NIST CYBER

fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

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

June 22, 2020

Meeting the Need: Training that Rocks

- Kimberly Hemby
- Kassy LaBorie
- Lisa Plaggemier
- Ashley Rose

Host: Sarah Moffat

AGENDA

1:00 – 1:05	Welcome from NICE Director	Rodney Petersen
1:05 – 1:10	Vision & Theme for 2020 Summer Series	Sarah Moffat, Program Chair
1:10 – 1:15	Webinar housekeeping, Key Updates	Sarah Moffat, Program Chair
1:15 – 2:00	Meeting the Need, Training that Rocks Panel	

Moderated by Sarah Moffat

1:20 – 1:30	Kassy Laborie, *Virtual Classroom Master Trainer, Author, & Speaker*
1:30 – 1:40	Lisa Plaggemier, *Chief Strategist with MediaPRO: Cybersecurity & Privacy*
1:40 – 1:50	Kim Hemby, *Cybersecurity, Privacy Awareness & Training Team Lead*
1:50 – 2:00	Ashley Rose, *CEO & Founder at Living Security*

2:00 – 2:15	Audience participation/Q&A	
2:15 – 2:23	Closing Remarks	Speakers
2:23 – 2:25	Closeout, Reminder for next session	Sarah Moffat, Program Chair

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

FISSEA 2020: Summer Series

fissea FEDERAL 2020

Summer Series

- Welcome
- Thanks to
  - Rodney Petersen
  - FISSEA 2020 Program Committee
  - Amber Crutchfield, Keri Bray
  - NICE Program Staff
  - Panelists
- Vision/Theme for FISSEA 2020
- Next Session: July 20, 2020
- Save the Date: FISSEA 2021 – June 16-17, 2021
- FISSEA Cybersecurity Awareness & Training Innovator Award, Nominations due Aug 7, 2020
- FISSEA Security Awareness & Training Contest, Nominations due July 24. 2020

NIST CYBER

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Save the Date

FISSEA 2021

June 16-17, 2021
NIST Campus
Gaithersburg, Maryland

Webinar Information

Q/A Panel

- Communicate with Moderator and Panelists using the Q/A panel
- Chat will be turned on during the Q/A session at the end and during one panelist presentation

Polls

- Polls throughout the session (starting now!)
- Responses will be collected and used to improve future sessions
- Some responses will be shared with panelists

Recording

- Session will be recorded and made available on a date/location TBD

Meeting the Need: Training that Rocks

The world is changing before our eyes – no doubt about it. If we, as learning and development leaders, are to keep up with the required changes, trends, and learner needs, we've also got to make some big changes. We've invited four incredibly high-impact learning and development leaders to talk with us about how we can take our training development and delivery to the next level. In this session, experts from both cybersecurity and training development are going to discuss how you can change your cybersecurity awareness program to be next-level, high-impact, and more relevant.

Our moderator

Sarah Moffat
FISSEA 2020 Program Chair, Enterprise Cybersecurity Awareness & Communication

Meet the panelists

Kimberly Hemby
Cybersecurity, Privacy Awareness & Training Team Lead

Kassy LaBorie
Virtual Classroom Master Trainer, Author, & Speaker with Kassy LaBorie Consulting, LLC.

Lisa Plaggemier
Chief Strategist with MediaPRO: Cybersecurity & Privacy

Ashley Rose
CEO & Founder at Living Security

NIST CYBER

Next Webinar
July 20, 2020 | 1pm– 2:30pm EST
CyberRap, Music, Dance, Gamification, and Fun in Cybersecurity Training

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

Meeting the Need: Training that Rocks

Sarah Moffat

Sarah Moffat
FISSEA 2020 Program Chair, Enterprise Cybersecurity Awareness & Communication

Sarah Moffat is a talent development expert, and both an 'ideas person' and strategic initiator. Sarah's passion is working with people, strengthening the culture of learning and leadership development, and finding new ways to engage, empower, and excite learners. Sarah has directed learning solutions that have reached over a half-million learners and developed thousands of training modules and ancillary products covering topics from cybersecurity to customer service. Sarah has more than 15 years in talent development, a B.S. in Psychology, and is an Independent Certified Coach, Trainer, and Speaker with the John Maxwell Team.

Follow me on IG and FB @LeadingLadiesCo
LinkedIn: http://www.linkedin.com/in/sarahcmoffat

Meeting the Need: Training that Rocks

Kassy LaBorie
Virtual Classroom Master Trainer, Author, & Speaker with Kassy LaBorie Consulting, LLC

Kassy LaBorie

My name is **Kassy LaBorie**, and I'm the founder and principal consultant at Kassy LaBorie Consulting, LLC. I am a virtual classroom master trainer, that is, I specialize in developing trainers to be engaging and effective when facilitating programs in platforms such as Zoom, WebEx, Adobe Connect, and more. I have worked with many Fortune 500 firms in a wide range of industries and sectors, including hospitality, pharma, energy, government, NGOs, non-profits, and more.

I also train and coach producers, the virtual classroom trainer's partner in effective facilitation, as well as instructional designers tasked with creating or converting content for virtual classroom delivery. And I advise learning and development leaders in areas like virtual classroom strategy, technology selection, logistics, and more.

In short, I have over 20 years of experience in passionately helping organizations, learning teams, and training professionals successfully move to the virtual environment. See my programs page to learn more.

Prior to this, I was an independent master virtual trainer, a Microsoft software trainer, and a senior trainer at WebEx, where I helped build and deliver training at the WebEx University.

I have co-authored *Interact and Engage! 50+ Activities for Virtual Training, Meetings, and Webinars* (ATD Press, 2015).

VIRTUAL CLASSROOM MASTER TRAINER

WHAT I DO

Strategy, Delivery, Design, Production, Technology

- Train the Virtual Trainer
- Webinars
- Workshops
- Consulting

KassyConsulting.com | kassy.laborie@gmail.com

5 Keys *for* Effective Virtual Classroom Training

TECHNOLOGY

TRAINING DELIVERY

INSTRUCTIONAL DESIGN

PRODUCTION

PARTICIPANTS

TECHNICALLY SOUND

It works in your environment and you know how to use it.

USER FRIENDLY

Participants can join. They can connect to and use it with ease.

CLEAR AUDIO

The audio connection works. Everyone can talk and be heard.

Platform Skillz

Engaging Voice

Active Participants

THE VIRTUAL TRAINER'S MANTRA

SAY

What did
I just say
that **YOU** could
have said?

DO

What did
I just do
that **YOU** could
have done?

Connect with me! on LinkedIn

VIRTUAL TRAINING HERO TIP #2

Look great on webcam!

Smile. And the participants will smile too.

Pay attention to the lighting. Do not be backlit, side-lit, or screen-lit.

Adjust the webcam angle. Position the lens equal to the forehead.

Look at the participants, not yourself. Don't treat the webcam as a mirror.

Create a professional & interesting background. Keep it simple, clear, & organized.

VIRTUAL TRAINING HERO TIP

Create engagement using nonverbal feedback

VIRTUAL TRAINING HERO TIP #3

Use a PRODUCER!

https://www.linkedin.com/in/kassylaborie/

Meeting the Need: Training that Rocks

Lisa Plaggemier

Lisa Plaggemier

Chief Strategist with MediaPRO: Cybersecurity & Privacy

Lisa is Chief Strategy Officer at MediaPRO, a leading provider of data privacy and security training solutions. She is a trailblazer in security training and awareness, a prominent security influencer, and a frequent speaker at major events. She uses her deep and diverse experience to fuel an innovative approach that engages learners and influences behavior.

