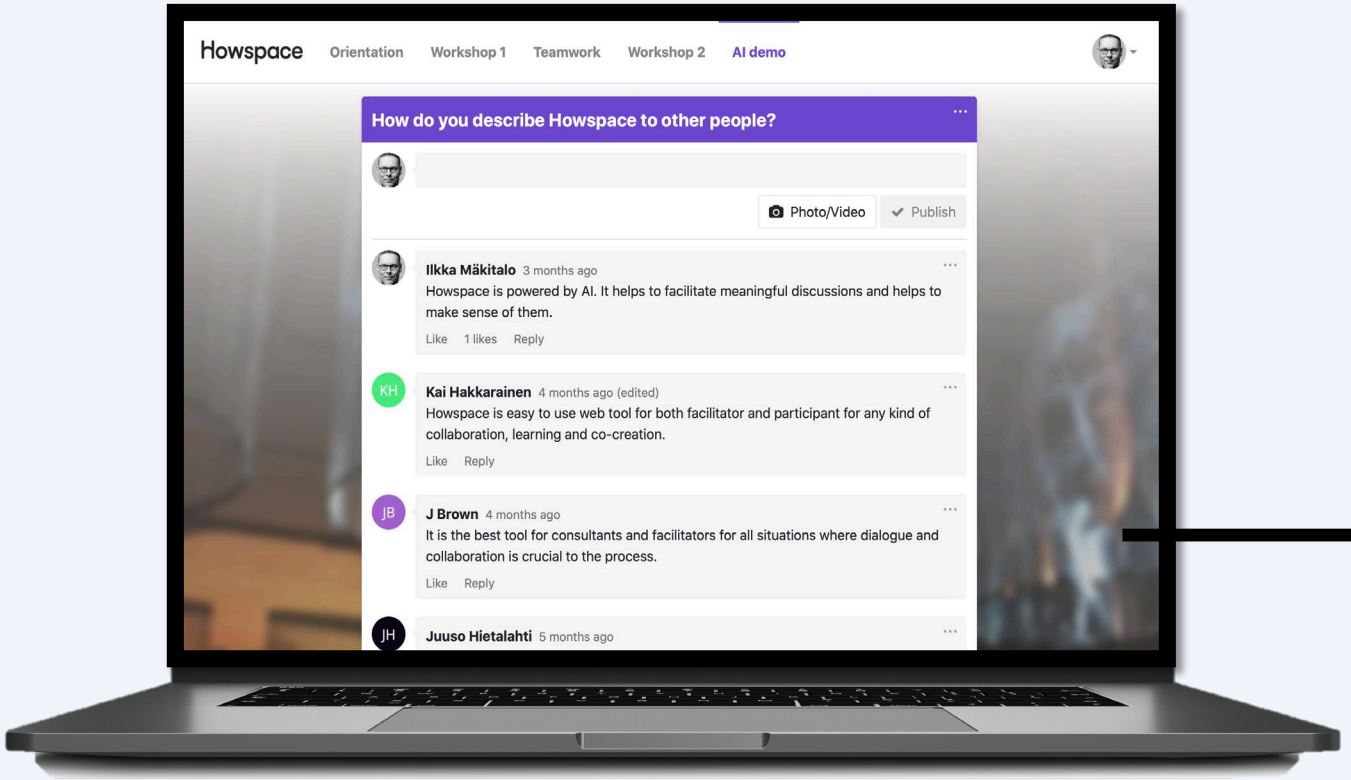
1. Easy and secure, **one-click access** to the online collaboration space anywhere on any device.

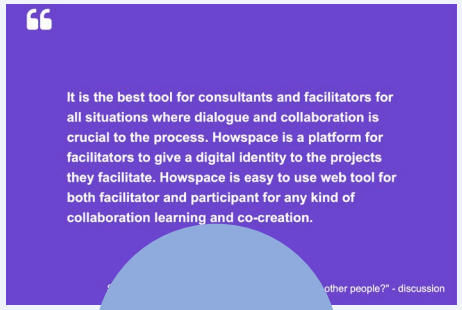
2. State-of-the-art **facilitation features** for effective social learning. Focus on the relevant context, social media like interaction, team and individual exchange, real- time learning.

3. **Artificial intelligence for sense making,** based on facilitated dialogue: Interactive word-cloud, analytical summaries and relevant theme clusters.

WORKSPACE = Dedicated digital environment for a given context, learning process and audience
PAGE = Stages of the learning process within a Workspace
CONTENT CONTAINER = Structural elements for building pages/templates within a Workspace
WIDGET = Working method e.g. chat, image, video, exam, file share, assignment, checkpoint, transition pulse, content embed etc.

Discussion Aid



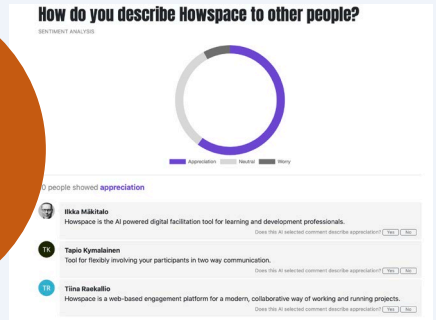


Summary

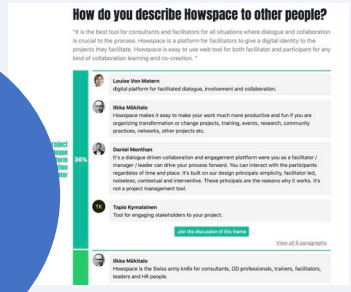
AI

AI Word Cloud *(Interactive)*

Sentiment Analyses



Theme Clustering



WHAT IFs?

Questions we will answer:

- What if your workforce had instant digital **access to the expert help they needed while they were working**?
- What if your workforce had an eLearning experience that **tailored itself to what each learner needed, right when they needed it?**
- What if instructor time could then be **focused on exactly what each student needs the most practice with?**

Answer:

We have to blend.

NIST CYBER

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

FISSEA

Security Awareness, Training, and Education

Contest

Gretchen Morris, CISSP
FISSEA Working Group Member
August 2020

Contest

Categories

- Blog*
- Motivational Item
- Newsletter
- Podcast*
- Poster
- Training
- Video
- Website

Judges

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

* New this year!

*Blog Entries (3)**

Entry 1:

Invoice Themed Phishing Emails Are Spreading from Trusted Links

Cofense • Internet Security Awareness,Microsoft 365 EOP,Phishing,Proofpoint,SEG Misses | July 16, 2020

Phishes Found in Environments Protected by SEGs

Proofpoint
Microsoft 365 EOP

By: Kian Mahdavi, Cofense Phishing Defense Center

The Cofense Phishing Defense Center (PDC) is seeing continued growth in phishing attacks which harvests users' credentials via genuine file-sharing websites, which are found in environments protected by Proofpoint's Secure Email Gateway (SEG). A huge factor in this campaign is the confidence users have in emails containing the "trusted" Dropbox reference.

It is tricky for SEGs to keep up with attempts to spread phishing attacks and malware via sharing services such as Dropbox, ShareFile, WeTransfer, Google Docs, Egnyte and even SharePoint. Fortunately, a few of our clients' users reported the phishing emails via the Cofense Reporter button.

The "traditional" methodology for attackers was to "break in." Nowadays, they easily can "login," thanks to sharing sites.

Entry 2:

U.S. Department of Health & Human Services

NIH National Institutes of Health
Office of Extramural Research

Extramural *Nexus*

Home | Open Mike | Archive | Subscribe | Contact

Open Mike

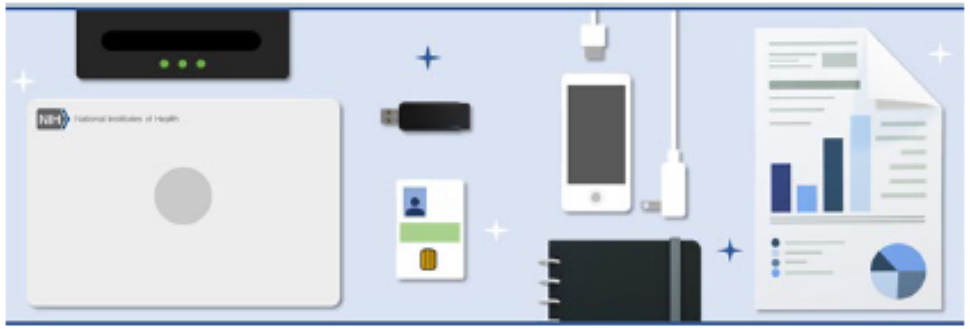
Helping connect you with the NIH perspective, and helping connect us with yours

Dr. Michael Lauer is NIH's Deputy Director for Extramural Research, serving as the principal scientific leader and advisor to the NIH Director on the NIH extramural research program.

Cyber Safety & COVID-19

Posted on April 17, 2020 by NIH Cyber Safety Campaign Team

The current outbreak of the novel coronavirus (COVID-19) has introduced new cybersecurity risks both at NIH and across the globe. As targeted phishing attacks prey on our desire to access trustworthy information and many of us make a shift toward remote work, we all need to be vigilant and take accountability for cyber safety.



Be Vigilant – Protect Against Phishing Attacks

Phishing attacks related to COVID-19 are on the rise. Over the past few weeks, several federal agencies and international organizations, including the World Health Organization, have issued cybersecurity alerts about criminal groups who are exploiting the pandemic for their own gain. INTERPOL also issued a targeted warning to hospitals and healthcare

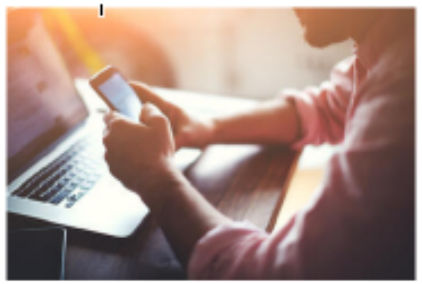
Entry 3:

Blog Post Example:

3
Jul

Half of all Remote Employees Aren't the Slightest Bit Prepared for Cyberattacks

Stu Sjouwerman



New data from IBM suggests that employees, their devices, training, and organizational policies are all lacking when it comes making sure remote workers don't become a victim of cybercrime.

We're well-past the shock of needing to setup remote operations with employees working from home. And enough time has passed that the world has seen how cybercriminals have changes their targets and tactics to take advantage of the unsuspecting remote worker.

So, surely, one would expect to see organizations taking steps to ensure the security of the employee, and the organization itself, right?

Well, according to IBM Security's newly-released Work from Home Study, cyber readiness in the remote workplace is still a mess:

- 53% of remote employees "have yet to be given any new security policies on how to securely work from home"
- Of the over half of remote employees using their personal device for work, 61% say their employer hasn't taken steps to help secure it
- 66% haven't been given any password management guidelines
- 45% haven't been given any new security training

The shift to working from home is not just about making employees operational; it's also about extending at least the same security policies and governance to the remote worker, while shoring up security upon realizing the increased risk of them working from home.

With so many security issues to address – from insecure WiFi, to personal devices, to home distractions, to a lack of guidance, *where should organizations pick up the pieces today?*

Given so many variables of how a given employee may be connecting to organizational resources, the answer lies in the one constant – the employee themselves. By enrolling employees in Security Awareness Training, the organization preps up the best possible defense against the ever-changing state of cyberattack. Employees can be taught to be mindful of corporate data, the use of phishing and social engineering, and how to spot suspicious email and web content.

Remote workers still have a lot of adjustment on their plate and it seems like every week, there's something new to deal with. By providing a source of stability through training, organizations can immediately see an improvement in their remote security stance, providing time to address the other factors.

For 2020 we hereby award:

COFENSE

the honor of being selected as the

Security Blog Contest Winner!