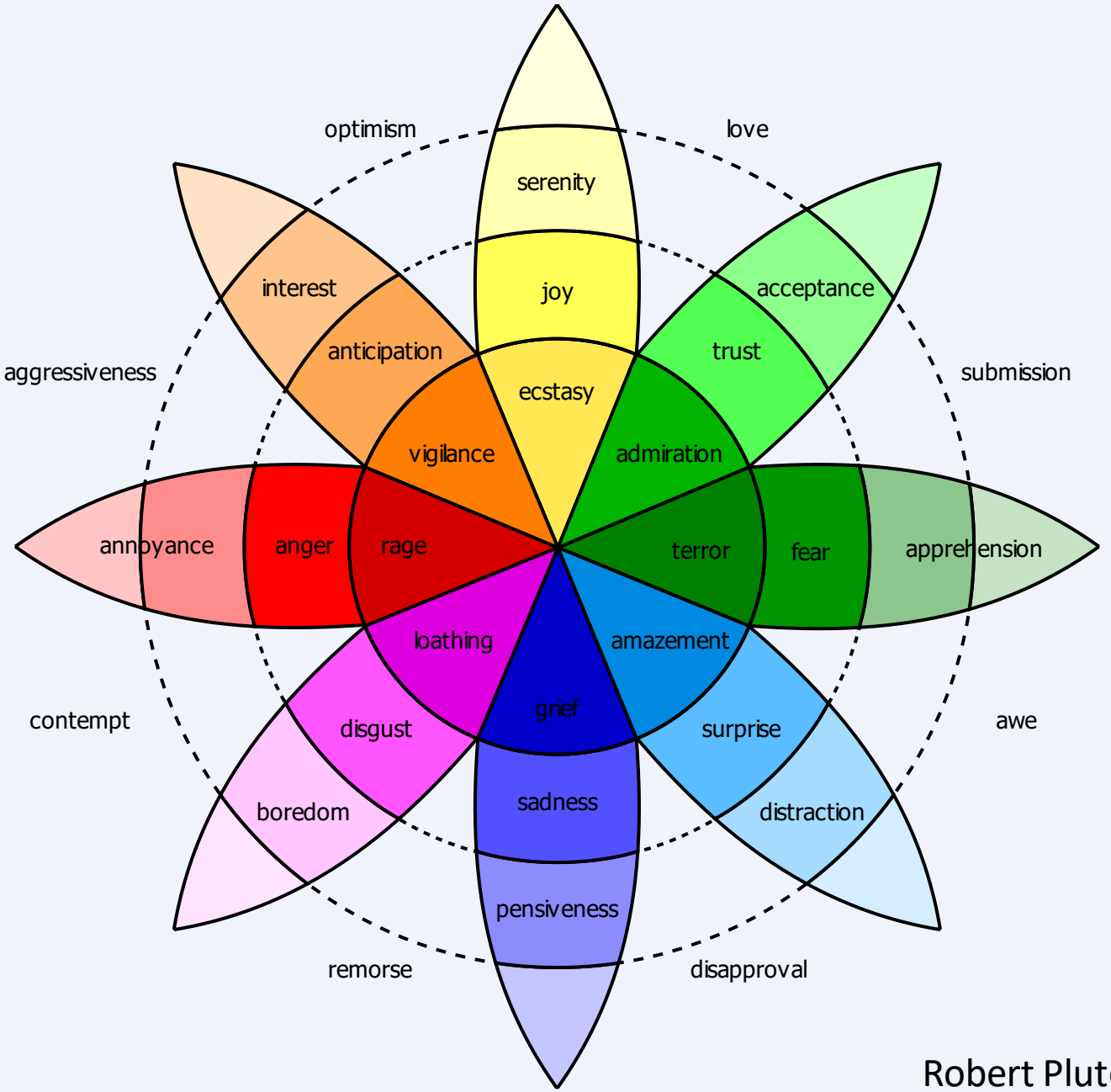
Lisa has worked as an international marketer with Ford Motor Company, Director of Security Culture, Risk and Client Advocacy for CDK Global, and Chief Evangelist at InfoSec. She is a University of Michigan graduate (Go Blue!) and recently traded her brisket in Austin, Texas for fresh salmon in Seattle, Washington.

TRAINING THAT ROCKS

MediaPRO
Cybersecurity & Privacy Education

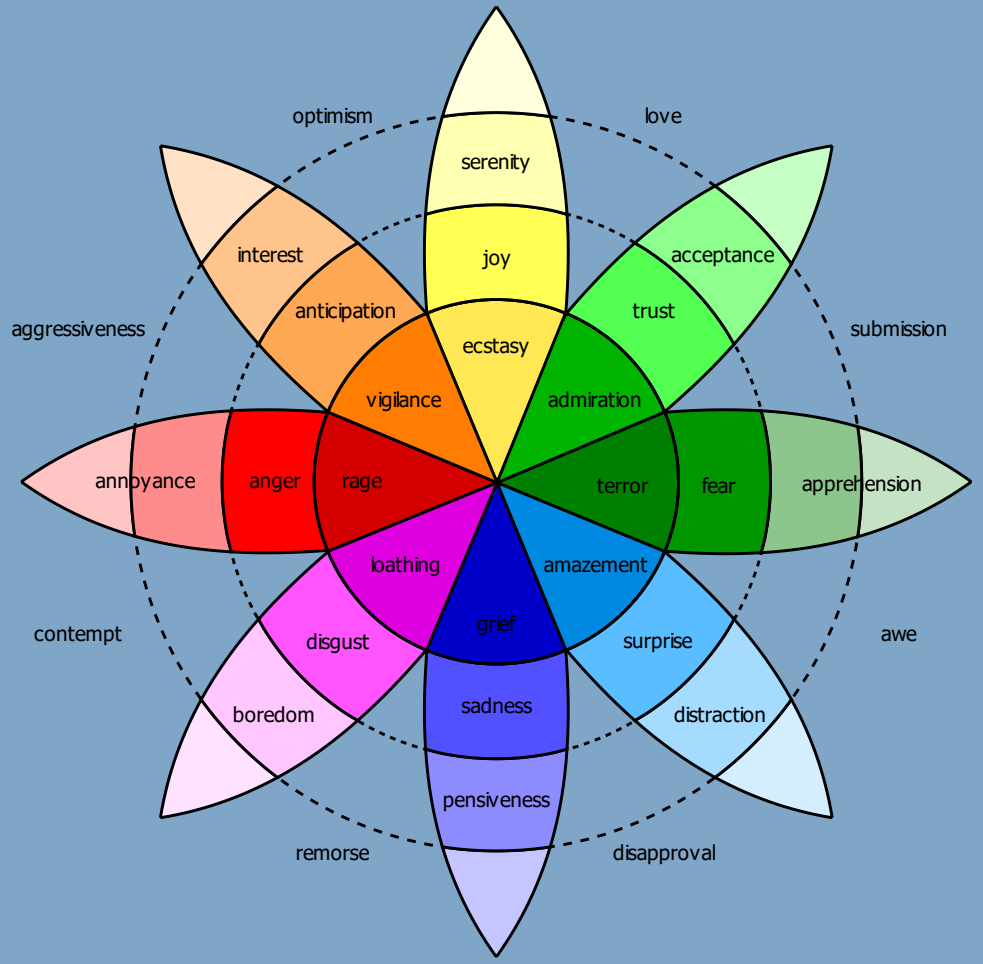
People are irrational and they usually make decisions that have nothing to do with facts. And yet we spend most of our time improving our facts and very little concerned with the rest.

Seth Godin



Robert Plutchik, *Wheel of Emotions*

Plutchik's wheel of emotion



trust goes from acceptance to admiration

fear goes from timidity to terror

anticipation goes from interest to vigilance

Anti-Phishing Essentials

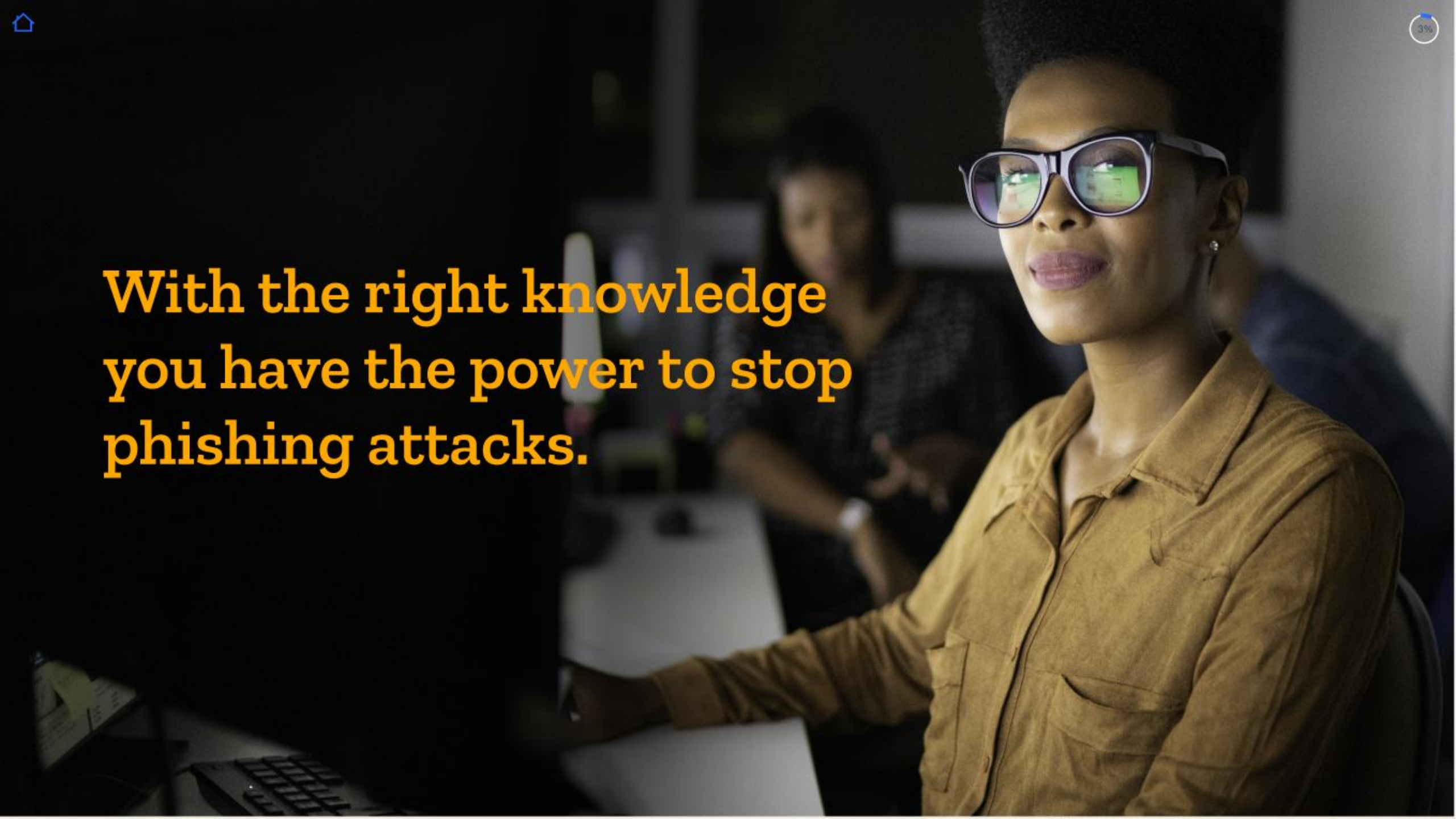
What you need to know about phishing

What you'll learn

- Explore how phishing scams work
- Recognize the risk they pose to our organization
- How to identify the warning signs of phishing attacks
- How to handle a phishing scam

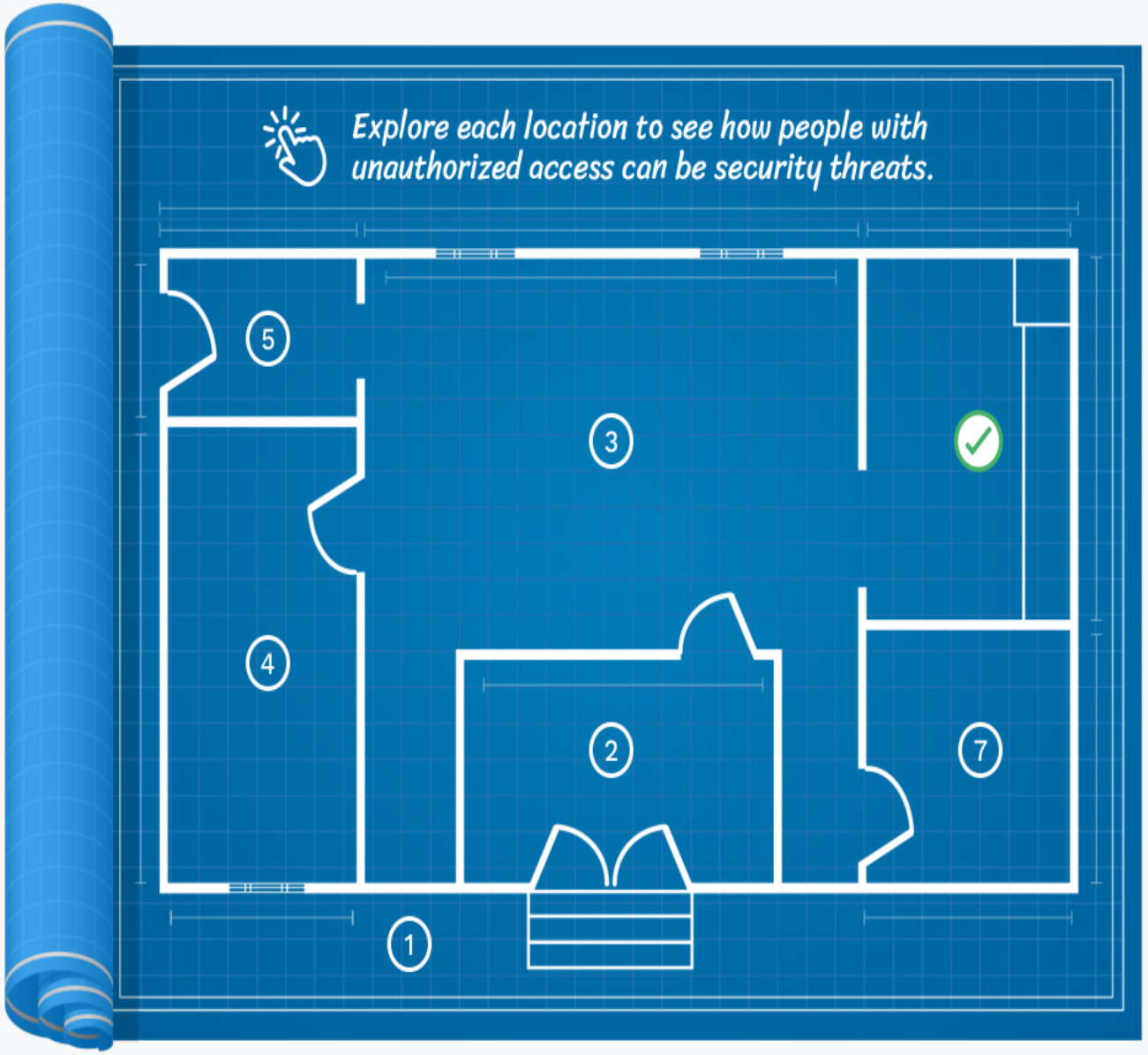
Estimated time :18

Scroll to continue


With the right knowledge
you have the power to stop
phishing attacks.

How to think like a thief

Where we see desks, meeting rooms, and supplies—a criminal sees opportunity.