Invoice Themed Phishing Emails Are Spreading from Trusted Links

Cofense • Internet Security Awareness,Microsoft 365 EOP,Phishing,Proofpoint,SEG Misses | July 16, 2020

Phishes Found in Environments Protected by SEGs

Proofpoint
Microsoft 365 EOP

By: Kian Mahdavi, Cofense Phishing Defense Center

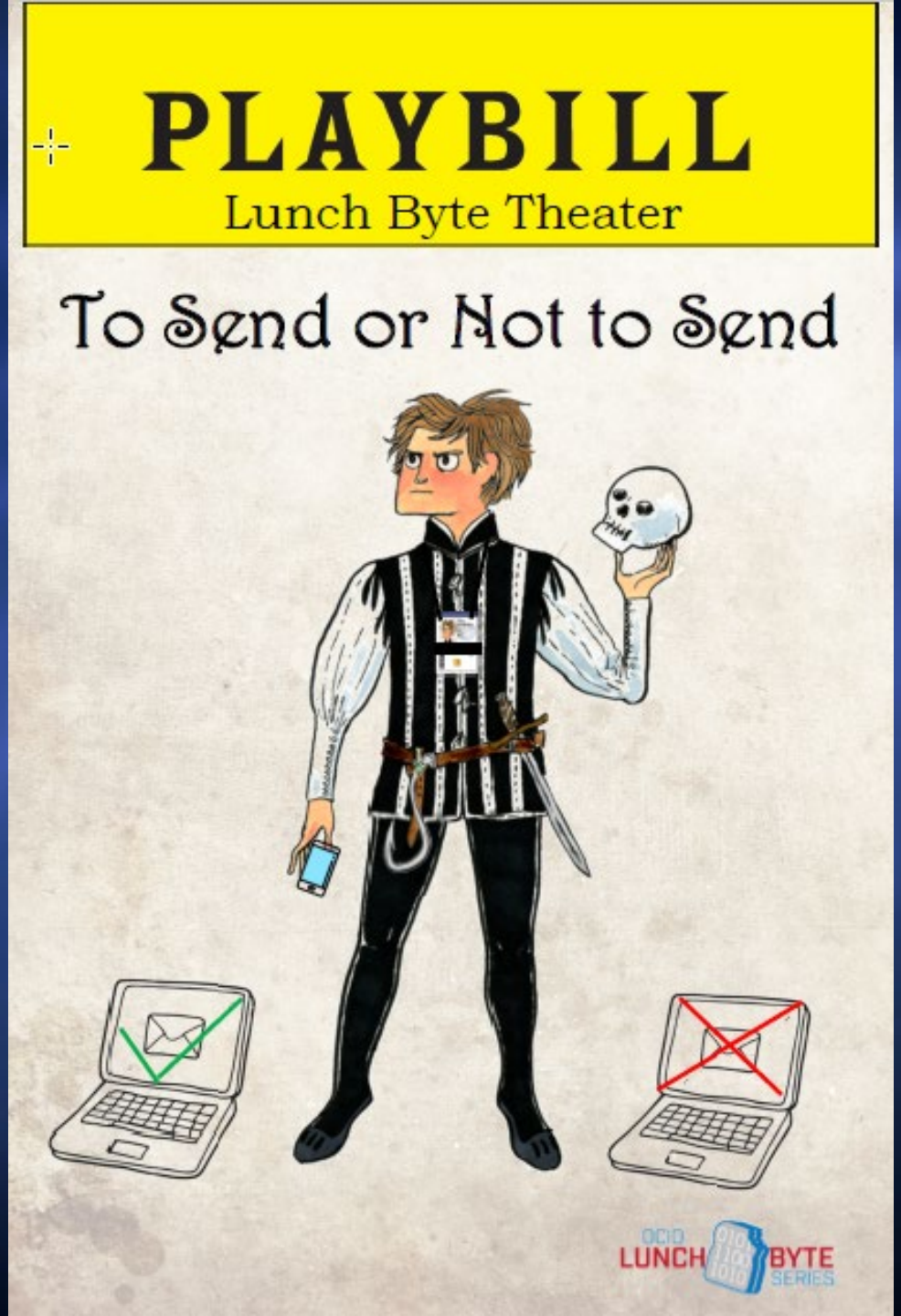
The Cofense Phishing Defense Center (PDC) is seeing continued growth in phishing attacks which harvests users' credentials via genuine file-sharing websites, which are found in environments protected by Proofpoint's Secure Email Gateway (SEG). A huge factor in this campaign is the confidence users have in emails containing the "trusted" Dropbox reference.

It is tricky for SEGs to keep up with attempts to spread phishing attacks and malware via sharing services such as Dropbox, ShareFile, WeTransfer, Google Docs, Egnyte and even SharePoint. Fortunately, a few of our clients' users reported the phishing emails via the Cofense Reporter button.

The "traditional" methodology for attackers was to "break in." Nowadays, they easily can "login," thanks to sharing sites.

Motivational Item Entries (6)

Entry 1:


PLAYBILL
Lunch Byte Theater
To Send or Not to Send
OCLC
LUNCH
BYTE
SERIES

Entry 2: Clean Desk/Clear Screen Security Awareness Activity

Be a Star! Secure Your Info.

Don't Let Your Info Go Sour.

Nobody Better Lay a Finger on My Sensitive Documents.

Be Twix You and Me, Secure Your Information.

Entry 3:

NCSAM Escape Room Start

The year is 2025. The Internet of Things (IoT) is everywhere and everything is connected to the Internet. Even your sock drawer is a "smart" sock drawer and will send you an email alert if you matched the wrong green socks together!

Entry 4:

Awareness Training | Role-Based Training | Cybersecurity Workforce Development | How Do I... | Resources | Contacts

And the Winner is... Top Phishing Reporter

Top Phishing Reporter

CONGRATULATIONS to the **Office of** for having the highest number of employees report the simulated phishing email during the phishing exercise on April 28-29. For the second phishing exercise in a row, OCTAE took advantage of the Department's new Report Phishing Button to rack up a record number of reports. The second and third place finishers, the Office of the Secretary and the Office of the Inspector General were also star reporters.

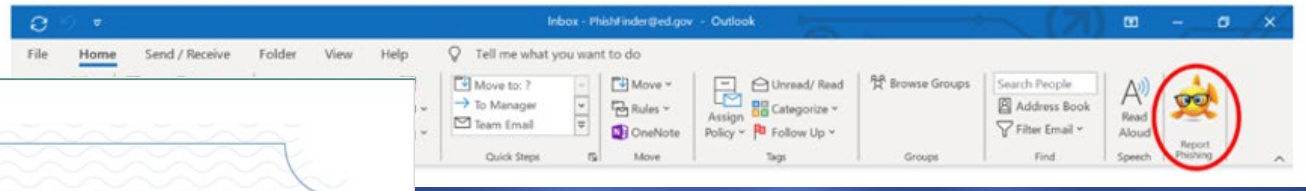
An email was sent to all ED Network users on Tuesday, April 28, 2020, as part of an authorized phishing exercise. percent (%) of all network users used the new ED Report Phishing button to report the email to the ED Security Operations Center. ED improved on the last exercise by again posting the highest level of reporting since the Simulated Phishing Exercise Program was initiated in 2014.

Top Performing Offices

Congratulations again to the top performing offices and the Information System Security Officers who lead their offices to victory:

Office	Report Percentage	ISSO
Office of		
Office of		
Office of		

REMINDER: If an email is asking you to click a link or submit personal information, always check the sender's name and email address. NEVER follow links in emails that route you outside the ED Network and NEVER give out your personal information. OCIO and its contractors will NEVER ask you for your password in an email or on the phone. If you are unsure of the legitimacy of an email, forward to the EDSOC using the Report Phishing Button, contact @ed.gov or call the EDSOC on (202) - .




CERTIFICATE OF AWARD

BEST PHISHING REPORTER

THIS CERTIFICATE IS AWARDED TO

Name of Office

DATE

PRESENTED BY

Entry 5:

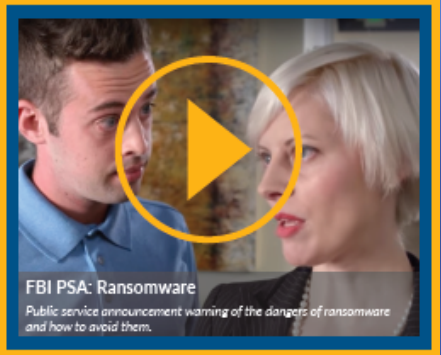

NIH National Institutes of Health
Cyber Safety. Protect our People and our Science.
Cyber Safety for Kids and Teens
An activity book from the National Institutes of Health
NIH Get Started
Welcome to Cyber Safety for Kids and Teens!

Entry 6:

HAVE YOU HEARD ABOUT RANSOMWARE?

What is Ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.



Healthcare is targeted more than any other industry

Source: Cylance Threat Report (2018)

~50% of all ransomware attacks in the last year targeted North America
McAfee Labs Threats Report (2019)

1 in 4 healthcare organizations are successfully **attacked by ransomware**
Kaspersky Cyber Pulse: The State of Cybersecurity in Healthcare (2018)

88% of all ransomware attacks target the **HEALTHCARE INDUSTRY**
Software Security Engineering Research Team (Q2, 2016)

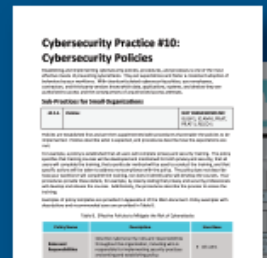
Ransomware attacks TRIPLED in 2017

Source: Cylance Threat Report (2018)

HEALTH INDUSTRY CYBERSECURITY PRACTICES:

Managing Threats and Protecting Patients

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication aims to raise awareness, provide vetted cybersecurity practices, and moves toward consistency in mitigating the current most pertinent cybersecurity threats to the sector. The main document examines cybersecurity



For 2020 we hereby award:

UNITED STATES POSTAL SERVICE, CISO

the honor of being selected as the

Security Motivational Item Contest Winner!

Be a Star! Secure Your Info.

Don’t Let Your Info Go Sour.

Nobody Better Lay a Finger on My Sensitive Documents.

Be Twix You and Me, Secure Your Information.

Newsletter Entries (8)

Entry 1:

The Security Scoop

March 2019

Are You OIG Ready?

CISO Corner

Dear Fellow Cybersecurity and IT Warriors,

The 2019 annual Office of the Inspector General (OIG) audit is upon us and set to begin in April. As we prepare it is important to refresh ourselves on the significance of these audits in the operations of the Department of Veterans Affairs (VA) and the Federal Government. The OIG provides an unbiased assessment on our efforts to safeguard information and information systems within the Department. This feedback is used at multiple levels, including our interactions with the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and Congress. Under law, federal employees are required to provide unrestricted access to requested information and resources within our individually assigned roles and responsibilities.

As a Department, it is imperative that we coordinate closely with the OIG. As cybersecurity and IT professionals, it is important for us to assist the IG team in their assessment within the area of responsibility we are assigned. Please take the time to work with the IG team. Listen to their questions, understand the context of their questions, and answer in a truthful and forthright manner. If the question is beyond the scope of your responsibility, let them know and elevate the question up to your Director.

Paul Cunningham, CISO

Historically, reoccurring OIG deficiencies are a major area for concern. The Office of Information Security (OIS) and Information Technology Operations and Services (ITOPS) have been actively sending technical support teams out to VA facilities since mid-January to assist in preparing for the coming OIG audit. Previous findings need to be resolved or identified to management as potential risk for a repeat finding.

It is our goal to ensure that the OIG audit reflects the Department's high-level of professionalism and commitment toward safeguarding VA and Veteran sensitive data. We can accomplish this goal by remediating past findings, applying strong risk management principles to known risks, and clearly articulating the Department's position during the audit. We need everyone's support and cooperation. By working together, we can ensure that the audit properly conveys the Department's focus toward security to our key stakeholders. ***Our success is VA's success!***

Preparing for the OIG Audit

The annual OIG audit gives a new meaning to the IT security phrase 'continuous monitoring'. Many may feel the 120 days between the end of one OIG audit and the following year's audit in April is too short. However, the OIG audits play a vital role in ensuring the security of sensitive VA and Veteran data. Consequently, inspectors are critical team players and their findings should be viewed as a positive factor toward improving the overall information security posture of the VA.

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

Entry 2:

National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

OCTOBER 2019 WEEK 1

Protecting Your Information and Devices

The Internet of Things

Technology has made our lives easier in so many ways. We can write more quickly, enjoy our favorite movies or music, anytime, anywhere, and speak to people in other countries almost instantaneously. Doctors can even use the Internet to perform surgery from hundreds of miles' distance from the patient.

What is Network Security?

In its Security Tip (ST15-002), the US Department of Homeland Security defines home network security in part as *"...the protection of a network that connects devices to each other and to the Internet within a home..."*

It's so convenient to be able to start your dinner or your car, unlock your doors or turn on your lights, start a load of laundry, or ask the refrigerator what you need to shop for on the way home, all at the tip of a finger; however, all that convenience provides means for malicious actors to steal our information, our sense of security, and our very identities. Online crime is the fastest-growing crime in the US.

In order to navigate the shark-infested waters of our technology-based society, users of that technology need to be aware of the risks that their devices present and how to secure those devices and the information that they process.

What are the Risks?

If a malicious actor manages to hack into a single one of your devices, it might allow them to steal your identity and open up all your other devices to malicious activity. This could mean:

- Clearing out your bank account.
- Opening credit cards, taking out loans, or running up medical bills in your name.
- Using your network to access illicit websites.
- Hacking into your social media accounts to phish your contacts.

The Deep Web

The Deep Web, also known as the Dark Web or the Invisible Web, contains approximately 95% of www content. This content cannot be indexed by search engines like Google and Bing and is difficult to navigate. Early developers of this peer-to-peer, heavily encrypted system, aimed to allow Internet users to access sites without leaving a browsing history or personal information that others could exploit for everything from targeted advertising to stealing identities. A criminal can use a stolen identity as cover while performing malicious activities like medical or mortgage fraud, selling illicit drugs, or trafficking child porn. As tempting as it may be to shield your online activity from advertisers, the Deep Web exposes users to more dangers than it protects them from, and may land them on the FBI watch list.

Teach Your Children Well

Remember you can use your devices to help keep your children safe online. Children are the fastest-growing group of victims of online crime. Websites such as us-cert.gov and staysafeonline.org have great tips for keeping your children safe online. The www.cynja.com site provides an age-appropriate, safe space for kids that includes activity reports for parents, as well as engaging graphic novels that teach kids about online safety. The KidzSearch app filters Google searches to remove inappropriate content and unsafe sites.

Many apps track your child's location or screen time, and allow you to access that information using your computer or smart phone. Others monitor their social media usage or limit the times when they are allowed to be online.

Being aware of what they are doing online and teaching them safe online habits is your best means of protecting your children from online crooks:

- Talk to your children about online safety, like not talking to strangers or giving out personal information.
- Keep Internet-capable devices where you can see what your children are doing.
- Use device- and app-provided parental controls.
- Set reasonable time and usage limits.