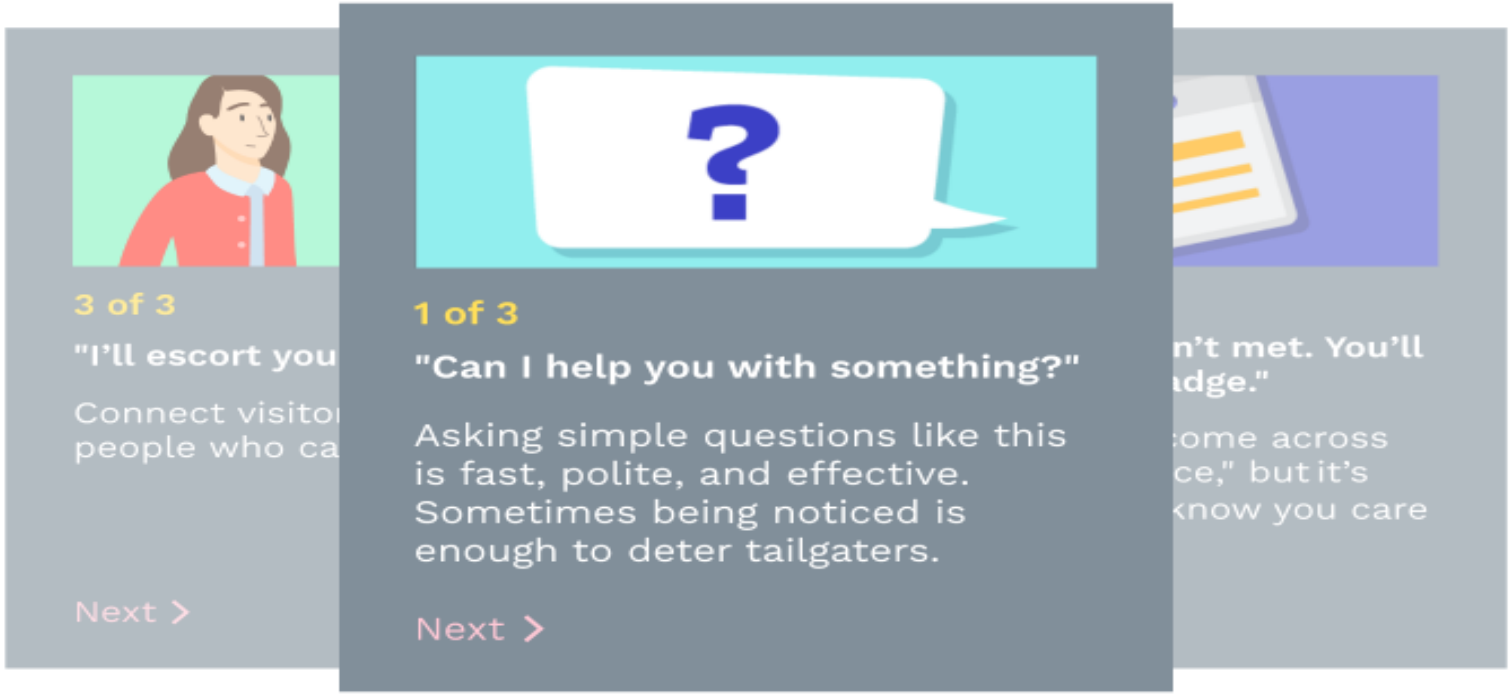


Head off tailgating

"Tailgating" is when someone follows you through a secure door without using their ID badge. It happens all the time, mostly because we hold the door to be polite.

But, it's a bigger security risk than you may realize.

Try some of these strategies to stop tailgaters without being rude or confrontational.



Free Stuff!

https://www.mediapro.com/free-course-stay-secure-work-from-home/

https://www.mediapro.com/this-is-ccpa-jeopardy/

Get In Touch

https://www.linkedin.com/in/lisaplaggemier

Lisa.Plaggemier@mediapro.com

MediaPRO

MediaPRO is the trusted partner security and privacy professionals rely on to help meet their goals of reducing risk and changing employee culture for the better.

Message by message, action by action, employee by employee, we engage and inspire employees to protect each other and their organizations. What we offer is configurable so you can make it your own, engaging so your people want to learn, and proven so you know it works.

Meeting the Need: Training that Rocks

Kimberly Hemby

Kimberly Hemby

Cybersecurity, Privacy Awareness & Training Team Lead

Kim, has over 13 years of information technology experience within the state, federal government sectors, as well as private industry. She's currently working at the Department of Health and Human Services (DHHS), Centers for Medicare and Medicaid Services (CMS) as the Cybersecurity and Privacy Training Lead for the Chief Information Security Officers (CISO) office. Kimberly has dedicated her career to the safety and privacy of millions of Americans Personally Identifiable Information (PII), Protected Healthcare Information (PHI), and Federal Tax Information (FTI). This information is of great interest to bad actors attempting to data mine or exploit our data for personal, political, and/or usually financial gain.

Her expertise in devising innovative cybersecurity training and leveraging well considered risk to optimum outcome is well documented.
Kimberly received BS degree from University of Baltimore. In her spare time, she mentors' middle and high school girls in Baltimore City.

5 CARAT TRAINING

Meeting the Need:

Centers for Medicare & Medicaid Services (CMS) Training that Rocks

By: Kimberly Hemby:
CMS Cybersecurity & Priv

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

1 NEW HIRE ORIENTATION

Redesigned New Employee Orientation cybersecurity and privacy training for Zoom to keep CMS hiring on-track

For Official Use Only (FOUO)

Risk

Hacked Passwords

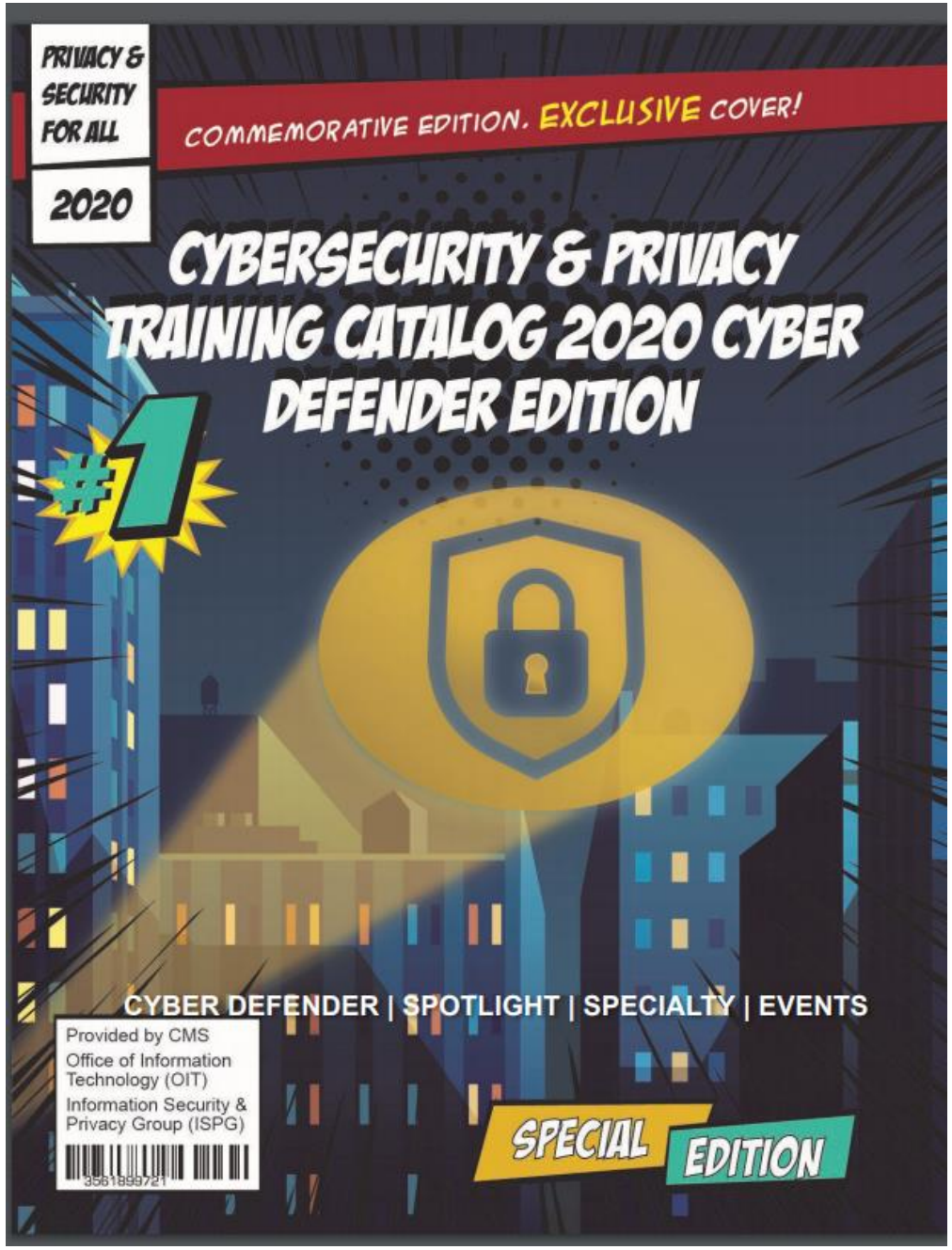
Social Engineering

Insider Threats

Cyber Attacks

2 TRAINING CATALOG

Cybersecurity and Privacy Training Catalog: Featuring Cyber Defenders and NICE Framework course mappings

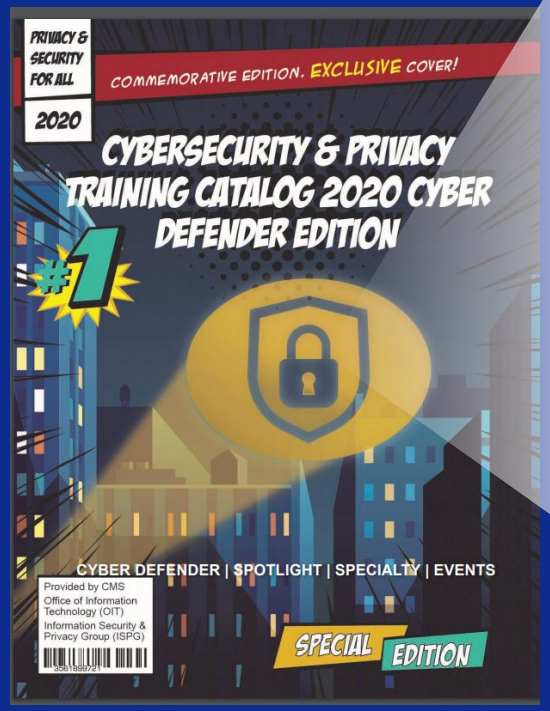


2 TRAINING CATALOG

Cybersecurity and Privacy Training Catalog: Featuring Cyber Defenders and NICE Framework course mappings

CAST OF CMS CYBER DEFENDERS

CATALOG NICE MAPPING EXAMPLE



All About the CMS Acceptable Risk Safeguards (ARS) 3.1

This webinar provides additional clarification on the ARS which was released January 31, 2017. Learn how the mandatory baseline controls align with NIST and how controls can be implemented to achieve cost-effective, risk-based security that supports organizational mission and business requirements. A case study by a Medicare Administrative Contractors (MACs) will be provided on how a defined set of controls have been incorporated into a mandatory baseline to meet their specific requirements.

Target Audience: This webinar is designed to provide useful information to ISSOs, Business Owners, System Owners and other stakeholders in implementing the CMS ARS requirements.

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	SECURELY PROVISION	PROTECT AND DEFEND	ANALYZE
Role ID (OPM Code)	711, 712, 722, 804	441, 451, 461	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 541	141, 121, 111, 112, 131, 132, 151

3 ROLE-BASED TRAINING

Cyber Training Videos: a collection of on-demand, online 24/7, entertaining micro learning lessons

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

Cyber Training Videos

Adaptive Capabilities Testing
NICE Role ID
Download Transcript

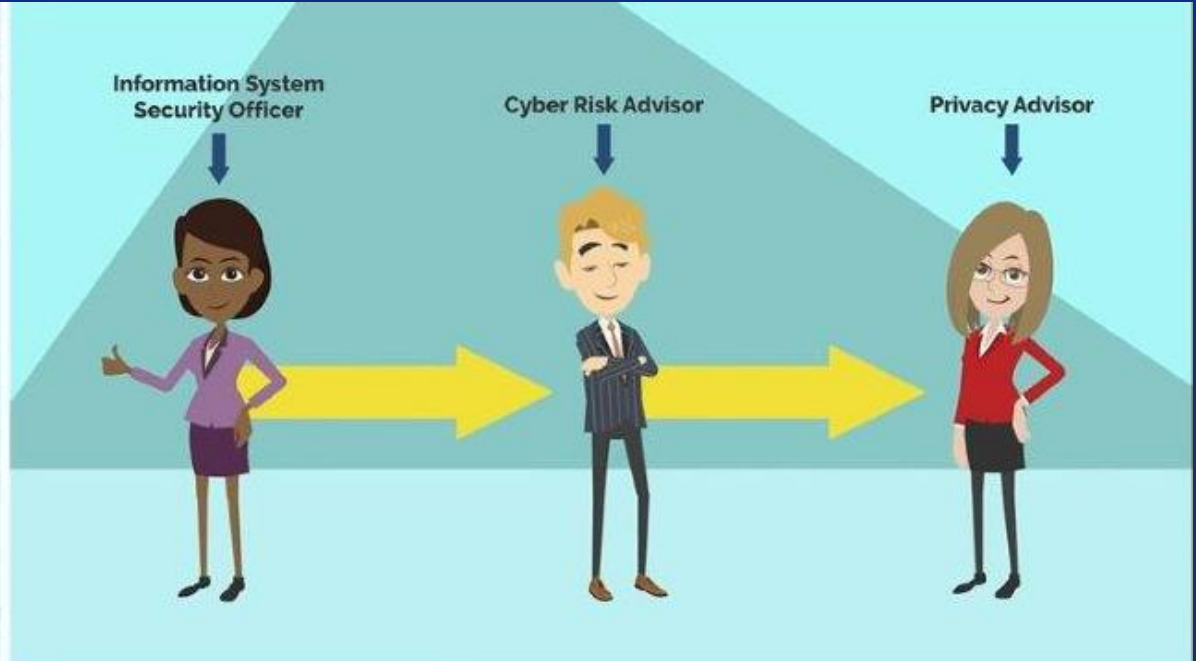
Privacy Impact Assessment
NICE Role ID
Download Transcript

ISSO Reports

3

ROLL-BASE TRAINING – Privacy Impact Assessment Micro Learning Video

It went smoothly. PIAs are needed before a new system goes into operation or when a program change requires a privacy impact review.



The CRA may additionally consult with a Privacy Advisor, who is also part of the Information Security and Privacy Group.