Entry 3:

April 2019, Volume 3, Issue 4

CYBER Outlook

Mission

The FORSCOM G6 Cybersecurity Branch assists subordinate units with the framework to operate securely, efficiently, and reduce the operational risks associated with managing technology.

Cyberforce Online Training Platform

Cyberforce is an online training platform that is currently accessible to DoD CAC holders. The cybersecurity community is highly encouraged to utilize this resource as it provides a wealth of sustainment and skill-honing content. Hands-on lab environment training is a major feature of the platform with exercises in network traffic analysis, malware hunting, incident response, scripting, defensive and offensive cyber tools; just to name a few. Explore the myriad of features and bolster your readiness today.

Link: https://portal.cyberforce.site

DoD CIO Cybersecurity Reference and Resource Guide 2018

The purpose of this document is to provide an overview of useful open source references to support Security Cooperation across the U.S. government, commercial sector, and U.S. allies and partners. Within this document, readers will find information regarding cybersecurity norms, best practices, policies, and standards written and adopted by the U.S. federal government, the U.S. Department of Defense, and recognized institutional standards.

Link: https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD%20CIO%20CS%20Reference%20and%20Resource%20Guide%202018_v9.1_Final_2018.pdf

Summary of the 2018 DOD Artificial intelligence Strategy

The Department of Defense's (DoD) Artificial Intelligence (AI) Strategy directs the DoD to accelerate the adoption of AI and the creation of a force fit for our time. A strong, technologically advanced Department is essential for protecting the security of our nation, preserving access to markets that will improve our standard of living, and ensuring that we are capable of passing intact to the younger generations the freedoms we currently enjoy.

Link: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

For corrections or comments email us at: usarmy.bragg.forscom.list.g6-cyber-security-branch@mail.mil

Entry 4:

From: Security Awareness <awareness>
Subject: Emails From External Sources: What You Need To Know

what you need to know about

EMAILS FROM EXTERNAL SOURCES

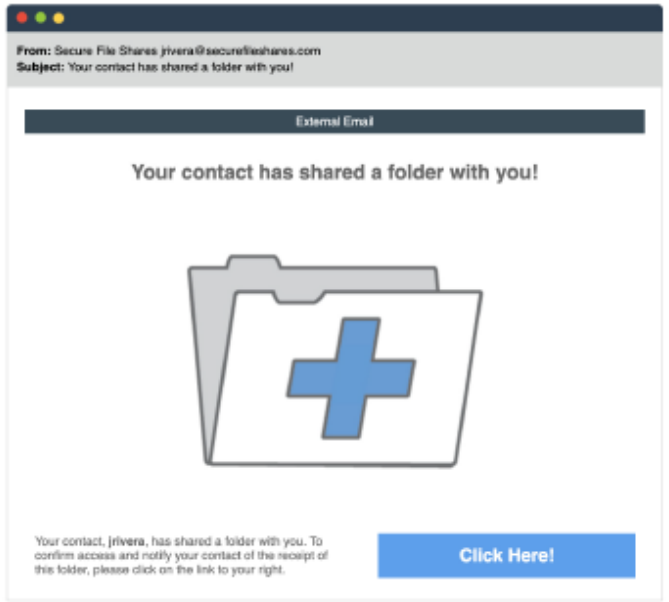
If you receive an email from a sender outside our organization, use extra caution. Look at the email subject and header to see if it is from an external sender.

External tagging is the practice of including one or more visual clues to help identify emails that are received from addresses outside of our internal network. Clues such as **[EXTERNAL]** in the email subject indicate potentially fraudulent messages.

Even if an email looks like it is from an internal sender, it doesn't guarantee that it is safe. Phishers can spoof email addresses and signatures belonging to your supervisors and colleagues.

Be careful whenever an email prompts you to open a link, download an attachment, or log into an account—even if that email isn't marked "External".

See an example of external tagging below.



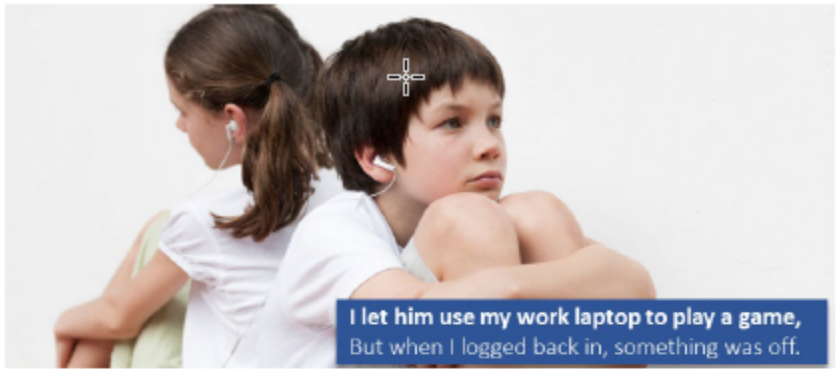
Look carefully at every email to determine if anything is suspicious:

1. **Was it sent from a non-standard company address?**
   Does the email include our standard company signature?
2. **Are there spelling or grammar mistakes?**
   Also look for unusual spacing or formatting.
3. **Look for inconsistencies.**
   Does the sender's tone or language match what you've come to expect from that colleague? Call the sender to verify the email is legitimate.

Entry 5:

National Institutes of Health

Cyber Safety. Protect our People and our Science.



Julie's Cyber Safety Story – "I Let My Son Use My Laptop."

Each month the Cyber Safety Awareness Campaign team will be sharing a story that's based on a real-life cybersecurity risk or incident at NIH. This effort is meant to raise awareness that cyber safety is a very real concern for all of us at NIH.

"My name is Julie, and this is the story of what happened when I let my ten-year-old son use my NIH laptop."

I had wrapped up working from home and was starting to make dinner when my son walked in. He wanted to know if he could use my NIH laptop to play a game he had heard about online.

Hoping to keep him busy until dinner was ready, I logged into the computer for him and left to finish cooking.

Later that evening, I opened my laptop to check my email and immediately noticed a pop-up message saying that my system had been compromised by malware. That's when it hit me that I had made a huge mistake. I called the NIH IT Service Desk to report a cyber incident.

Which of the following remote work best practices could have helped Julie prevent this potentially dangerous cybersecurity incident?

A. Never allow anyone, even your family, to use your government-issued equipment
B. Only allow others to use your government-issued equipment with close supervision
C. Use a designated space within your home as a remote work office to control access

To find out the correct answer(s) and learn more about working from home securely, visit the Sharing Our Cyber Stories page on the Cyber Safety Awareness Campaign website.

Thank you for your ongoing commitment to cyber safety. Your hard work enables us to continue to Protect our People and our Science and to safeguard the mission of the NIH.

Best,

Jothi Dugar
Cyber Safety Awareness Campaign Lead

Entry 6:

SOCIAL MEDIA

GUIDELINES AND
BEST PRACTICES

BROUGHT TO YOU BY THE
BUREAU OF DIPLOMATIC SECURITY
DIRECTORATE OF CYBER AND TECHNOLOGY SECURITY

Entry 7:

Published by KnowBe4
CYBERHEISTNEWS
arming you with the facts

CyberheistNews Vol 10 #30 | July 21st., 2020

[Heads Up] What Is Consent-Phishing? Microsoft Warns About New App-Based Attack Angle

Microsoft has issued an advisory warning about "consent phishing," or application-based phishing attacks that rely on users granting permissions to malicious apps. These attacks aren't as well-known or as obvious as credential-harvesting or email-based phishing attacks, but they can be just as dangerous.

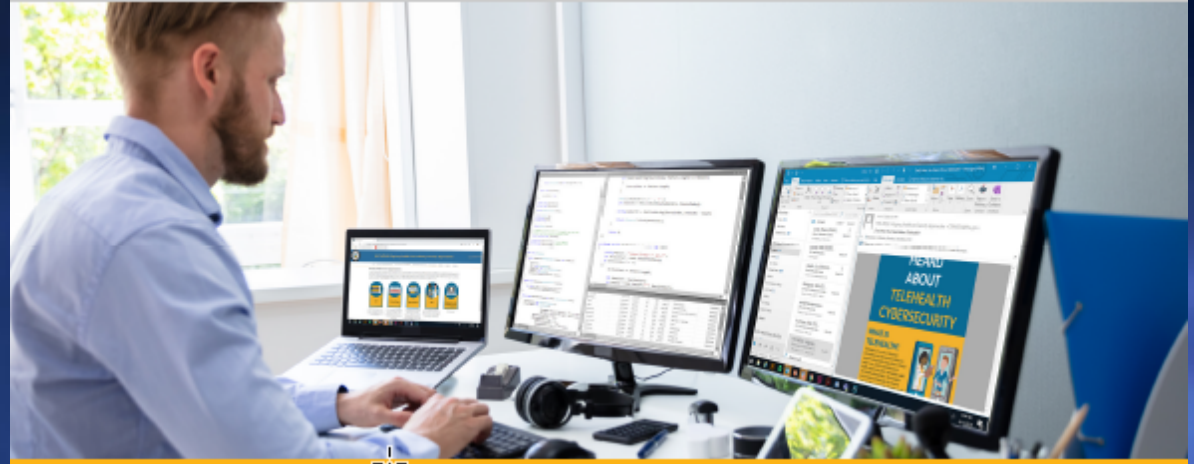
In consent phishing attacks, the user sees a pop-up from an application requesting extensive permissions. This consent screen lists all the permissions the app will receive, and many users may go on to accept the terms uncritically because they assume the app is trustworthy.

"If the user accepts, the attacker can gain access to their mail, forwarding rules, files, contacts, notes, profile, and other sensitive data and resources," Microsoft explains.

Microsoft describes the steps in such an attack:

- "An attacker registers an app with an OAuth 2.0 provider, such as Azure Active Directory.
- "The app is configured in a way that makes it seem trustworthy, like using the name of a popular product used in the same ecosystem.
- "The attacker gets a link in front of users, which may be done through conventional email-based phishing, by compromising a non-malicious website, or other techniques.
- "The user clicks the link and is shown an authentic consent prompt asking them to grant the malicious app permissions to data.
- "If a user clicks accept, they will grant the app permissions to access sensitive data.

Entry 8:



Telework During COVID-19
Good Practices To Protect From Cyberattacks

By Sekar Thanigaimani, 405(d) Task Group Member

As the COVID-19 pandemic spreads around the world, the World Health Organization (WHO) has made the suggestion that organizations introduce more teleworking. Many organizations are considering work from home options to reduce the risk of their staff getting infected. Typically, when employees are working inside the corporate network, the enterprise security team can monitor and protect them. But working from home exposes the employee's devices and through them, the organization's network to various threats.

Attackers are taking advantage of the fact that many employees who are working from home have not applied the same security on their own networks that would be in place in a corporate environment. There have been multiple cases of malicious COVID-19 mobile applications and malicious emails that give attackers potential access to data or the ability to encrypt devices for ransom. Organizations should continue to assess the security controls in the context of telework which can include: implementation of single sign-on, multi-factor authentication, encryption of data, protecting the home Wifi network, VPN to connect to the organization's network, and monitoring and applying security patches regularly. However, there are ways to protect and mitigate risks from cyberattacks using the Health Industry Cybersecurity Practices (HICP) Publication. HICP focuses on five threats and ten best practices that help organizations improve the strength of their security controls.

The two things I like most about the HICP framework is that, it is designed to be used by healthcare organizations of all sizes (small to large enterprises), and the best practices are documented at a granular level which serve as an easy tool for a quick assessment which helps organizations improve their security posture. For example, "Deploy multifactor authentication (MFA) before enabling access to your e-mail system. MFA prevents hackers who have obtained a legitimate user's credentials from accessing your system". I was able to do a quick assessment using HICP and implement the recommended best practices.

For 2020 we hereby award:

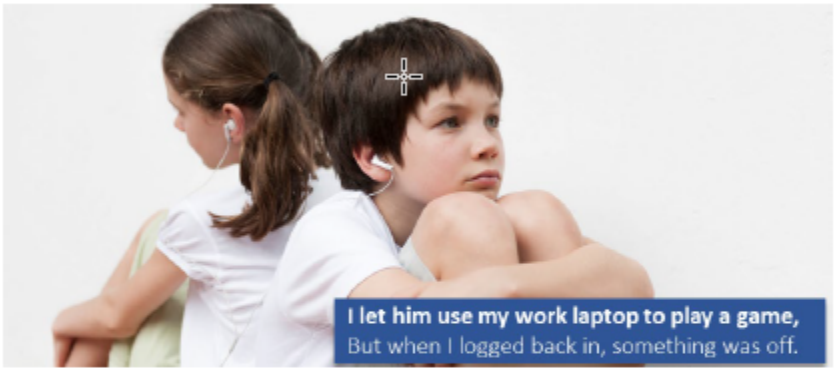
NATIONAL INSTITUTES OF HEALTH – CYBER SAFETY AWARENESS CAMPAIGN

the honor of being selected as the

Security Newsletter Contest Winner!

NIH National Institutes of Health

Cyber Safety. Protect our People and our Science.



Julie's Cyber Safety Story – "I Let My Son Use My Laptop."

Each month the Cyber Safety Awareness Campaign team will be sharing a story that's based on a real-life cybersecurity risk or incident at NIH. This effort is meant to raise awareness that cyber safety is a very real concern for all of us at NIH.

"My name is Julie, and this is the story of what happened when I let my ten-year-old son use my NIH laptop."

I had wrapped up working from home and was starting to make dinner when my son walked in. He wanted to know if he could use my NIH laptop to play a game he had heard about online.