Navigator Tool - Used to find role-based training mapped to NICE roles

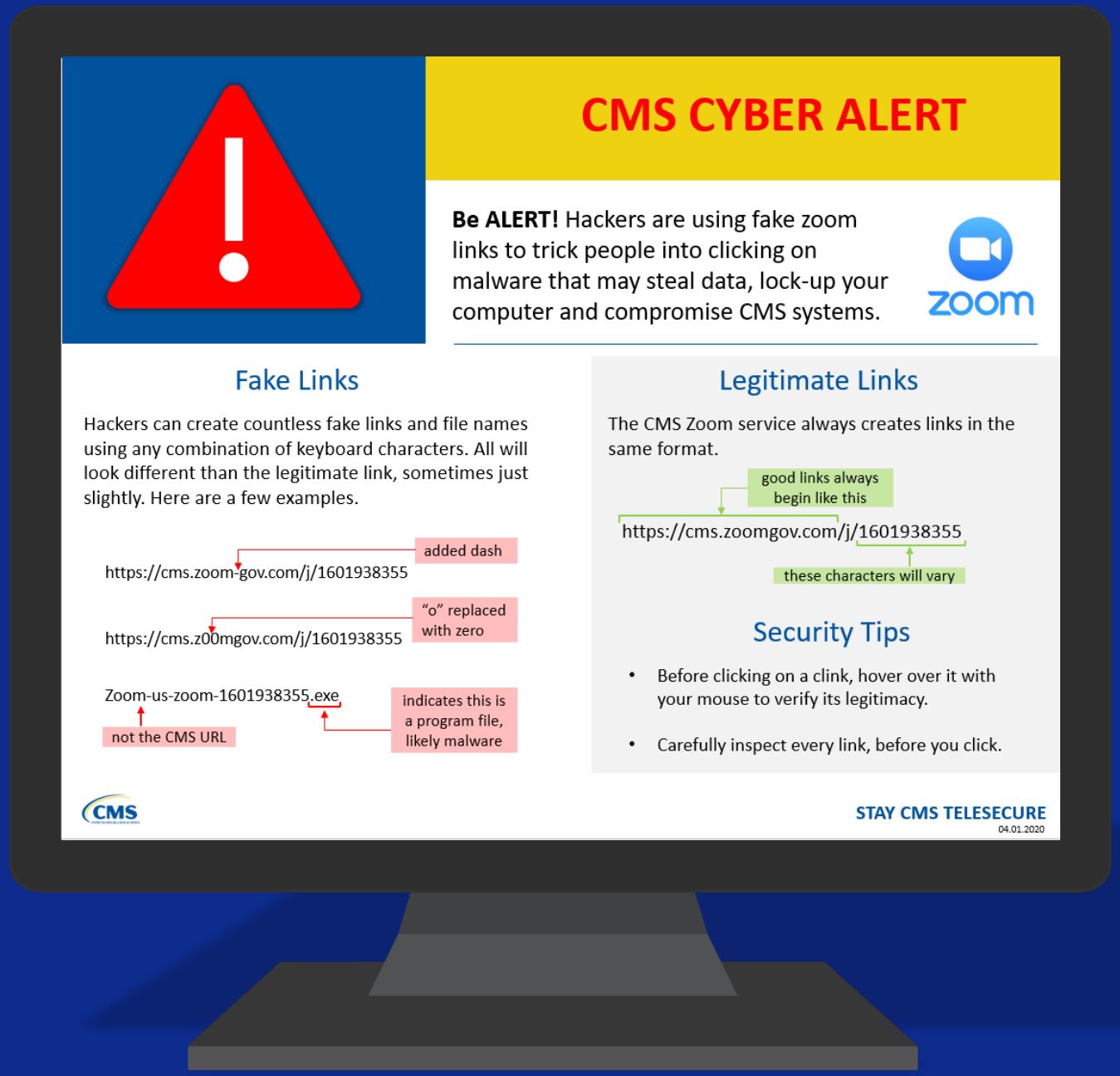
Role-based Training (RBT) Navigation Tool

This navigation tool contains a collection of cybersecurity and privacy training available from industry and government. Courses are mapped to the NIST NICE framework to provide a quick method to identify role-aligned training opportunities.

Nice Category	Skill	NICE Role ID	Courseware	Books	FedVTE	CMS Training	SANS
Securely Provision (SP)			X	X	X		
	Risk Management (RSK)	611, 612	X	X			
	Software Development (DEV)	621, 622	X	X			
	Systems Architecture (ARC)	651, 652	X	X			
	Technology R&D (TRD)	661	X	X			
	Systems Requirements Planning (SRP)	641	X	X			
	Test and Evaluation (TST)	671	X	X			
	Systems Development (SYS)	631, 632	X	X			
Operate and Maintain (OM)			X	X	X	X	X
	Data Administration (DTA)	421, 422	X	X			
	Knowledge Management (KMG)	431	X	X			
	Customer Service and Technical Support (STS)	411	X	X			
	Network Services (NET)	441	X	X			
	Systems Administration (ADM)	451	X	X			
	Systems Analysis (ANA)	461	X	X			
Oversee and Govern (OV)			X	X	X	X	X
	Legal Advice and Advocacy (LGA)	731, 732	X	X			
	Training, Education, and Awareness (TEA)	711, 712	X	X			
	Cybersecurity Management (MGT)	722, 723	X	X			
	Strategic Planning and Policy (SPP)	751, 752	X	X			
	Executive Cyber Leadership (EXL)	901	X	X			
	Program/Project Management (PMA) and Acquisition	801, 802, 803, 804, 805	X	X			
Protect and Defend (PR)			X	X	X	X	X
	Cybersecurity Defense Analysis (CDA)	511	X	X			
	Cybersecurity Defense Infrastructure Support (INF)	521	X	X			
	Incident Response (CIR)	531	X	X			
	Vulnerability Assessment and Management (VAM)	541	X	X			
Analyze (AN)			X	X	X	X	X
	Threat Analysis (TWA)	141	X	X			

4 SECURITY SPLASH SCREENS:

Provide cybersecurity and privacy tips, just-in-time knowledge, alerts and more. (message pop –up on all CMS computers upon launch)



Security Splash Screen: Example

STAY CMS TELESECURE!

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

You Got This

Help keep the CMS network secure and running in tiptop shape. Follow these telework tips to protect CMS and to optimize availability of shared resources.

Telesecure Check List

- ☑ Avoid using streaming services on your CMS computer
- ☑ "End" WebEx and Zoom sessions when meetings are finished
- ☑ Shut Down your CMS computer daily
- ☑ Be patient transferring large files

Telework Tips

Streaming

Streaming services, such as Spotify or Netflix, can cause the network to slow down. Avoid streaming from your CMS computer to keep the network moving as fast as possible.

Virtual Meetings

Online meeting services are a great resources shared across CMS. When you host a WebEx or Zoom meeting, please be sure to "end" (not just "leave") the session when finished.

Shut Down

At the end of each day, Shut Down your CMS computer from the Windows Start menu. This helps to protect your computer and the network from inactive remote connections.

Transferring Files

Please be patient. Large file transfers to CMS' SharePoint can take longer when connecting from home. Remember, the tortoise wins the race.

Want more information? Visit the CMS Information Security and Privacy Overview here: cms.gov/informationsecurity.

May 2020

5 Phishing Awareness

Micro Training Video Example

5 Phishing Awareness

Questions and Contact Information

Kimberly Hemby, (CMS OIT) Cybersecurity and Privacy Lead
Email: Kimberly.Hemby@cms.hhs.gov
LinkedIn: linkedin.com/in/kimberly-hemby-141b562b

THANK YOU


CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

Meeting the Need: Training that Rocks

Ashley Rose

Ashley Rose

CEO & Founder at Living Security

As the CEO of Living Security, Ashley is passionate about helping companies build positive security cultures. An adaptable problem solver, she is thoughtful and transparent in her approach to running the company and working with clients toward a singular goal: to reduce risk by making security awareness engaging and quantifiable.

Ashley has a Bachelors of Business Administration from the University of Michigan and is a serial entrepreneur with experience designing and managing product lines. After launching her career in the tech industry, she became intrigued by cybersecurity and its accelerating impact. Now Living Security combines that interest with her passions for entrepreneurship and helping people.