Hoping to keep him busy until dinner was ready, I logged into the computer for him and left to finish cooking.

Later that evening, I opened my laptop to check my email and immediately noticed a pop-up message saying that my system had been compromised by malware. That's when it hit me that I had made a huge mistake. I called the NIH IT Service Desk to report a cyber incident.

Which of the following remote work best practices could have helped Julie prevent this potentially dangerous cybersecurity incident?

A. Never allow anyone, even your family, to use your government-issued equipment
B. Only allow others to use your government-issued equipment with close supervision
C. Use a designated space within your home as a remote work office to control access

To find out the correct answer(s) and learn more about working from home securely, visit the Sharing Our Cyber Stories page on the Cyber Safety Awareness Campaign website.

Thank you for your ongoing commitment to cyber safety. Your hard work enables us to continue to Protect our People and our Science and to safeguard the mission of the NIH.

Best,

Jothi Dugar
Cyber Safety Awareness Campaign Lead

*Podcast Entries (4)**

Entry 1: *Coronavirus and Awareness Training*

With much of the world focused on COVID-19, or Coronavirus, attackers are taking advantage of the resulting concern to target potential victims with Coronavirus-themed scams. A result of this is the decision to use these scams as part of phishing awareness training.

Entry 2:

The Cyber Tap Podcast – Episode 10 "Fast Times at Online High"

Join Mat and Mike from cyberTAP at Purdue University for a fun and informative discussion. Listen as they unpack cybersecurity news, conduct interviews with industry experts, and dish the latest tech, tools, tips and tricks…as long as they stay focused.

Entry 3: *Cyber Safety is Patient Safety: The importance of Healthcare Cybersecurity*

In this podcast, your hosts are two leaders in health care cybersecurity. Listen in as they discuss evolving threats and collaborative mitigations for healthcare cybersecurity.

Entry 4: *Podcast "How Hackers Hack and How to Protect Yourself"*

This innovative podcast contains three fascinating interviews, which delve into the devious minds of different types of hackers. We answer questions such as, "What's your role in helping to protect CMS systems and information?"

For 2020 we hereby award:

INFORMATION SECURITY & PRIVACY GROUP (ISPG)
OFFICE OF INFORMATION TECHNOLOGY (OIT)
CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

the honor of being selected as the

Security Podcast Contest Winner!

Entry 4: *Podcast "How Hackers Hack and How to Protect Yourself"*

This innovative podcast contains three fascinating interviews, which delve into the devious minds of different types of hackers. We answer questions such as, "What's your role in helping to protect CMS systems and information?"

Poster Entries (9)

Entry 1:


IN SUPPORT OF
NATIONAL CYBERSECURITY AWARENESS MONTH (NCSAM),
USPS CORPORATE INFORMATION SECURITY OFFICE (CISO) PRESENTS:
UNITED STATES POSTAL SERVICE
WELCOME TO THE
NEW CYBER
FRONTIER
4TH ANNUAL CYBERSECURITY AWARENESS FAIR
THURSDAY, OCTOBER 10, 2019
11 AM - 1 PM • USPS HQ ROOM 1P410
SECURE IT. PROTECT IT. OWN IT.
UNITED STATES POSTAL SERVICE

Entry 2:


Cyber Hygiene
Make it a part of your daily routine.
vaww.portal2.va.gov/sites/Infosecurity/IAM/
CTM
VA
U.S. Department of Veterans Affairs
Office of Information and Technology
Office of Information Security

Entry 3:

National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

OCTOBER 2019

WEEK 5

Cybersecurity Bag of Tricks

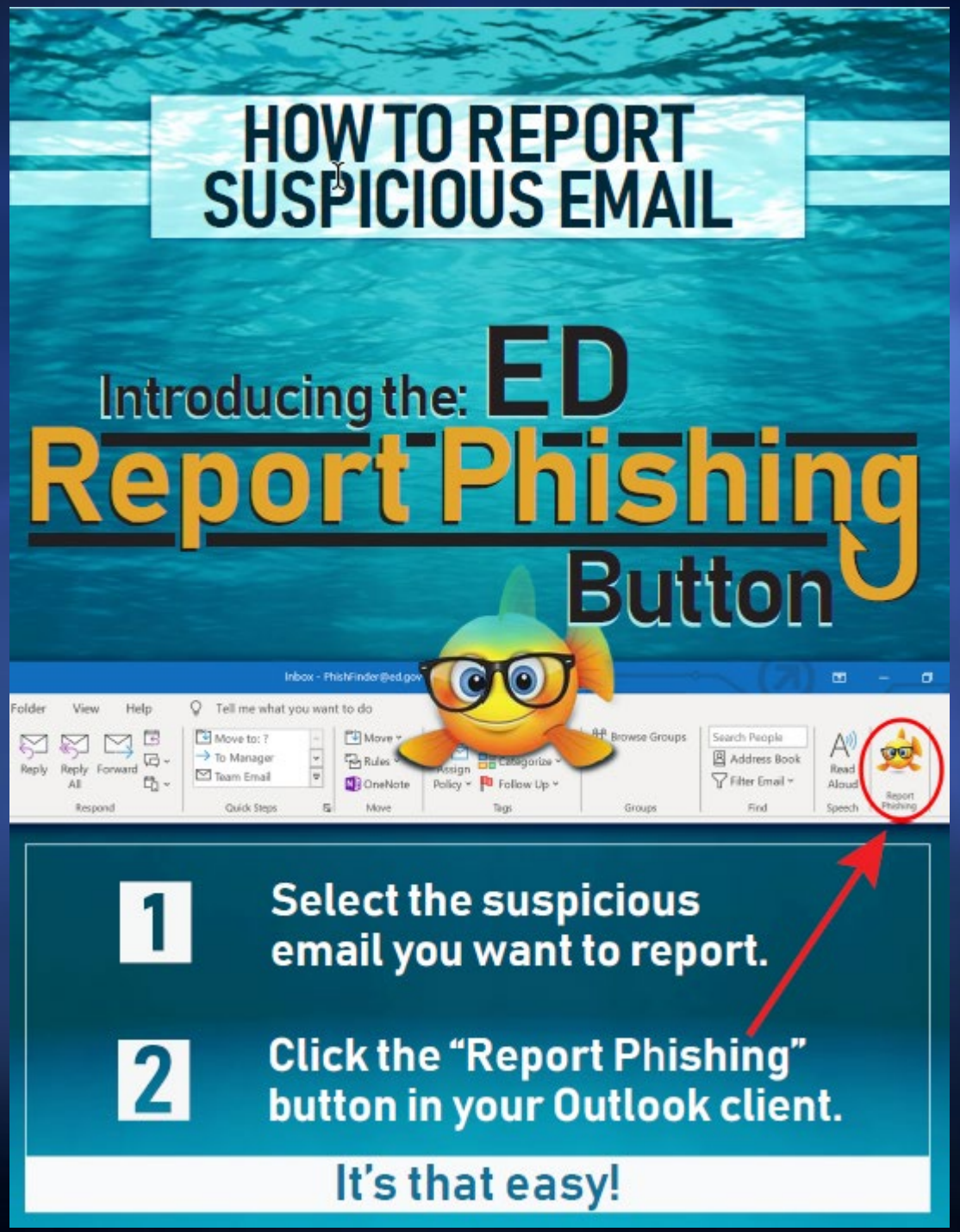
When you're a superhero like Captain Cybersecurity, maintaining proper cybersecurity hygiene is a must, especially when you are traveling on assignment as your mild-mannered secret identity.

Captain Cybersecurity always makes sure to pack his bag of Internet Security Essentials whenever he travels.

Follow these tips to make sure your cybersecurity bag is packed correctly!

1. **Selective Sharer.** Be sure to always keep your personal information private and don't share anything with people you don't know.
2. **Security Patches.** Always install the latest security patches and updates for your software and hardware.
3. **Two-Factor Authentication.** Make sure that all of your devices and accounts are protected by a second level of security just in case the first level fails.
4. **Safe Shopping.** Never use a site that doesn't have HTTPS in the URL to verify your transactions are secure.
5. **VPN.** Set up a Virtual Private Network to keep your WiFi connection encrypted.
6. **Click Smart.** Always hover over a link before clicking on it. This lets you see the actual URL you are heading to and avoid going to dangerous sites.
7. **Password Manager.** Use a trusted password manager to store and generate secure passwords for all of your devices.
8. **Passphrase.** Passphrases are more secure due to their length and complexity, but easier for a user to rememeber due to their familiarity to the user.
9. **Glasses.** No one can ever tell that you're secretly a super hero as long as you are wearing your trusted glasses.
10. **Super Team Membership Card.** Your PIV Card is your IHS Defender Membership card. Always protect it and keep it with you. Never share your PIN.

Entry 4:


HOW TO REPORT SUSPICIOUS EMAIL
Introducing the: ED
Report Phishing Button
Inbox - PhishFinder@ed.gov
Folder
View
Help
Tell me what you want to do
Reply
Reply All
Forward
Move to: ?
To Manager
Team Email
Move
Rules
OneNote
Assign Policy
Follow Up
Browse Groups
Search People
Address Book
Filter Email
Read Aloud
Report Phishing
Respond
Quick Steps
Move
Tags
Groups
Find
Speech
1
Select the suspicious email you want to report.
2
Click the "Report Phishing" button in your Outlook client.
It's that easy!

Entry 5:

10 Tips for Protecting Privacy

Whether at work, home, or on the go, it is your responsibility to follow our policies to safeguard information.

Treat emails with caution

Spear phishing emails bypass technical safeguards. Examine all emails, and look for warning signs of a phish. Report all suspicious emails.

Keep your work station organized. It will be easier to spot if anything is missing.

Use strong passwords. Long passwords with uppercase and lowercase letters, numbers, and special characters are more difficult to crack. Change your passwords regularly, and use multi-factor authentication when available.

Keep software updated. Update software frequently to patch security holes, but only download updates from a trusted source.

Review your privacy settings. Be mindful of what you post on social media, and limit who can view your profile.

Remember - the recycle bin isn't enough. Files deleted using a computer's recycle bin can be easily restored. Use a secure wipe method, and shred documents that with sensitive information.

Connect securely to public wifi. Use a trustworthy Virtual Private Network (VPN), which hides your location and encrypts your data.

Be aware of your surroundings. Visual hacking or shoulder-surfing is when someone looks over your shoulder to steal information. Minimize the risk by closing unused windows and tabs or using a privacy screen.

Lock your devices. Don't leave documents or devices unattended. Lock your device before stepping away, and encrypt any personal devices used to access work-related information.

Be prepared. Set up "Find my Phone" and "Remote Wipe" apps ahead of time to locate a lost device or restore your phone to factory settings in case it can't be found.

Entry 6:


DON'T GET PHISHED!
SOME THINGS DESERVE
A SECOND GLANCE
Email messages are not always what they appear to be.
Contact the DOT SOC as soon as possible if you have received a suspicious email or believe you have fallen victim to a phishing attack.
DOT SOC Phone:
or DOT SOC E-mail:
U.S. Department of Transportation

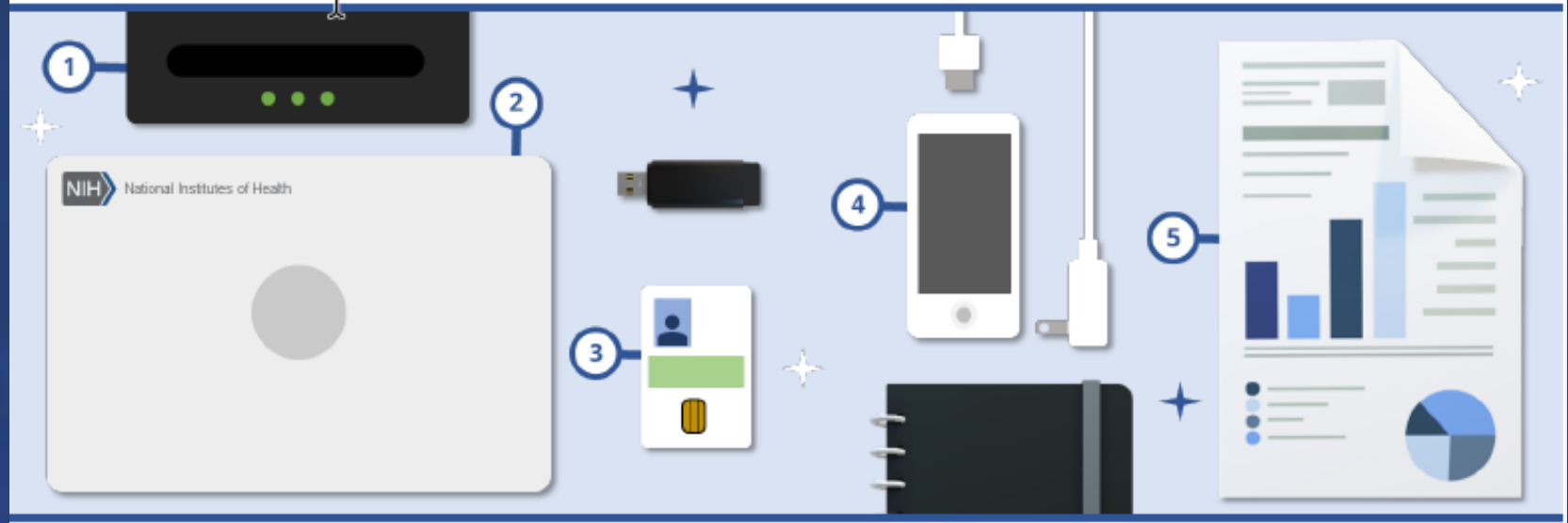
Entry 7:

Cyber Safety | Remote Work

Even though you may be working from home, you still have a critical role to play in defending against cyberattacks that target the NIH. Use the tips below to protect yourself and our organization by keeping your remote workspace secure.

National Institutes of Health

Cyber Safety. Protect our People and our Science.



1. Protect Your Network

- Enable WPA2 encryption on your router
- Use a strong password for your router with at least eight characters, including upper and lowercase letters, numbers, and symbols
- Consider using a personal firewall for your home network

2. Secure Your Equipment

- Never let friends or family use work devices
- Use a surge protector, not just a power strip
- Work from a secure, designated workspace
- Don't cable unsecured devices to your laptop
- Use a screen lock with a strong password

3. Stay Connected

- Follow the steps in the Remote Network Connection Guide to initiate VPN access
- Use a PIV and trusted network connection to access Microsoft 365 services without VPN
- Use only approved virtual meeting tools

4. Be Safe on the Go

- Don't connect to free open Wi-Fi; use your phone's mobile hotspot instead
- Use a privacy screen in public and don't leave devices or papers unattended
- Never discuss sensitive information in public
- If you must leave a laptop in the car, lock it in the trunk before arriving at your destination

5. Safeguard Sensitive Information (SI)

- Lock paper SI in a cabinet, and shred at NIH
- When mailing SI, do so from a post office
- Don't use personal phones for work unless protected by NIH's mobile device management solution
- Use only NIH USBs; encrypt USBs that hold SI
- Never use a personal email account for work

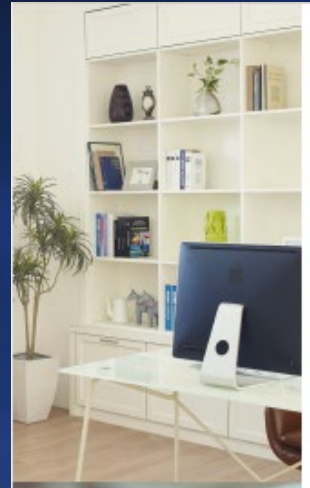
Report an Incident

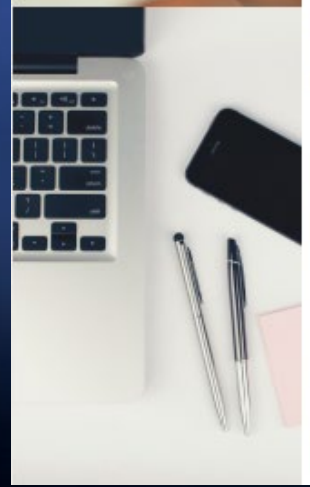
To report an incident, contact your ISSO and the IT Service Desk (301-496-4357).

Learn More

To learn more about cyber safety, visit the Cyber Safety Awareness Campaign website.

Entry 8:





CYBERSECURITY AWARENESS PROGRAM | DEPARTMENT OF STATE

PRACTICE CYBER VIGILANCE WHILE WORKING FROM HOME

With increased levels of telework continuing across federal agencies, malicious actors are targeting employees working remotely who may be more vulnerable to manipulation during times of crisis. Whether we are working from home or alternate sites, we are all responsible for practicing the same, if not higher, level of vigilance as we do on an on-site computer or workstation. If accessing government information or systems remotely, implement the following measures to protect yourself and the government.

MAINTAIN PRIVACY

Be aware of your surroundings when discussing or processing sensitive information in any alternate location, and if you feel that a conversation is edging toward an improperly sensitive level given the conditions (e.g., outside of a secure location), please inform your colleagues and remove yourself from the conversation if needed.

Keep all sensitive conversations, whether via phone call, video conferencing, or online messaging, private. When establishing a video or audio teleconference, remind all meeting participants to keep discussions at the appropriate classification level. Make sure your screen is not visible to others, especially in public spaces (e.g., cafes, parks).

If you must use a shared family computer, make sure you have a password protected account that only you access, and lock your screen when stepping away. Share your knowledge with family members on how to practice proper cyber hygiene. As needed, set parental controls and safety settings, filters, and pop-up blockers in search engines and online games.

STAY PROTECTED

Remember that personal devices do not have the same levels of protection as government or in-office devices, so it is imperative that you keep your operating system, firewalls, and anti-malware software up to date.

MIND YOUR DEVICES

Personally-owned IoT devices (Echo, Ring, smartwatch) often have audio and video recording capabilities turned on at all times, ready to set an alarm or tell you the weather at your command. However, you should disable these capabilities when discussing or processing sensitive information at home. Many devices have physical buttons or app settings that allow you to turn off audio and video recording capabilities, and you can refer to your device's user manual for specific instructions on how to disable them. If you are still unsure of how to disable recording capabilities, simply unplug the device.

You may even consider stepping away from these technologies by making calls outside your home, but remember to maintain awareness of your environment and use discretion to ensure no one is within earshot of sensitive conversations.

BEWARE PHISHING ATTEMPTS

Take extra caution when opening attachments or clicking links from your personal, government or business email, as well as when browsing the Internet, downloading software or executable files, or responding to unsolicited phone calls, text messages, or social media messages.

Phishing attempts may come in the form of emails with updates about COVID-19 from unverified senders, as calls, emails, or texts from scammers posing as Microsoft tech support, or as fake Microsoft O365 login pages which will steal your credentials if entered.

Additional topical scams include phony requests for personal or financial information related to government stimulus payments and other financial assistance, malicious COVID-19 tracking platforms, and websites and robocalls peddling counterfeit face masks or testing kits.

STRENGTHEN PASSWORDS

Use a strong, complex, and unique password or passphrase for each device, app, and connected WI-FI network. Be sure to change default usernames and passwords, which can be hacked easily. Passwords for multiple devices and accounts should not be the same. If you suspect your work password has been compromised, change it immediately and report the suspected breach to the designated contact.

UPDATE APPS AND CLOUD SECURITY

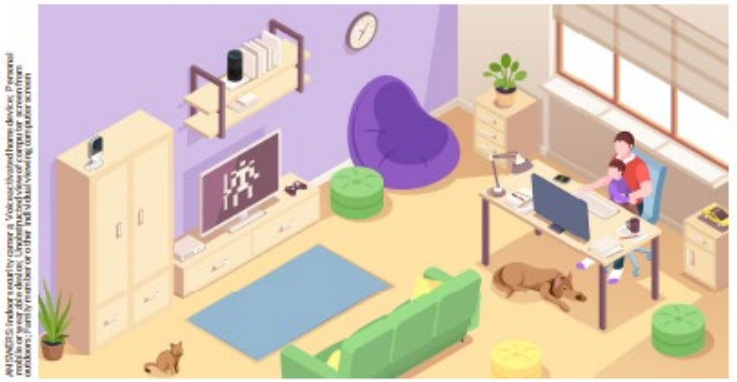
Keep tabs on your apps. Many connected devices are supported by mobile applications with default permissions you never realized you approved – gathering your personal information in the background without your knowledge. Also ensure that you process official or business sensitive information only on approved platforms and applications when working remotely.

REMAIN ACCOUNTABLE

Government employees have always been popular targets of cyber crime because of their access to potentially sensitive data and systems. As you carry out official duties from home, understand that you have a shared responsibility to protect your agency from malicious attacks. Therefore, if you believe your account has been compromised, immediately contact your designated information security officer and inform your supervisor.

QUIZ

Can you spot the five potential cybersecurity risks in this telework environment?



Entry 9:

CYBER DILIGENCE & HEALTH CRISES

During a health crisis, keeping patients safe is the #1 priority so remember, Cyber Safety is Patient Safety.

Be cautious of the 5 most prevalent cybersecurity threats during a health crisis:

1. Ransomware Attack
2. Email Phishing
3. Network Vulnerabilities
4. Loss or Theft of Equipment or Data
5. Medical Device Security

To protect your patients and organization, keep in mind these cyber safety tips:

1. Don't click it, check it
2. Prevent it, See it, Report it
3. Secure your home office
4. Know your back up plans
5. Be mindful not to connect or plug in personal devices into work stations

KEEP YOUR PATIENTS SAFE BY PRACTICING THESE CYBER TIPS!

HHS 405(d)
Aligning Health Care Industry Security Approaches

If you are looking for other cybersecurity best practices, cybersecurity tips, or resources for your healthcare organization check out the 405(d) Program Social Media @ask405d on Twitter, Instagram, and Facebook!

For 2020 we hereby award:

DEBORAH COLEMAN
U.S. DEPARTMENT OF EDUCATION

the honor of being selected as the

Security Poster Contest Winner!

HOW TO REPORT SUSPICIOUS EMAIL

Introducing the: ED Report Phishing Button

1 Select the suspicious email you want to report.

2 Click the "Report Phishing" button in your Outlook client.

It's that easy!

Training Entries (7)

Entry 1: https://links.mediapro.com/DAvPfM4U/

Entry 2: https://youtu.be/IfJrfVP9WM0

From: Delivery Notification <do-not-reply@freightinternationalservices.com>
Subject: Package Undeliverable

Delivery Notification

Order: SGH-9226-99950127

Dear Customer,

Your parcel has arrived at the post office. Our courier attempted but was unable to deliver the parcel to you.

To receive your parcel, please go to the nearest office and show this receipt.

GET AND PRINT RECEIPT

Thank you

Don't Close This Window

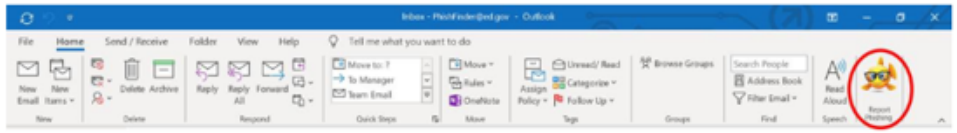
Until You Read the Information Below

You Took the Bait and Got Phished!

This authorized phishing exercise was conducted by the Department of Education to provide training on identifying and reporting phishing attacks.

Phishing emails ask you to provide sensitive information, encourage you to click links, or urge you to download attachments. When suspicious emails make it through our defenses, **YOU are our last line of defense.**

Next time use the **ED Report Phishing** button in your Outlook ribbon on your government furnished laptop or desktop to quickly, easily, and directly report suspicious emails to the Department of Education Security Operations Center (EDSOC).



Notify the EDSOC at or @ED.GOV as soon as possible if you think you may have clicked a link, opened an attachment, or provided your network credentials in response to a spear phishing email.

If you have questions or would like more information about phishing or the Department's phishing awareness program, please visit the Cybersecurity Awareness and Training site on ConnectED or email @ed.gov.

Entry 3: https://www.us-cert.gov/cdm/training

CDM AGENCY DASHBOARD TRAINING

CDM141-1 Examine the Agency Overview Lab

The Agency Overview dashboard within the new CDM Agency Dashboard is the baseline or home page view of the most important information designated by the CDM Program as critical for federal cybersecurity awareness. Each of the visualizations or panels are filtered views of CDM data that helps quickly isolate and drill into vulnerabilities, system components, and other data.

Learning Objectives

- Become familiar with the Kibana interface and terminology.
- Navigate the Agency Overview dashboard and the rest of the new CDM Agency Dashboard.
- Tour the different dashboard that identify the top contributors that are causing risk exposure.

Prerequisites

- none

What Is Needed to Complete This Lab

- this lab guide
- a logged-in session in the new CDM Agency Dashboard environment
- a completed evaluation (follow all lab steps before answering the evaluation questions)

Estimated Duration

- 30 minutes

Entry 4:

fissea FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

Cyber Range Challenge: Ransomware

In FY20Q3, CISA launched its' Identify, Mitigate, and Recover (IMR) Series of Incident Handling awareness webinars and training classes.

The webinars provide an overview of an attack vector and the training classes are designed as hands-on training activities, including live-fire cyber challenges.

CISA
CYBER+INFRASTRUCTURE

Ransomware Cyber Range Challenge: Can you Identify the Attack and Defend your Network?

The Ransomware exercise is a seven-hour, live-fire Cyber Range training exercise led by technical instructors and expert cybersecurity engineers.

Entry 5:

From: Calendar Invitations <no-reply@applerts.net>
Subject: Join Meeting Invite Now

You have a new Meeting Invitation Waiting for you right now.

CHECK IN

Event Details
Status: Pending Acceptance
Date: SCENARIO_START_DATETIME
Timeframe: 00:30 minutes

Confirmation code: PWRUZ7

Unsubscribe from list • Privacy statement
14609-15705 NE 40th Pl, Redmond, WA 98052

WHAT YOU NEED TO KNOW ABOUT

REMOTE WORK PHISHING SCAMS

WHY ARE THEY SUCCESSFUL?

These phishing emails bypass technical safeguards and leverage human vulnerabilities to infect our network.

They use social engineering tactics to trick you into opening an attachment, clicking a link to obtain your credentials, or download a malicious file.

Also, watch out for Business Email Compromise (BEC) email scams that try to trick you into sending money or gift cards.

POPULAR EXAMPLES

- Work remotely enrollment
- Workplace policy emails
- VPN updates
- Update your password

ALWAYS REMEMBER

01. EXAMINE THE URL.

If you click a URL that directs you to a login page, look at the URL to ensure it is correct.

02. KEEP PASSWORDS SAFE.

No reputable company will ask for your password over email.