NIST CYBER

fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Gone Virtual

Online Training Beyond the Checkbox

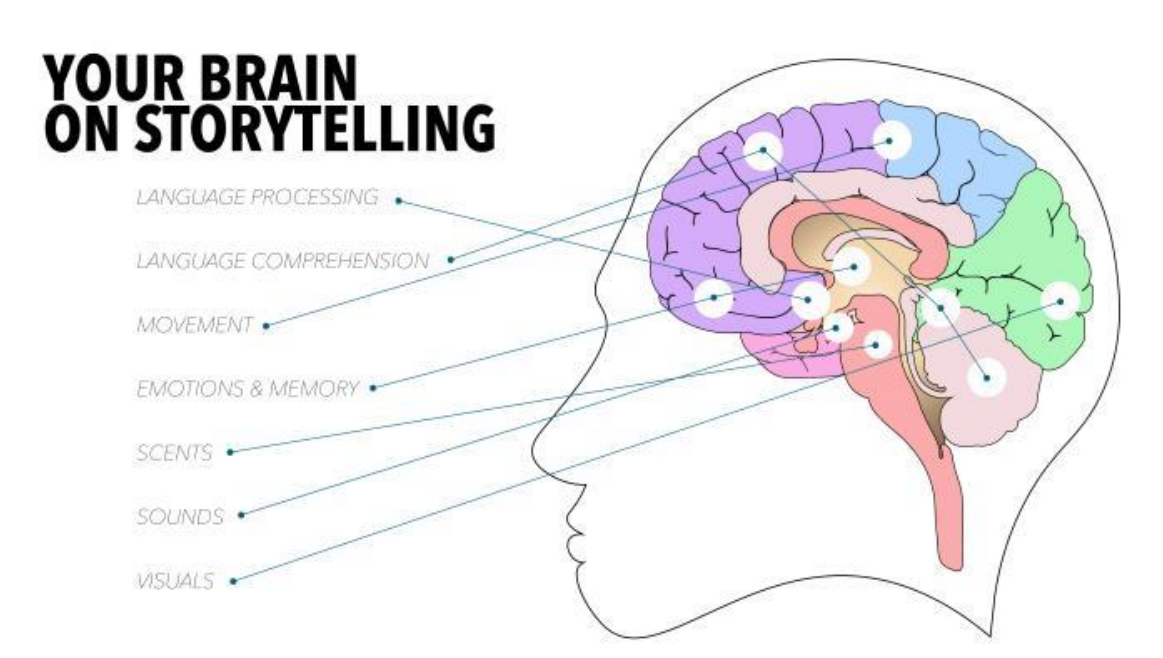
Ashley Rose

June 22, 2020

livingsecurity

SCIENCE TELLS US…

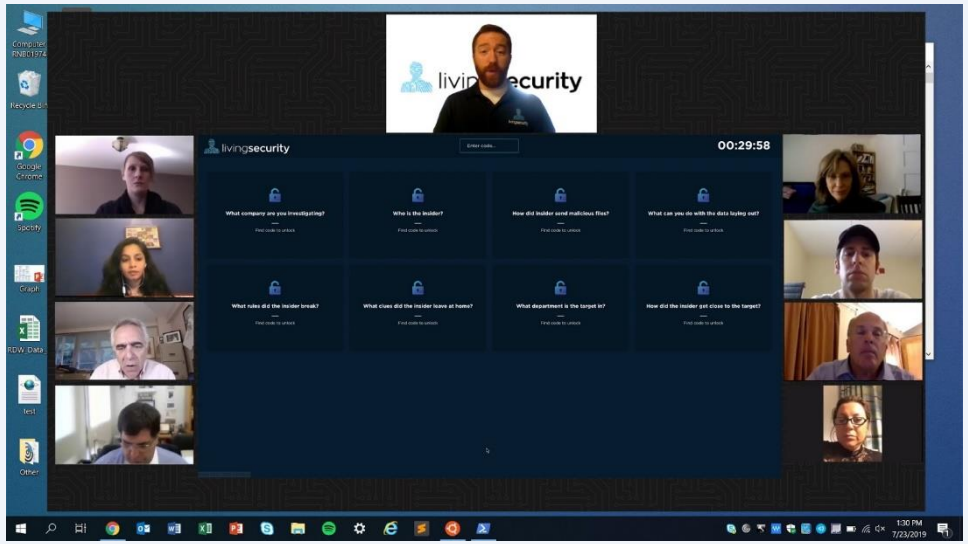
- The brain is 68% more active when having fun!
- Experiential learning = 16X greater retention!
- Gamification techniques:
  - Motivates participants and increases adoption
  - Improves knowledge absorption and retention
  - Makes learning fun!



livingsecurity

WE BELIEVE…

1. Cybersecurity awareness training doesn't have to be boring
2. Engaged learners retain information better, and make fewer mistakes
3. Teams learn better when they learn together, and hold each other accountable
4. One size doesn't fit all in cybersecurity awareness
5. Data, risk analytics, and targeted programs are key to preventing breaches



livingsecurity

DON'T TAKE MY WORD FOR IT!

4.75/5 STARS

"Cyber security training that is more fun than online videos! Interacting with the material in this experience encourages me to remember the material and apply it in my life."

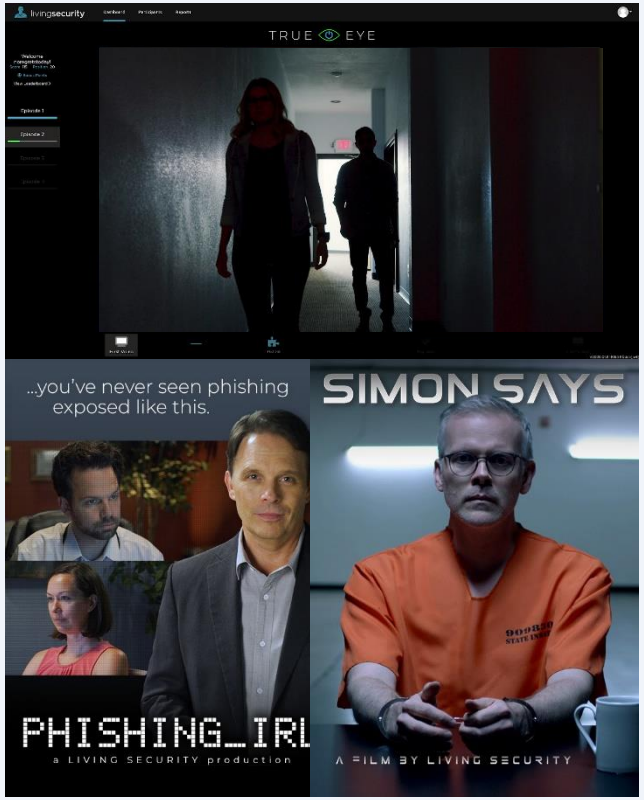
"I enjoyed working as a team. I have to do PHI lessons for work and they are dull and boring. This was interactive and made it enjoyable for everyone while still learning."

"Great time! Better than any other mandatory online cyber awareness training that I've been required to take, and I really like the idea of having my team/my people with me. Thanks!"