03. THINK TWICE.

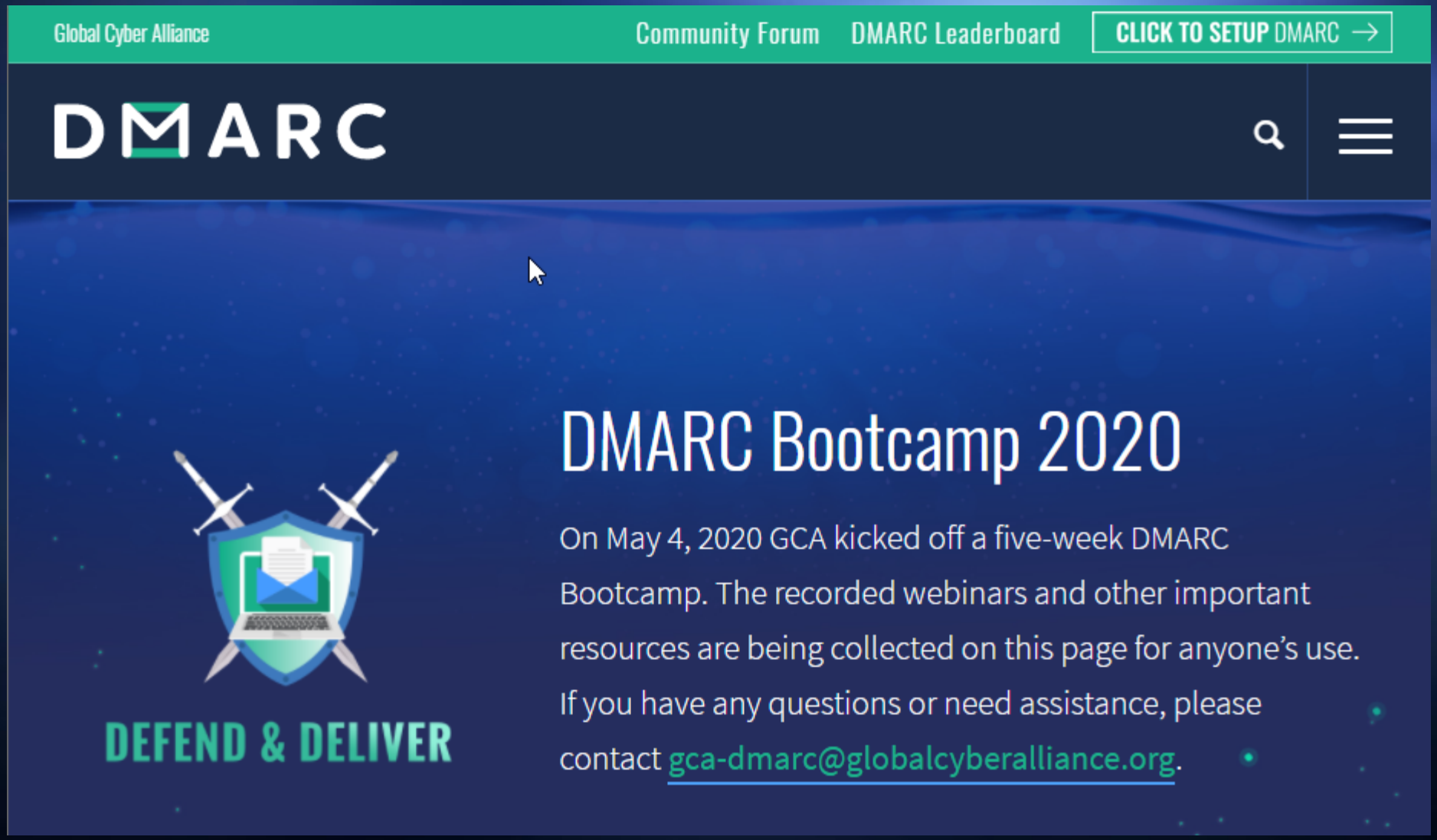
Attackers will use emotional appeals in their emails. Stay calm and look closely at the email for grammar or typos.

04. REPORT IT!

Even if you've already interacted with the link or attachment.

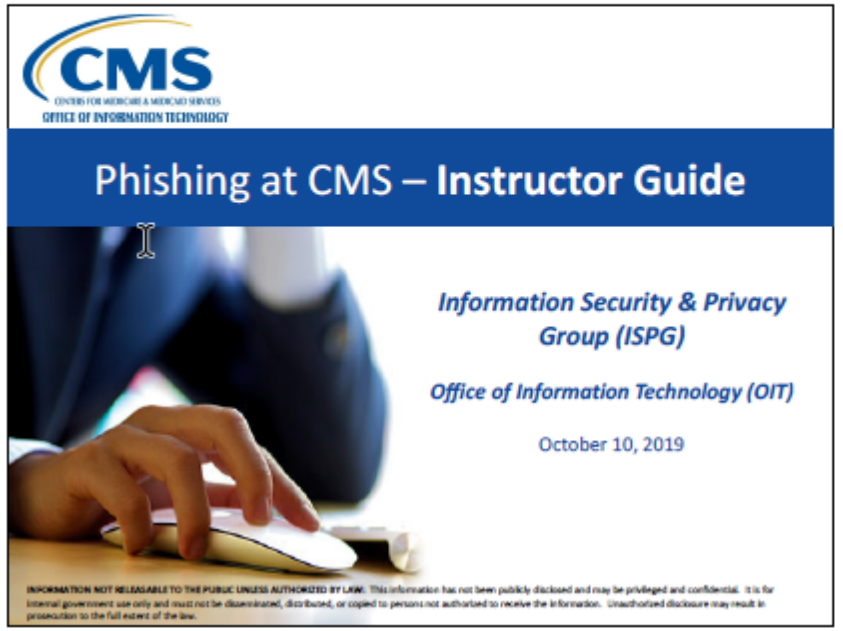
Report Phishing

Entry 6: https://dmarc.globalcyberalliance.org/dmarc-bootcamp/



Entry 7:

Phishing at CMS



Instructor Guide

Time:

Materials Required:
- Paper and pens/pencils
- Pre-survey results available
- Handouts

Preparation:
- Place paper and pens/pencils at each seat.

Facilitator Notes:
- Make sure the PowerPoint slides are on the computer that will be used the day of the presentation
- **Welcome to Phishing at CMS**
- **I'm your presenter ____ along with_____**
- **We have _____ from _____ who would like to say a few words…**

For 2020 we hereby award:

MEDIAPRO

the honor of being selected as the

Security Training Contest Winner!

https://links.mediapro.com/DAvPfM4U/

NIST Cybersecurity Framework

A framework for safeguarding data and protecting our organization.

Start | Table of Cont

MediaPRO
Cybersecurity & Privacy Education

NIST Cybersecurity Framework

The CSF in Real Life

A lot goes into implementing the CSF, and you may not always see the benefits until they're really needed.

> Think of the planning you do now like an investment which will help protect us in the future.

Let's see what could happen as a result of implementing ... or not implementing, each Function of the CSF.

To learn more about FUNCTIONS, click the characters above. When you're finished, click NEXT.

Video Entries (6)

Entry 1: https://youtu.be/IfJrfVP9WM0

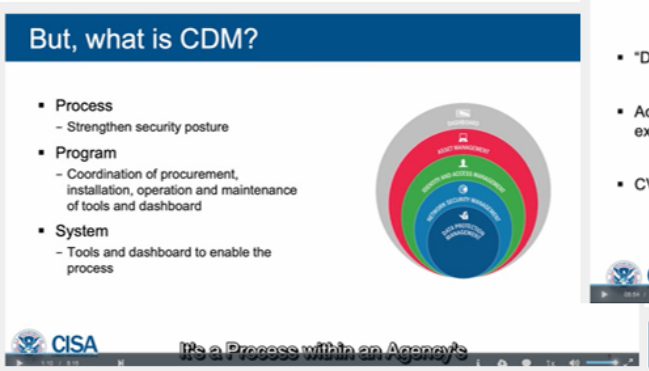
Entry 2:

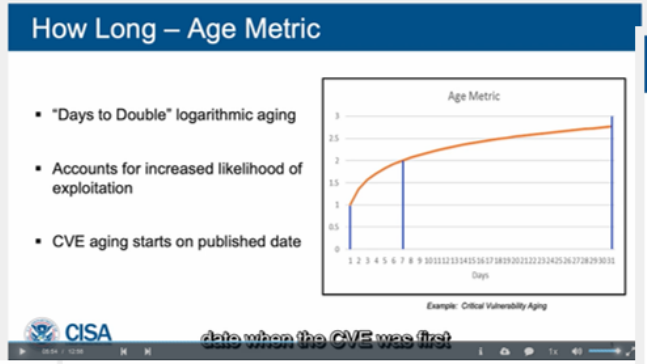
CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

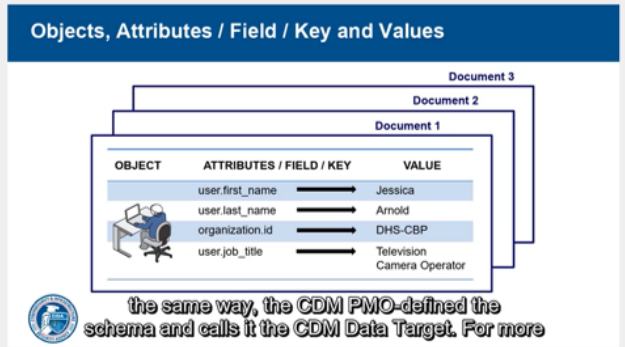
fissea FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

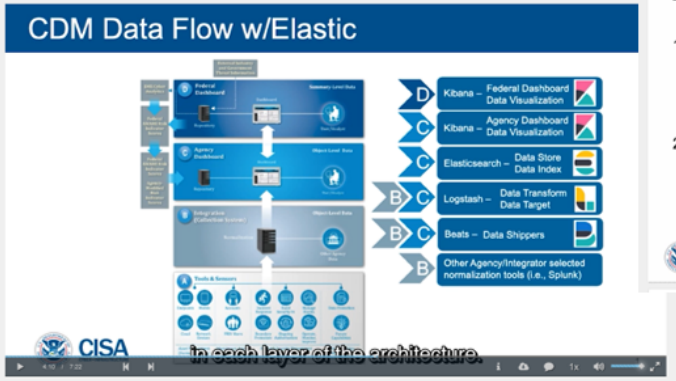
Website for info: https://www.us-cert.gov/cdm/training

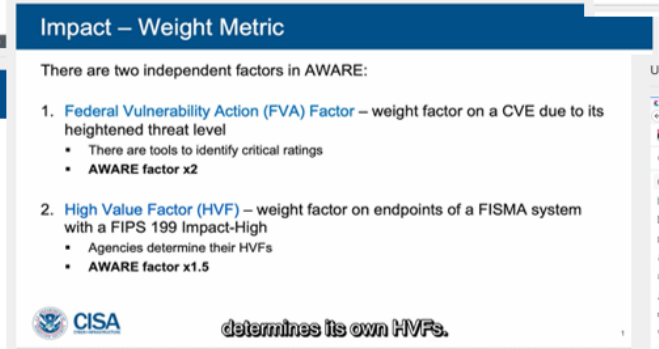
Selected Screen Captures from the Videos

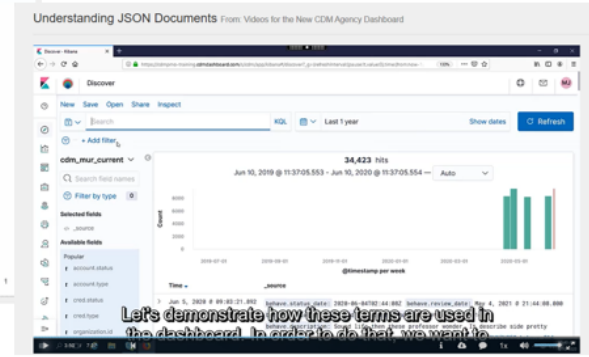










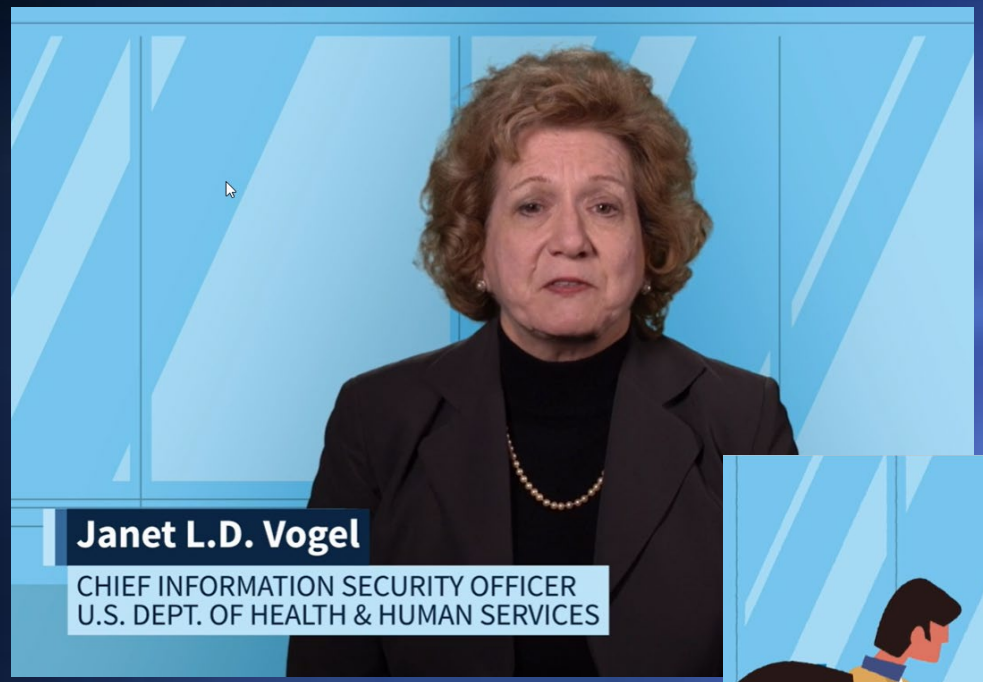


Entry 3:

https://vimeo.com/user9017396/review/430780171/931ff9e94a

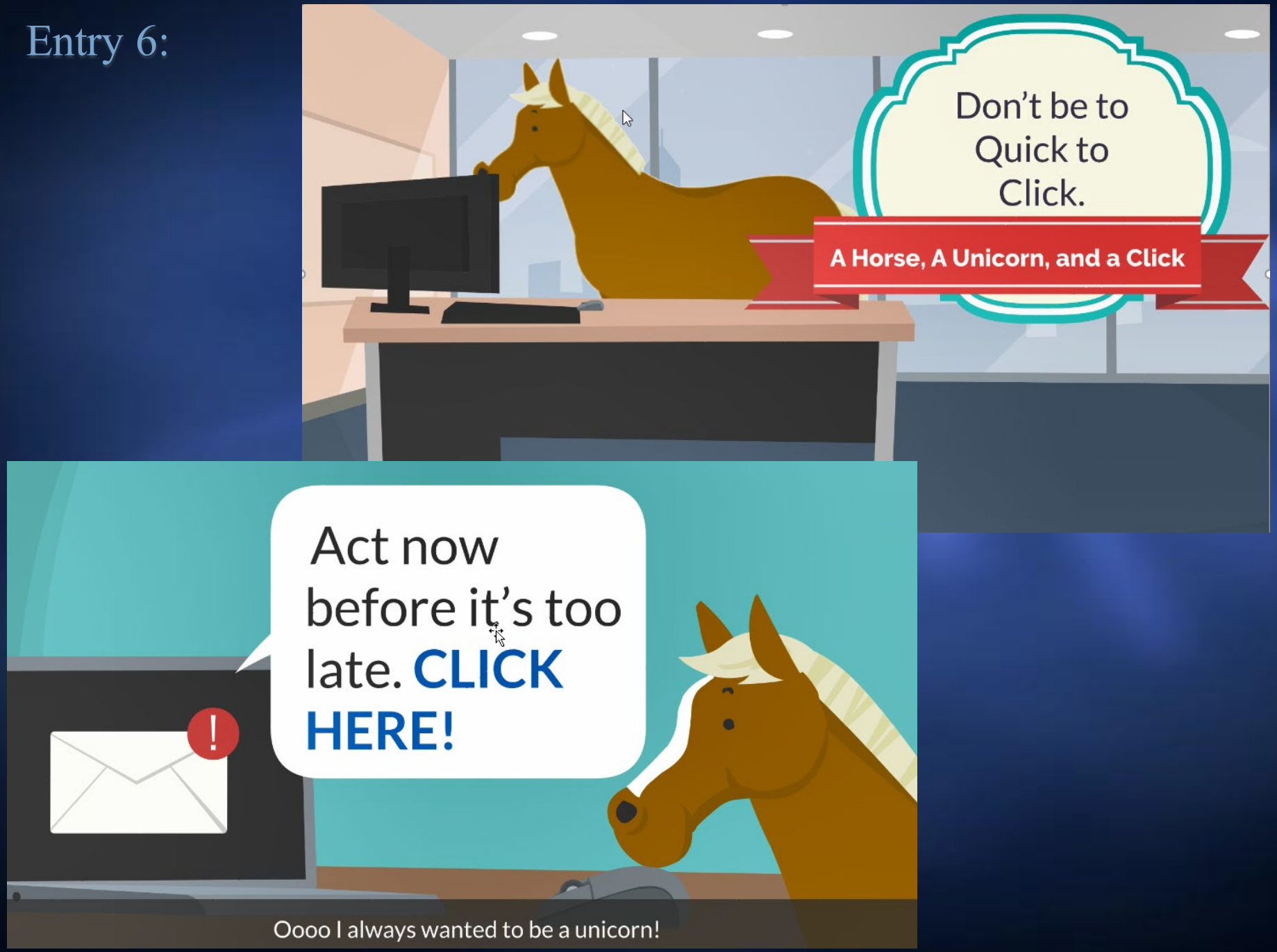
Entry 4: https://vimeo.com/441125214

Entry 5:



Link to Video

Entry 6:

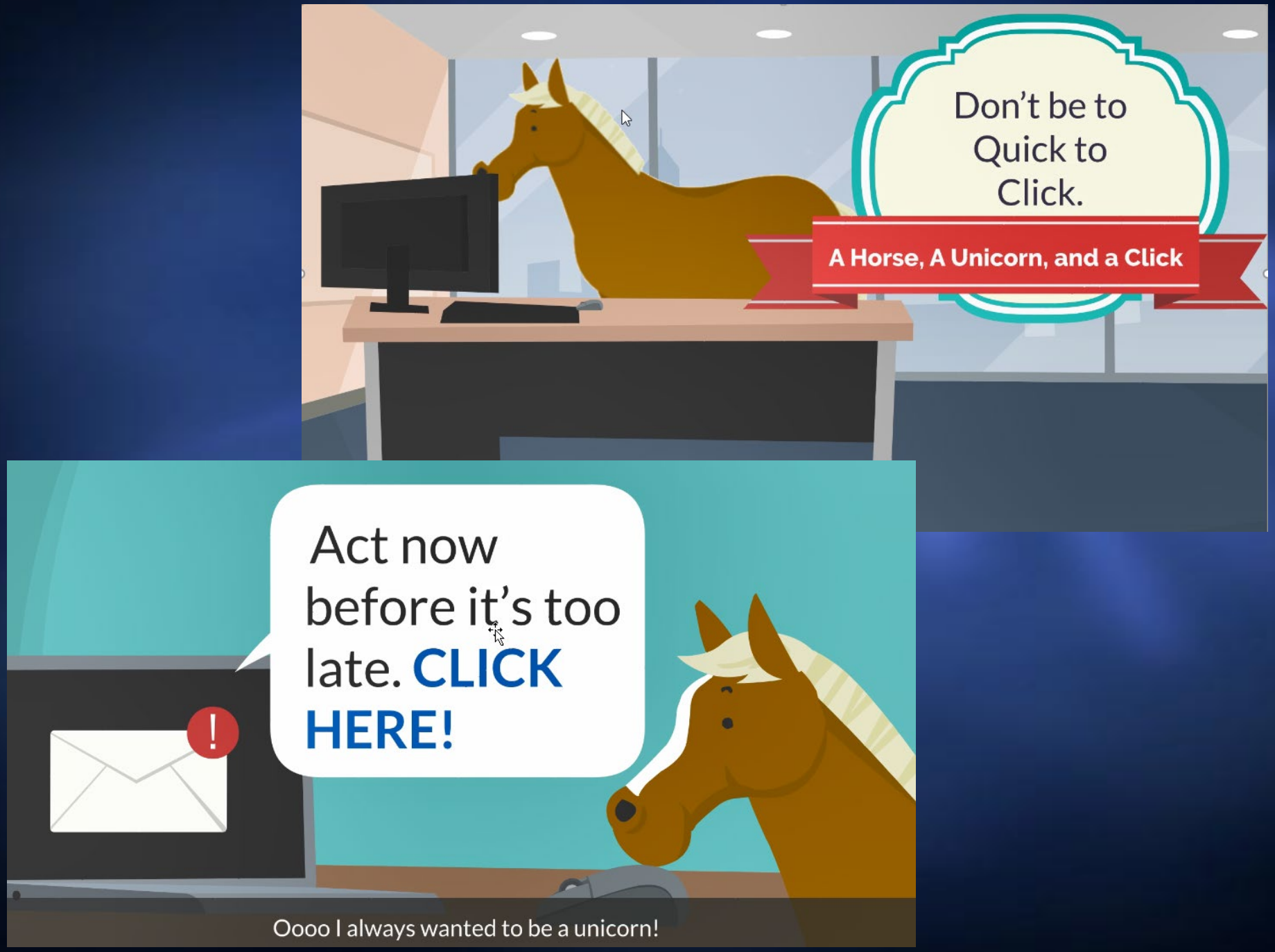

Don't be to Quick to Click.
A Horse, A Unicorn, and a Click
Act now before it's too late. CLICK HERE!
Oooo I always wanted to be a unicorn!

For 2020 we hereby award:

INFORMATION SECURITY & PRIVACY GROUP (ISPG)
OFFICE OF INFORMATION TECHNOLOGY (OIT)
CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

the honor of being selected as the

Security Video Contest Winner!


Don’t be to Quick to Click.
A Horse, A Unicorn, and a Click
Act now before it’s too late. CLICK HERE!
Oooo I always wanted to be a unicorn!

Website Entries (5)

Entry 1: http://www.mekabay.com/cyberwatch/index.htm

CYBERWATCH

Practical advice for novices and families on protecting themselves and their children against harm on the Internet.

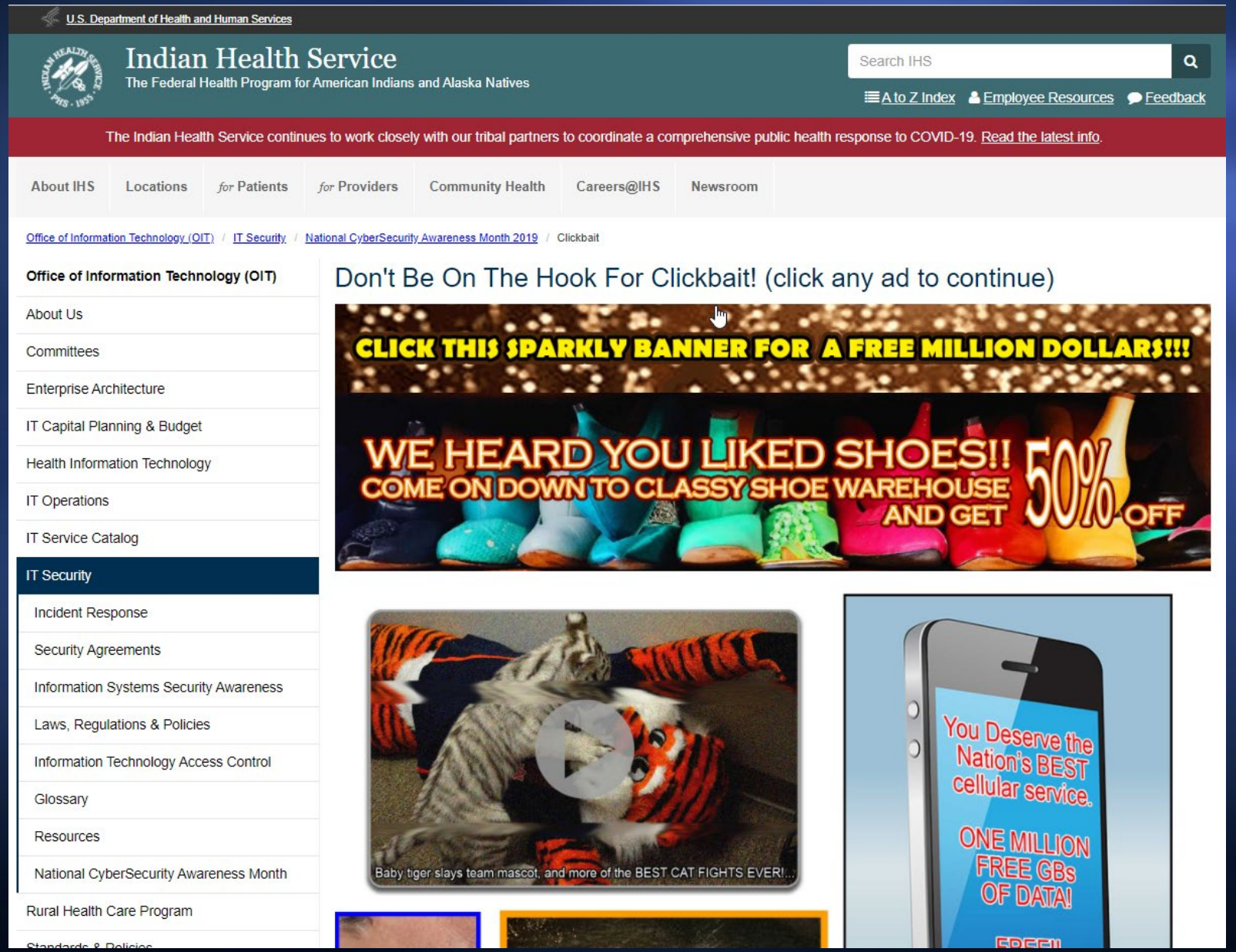
Home Page
Contact info
Courses
CV
Cyberwatch
Ethics
Fun
InfoSec Perception
IYIR
Methods
NetworkWorld Archive
Opinion
Ops Mgmt
Overviews
Security Mgmt

QuickLinks:

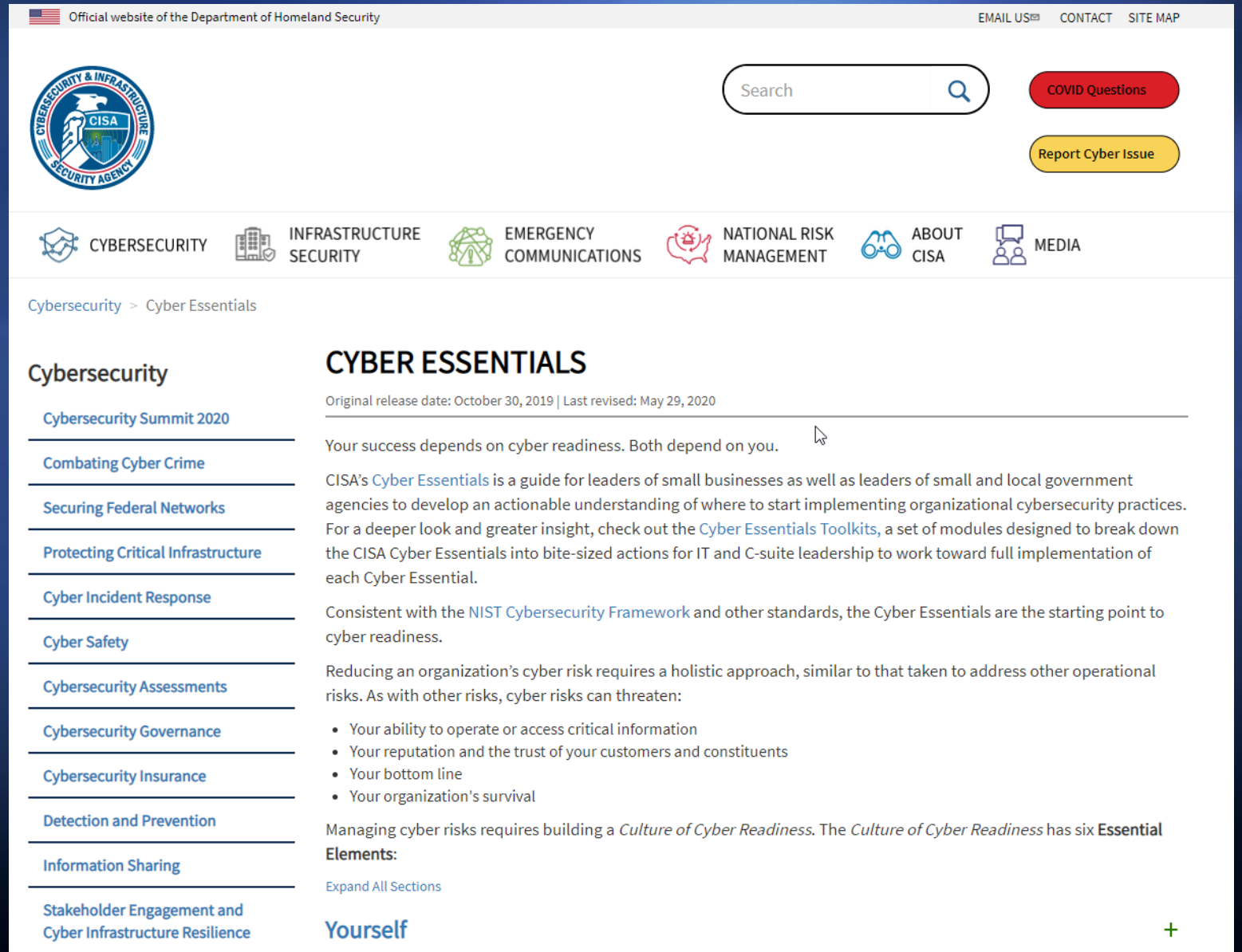
- 5 Ways to Recognize an Acting or Modeling Scam
- 10 Tips to Protect Yourself from Identity Theft
  11 Ways to Prevent Identity Theft While Traveling
- A Guide to Protecting Children's Privacy Online
- Anti-Fraud Resources
- Cyber-Safety for Everyone: from Kids to Elders
- How to Keep Your Children Safe Online
- How to Prevent Child Identity Theft
  How to Spot an Internet Dog Scam
- Identity Theft Protection as a Benefit
- Internet Safety for Teens, Kids, and Students
- Internet Safety: A Guide to Safe Online Shopping for Seniors
- Introduction to Cyber Security and Data Protection
- Million Mile Secrets guide for protecting your child's identity while traveling
- Online privacy: myth or reality?
- Practical Cyber-Safety Tips
- Practical Cyber-Safety Tips Large-Print
- Practical Guide to Help Prevent Elder Financial Fraud
- Protecting Children's Privacy Online
- Protecting Yourself Against Identity Theft & Fraud
- Quick Guide to Safe Online Shopping
- Reducing Privacy Risks of Using Facebook
- Tax Identity Theft: Protecting Your Credit and Finances
- The College Student's Guide to Internet Safety
- The Definitive Guide to Internet Privacy & Online Security
- The Lifecake Guide to Internet Safety & Privacy for Kids (And Parents)
- The Privacy Professor's Website
- The Post-Burglary Guide: What to Do After a Thief Strikes Your Home
- Teen Internet Safety: A Parent's Guide
- The solo traveler's guide to keep you and your cards safe
- Tips to Prevent Senior Scams
- Top Internet Scams Targeting the Elderly
- Ultimate Internet Safety Guide for Seniors
- Ultimate Online Shopping Safety: The Consumer's How-To Guide
  Working Well with Contractors: 15 Questions that Prevent Fraud & Ensure Satisfaction

Cyber-Safety for Everyone: from Kids to Elders *(PDF)*

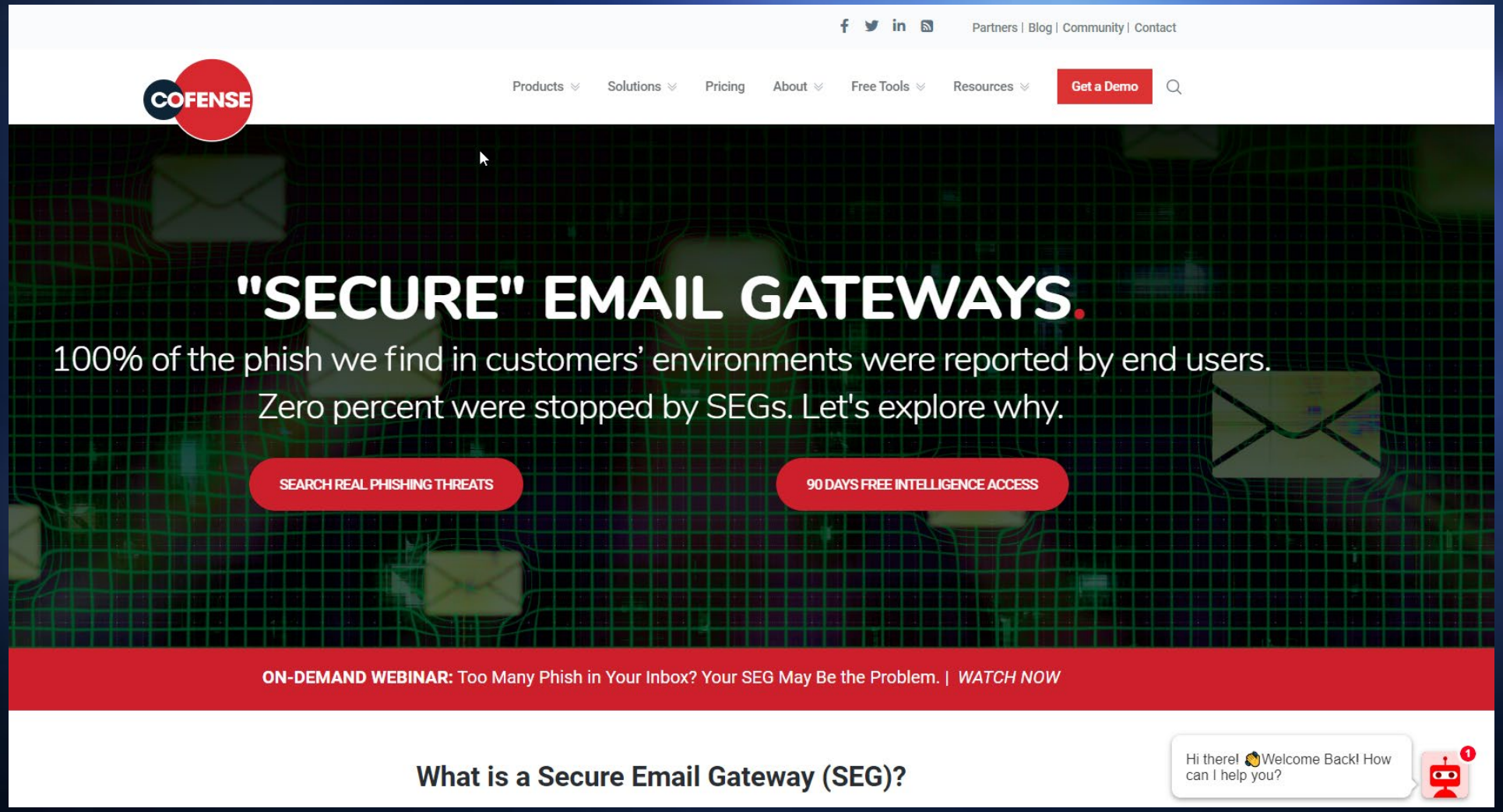
Entry 2: https://www.ihs.gov/oit/security/ncsam2019/clickbait/



Entry 3: https://www.cisa.gov/cyber-essentials and https://www.cisa.gov/publication/cyber-essentials-toolkits



Entry 4: https://cofense.com/what-is-a-seg/



Entry 5:

U. S. Department of Health & Human Services | Contact Us

NIH National Institutes of Health
Office of the Chief Information Officer

Search

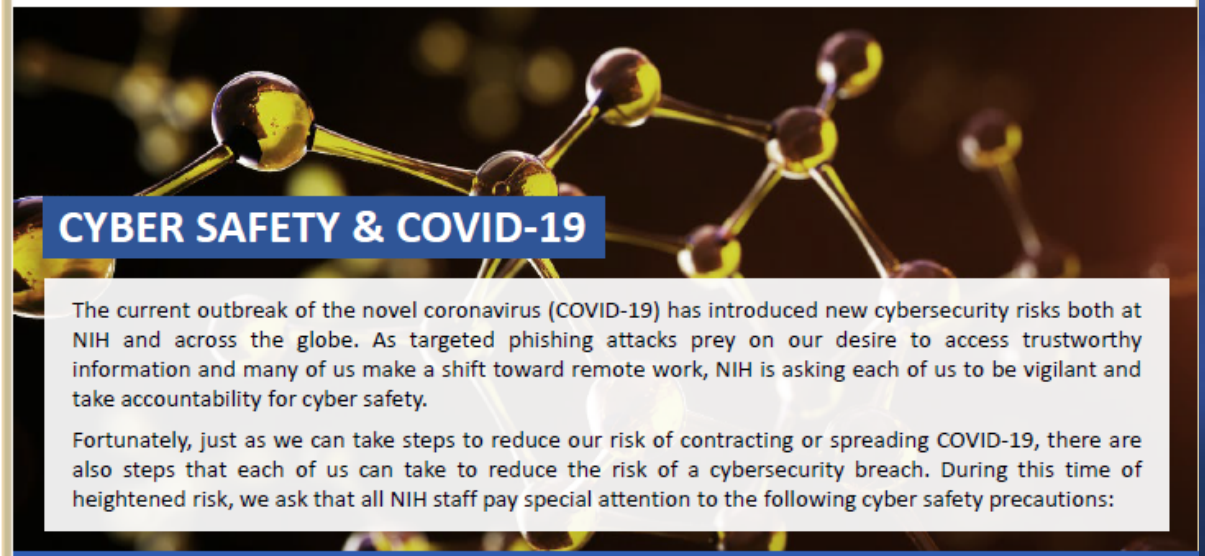
IT Governance & Policy | IT Budget | Project Management | About Us

Information Security

COVID-19 is an emerging, rapidly evolving situation.

Get the latest public health information from CDC: https://www.coronavirus.gov
Get the latest research information from NIH: https://www.nih.gov/coronavirus

Cyber Safety Awareness Campaign – Cyber Safety & COVID-19



The current outbreak of the novel coronavirus (COVID-19) has introduced new cybersecurity risks both at NIH and across the globe. As targeted phishing attacks prey on our desire to access trustworthy information and many of us make a shift toward remote work, NIH is asking each of us to be vigilant and take accountability for cyber safety.

Fortunately, just as we can take steps to reduce our risk of contracting or spreading COVID-19, there are also steps that each of us can take to reduce the risk of a cybersecurity breach. During this time of heightened risk, we ask that all NIH staff pay special attention to the following cyber safety precautions:

What steps can I take to stay cyber safe?

Be vigilant.

Know how to confidently identify, avoid, and report phishing attempts related to the outbreak of the novel coronavirus.

Learn more about COVID-19 phishing attacks.

For 2020 we hereby award:

INDIAN HEALTH SERVICE,
OFFICE OF INFORMATION TECHNOLOGY (OIT),
DIVISION OF INFORMATION SECURITY

the honor of being selected as the

Security Website Contest Winner!

The Indian Health Service continues to work closely with our tribal partners to coordinate a comprehensive public health response to COVID-19. Read the latest info.

Don't Be On The Hook For Clickbait! (click any ad to continue)

Thanks to all
who submitted entries!

A special thanks to our
judges!