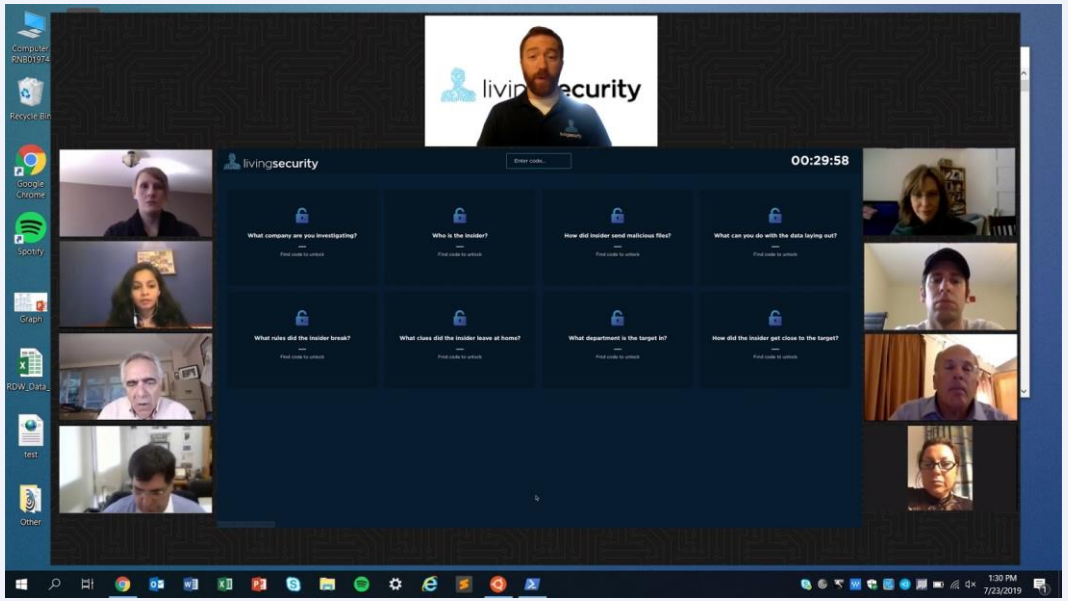
livingsecurity

TRY THIS!

Gamified Learning



Make It Social



Tell A Story

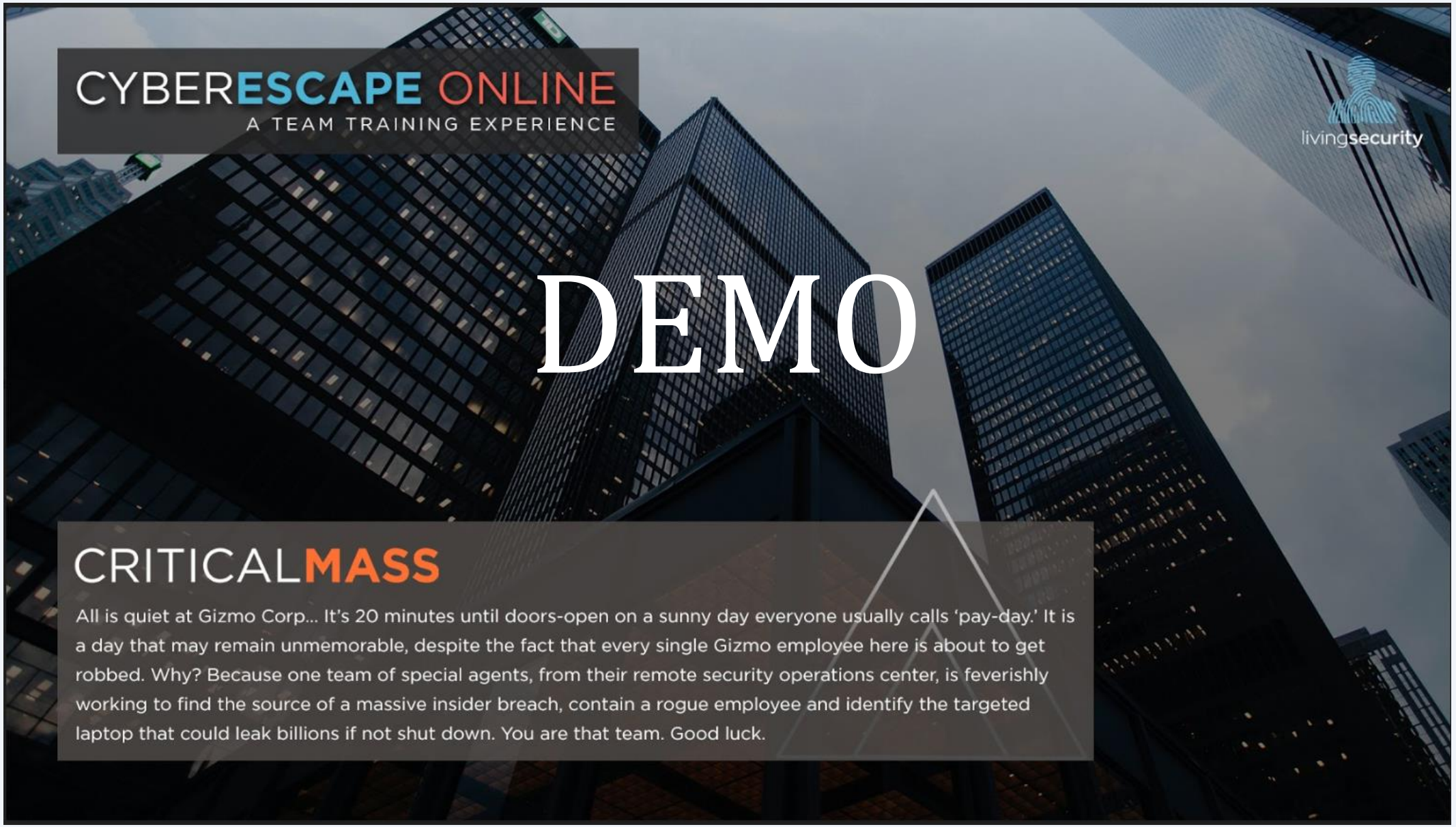
NIST CYBER

Next Webinar
July 20, 2020 | 1pm– 2:30pm EST
CyberRap, Music, Dance, Gamification, and Fun in Cybersecurity Training

fissea FEDERAL

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

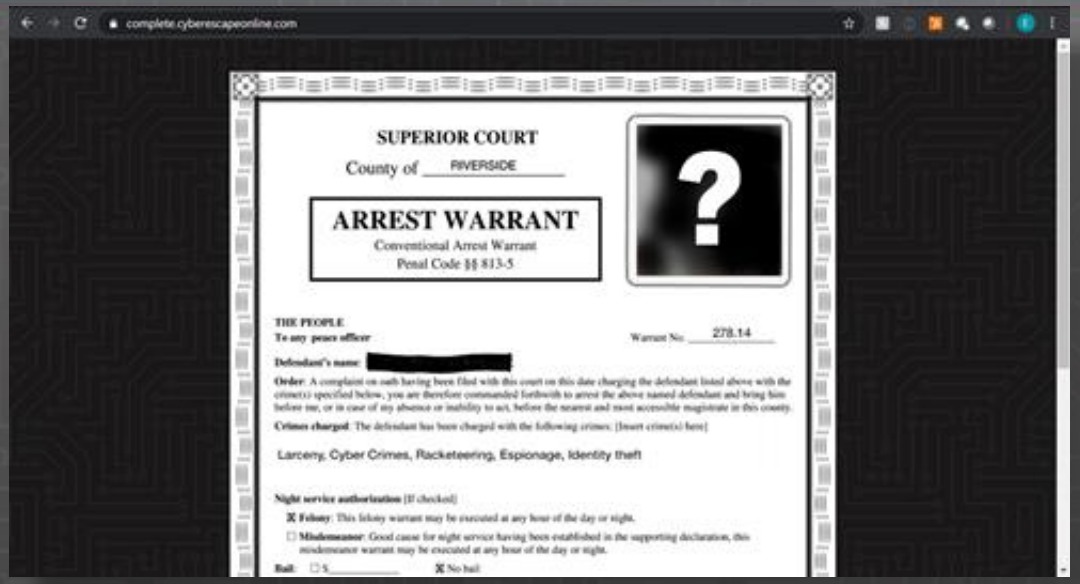
NIST National Institute of Standards and Technology U.S. Department of Commerce


CYBERESCAPE ONLINE
A TEAM TRAINING EXPERIENCE
livingsecurity
DEMO
CRITICALMASS
All is quiet at Gizmo Corp... It's 20 minutes until doors-open on a sunny day everyone usually calls 'pay-day.' It is a day that may remain unmemorable, despite the fact that every single Gizmo employee here is about to get robbed. Why? Because one team of special agents, from their remote security operations center, is feverishly working to find the source of a massive insider breach, contain a rogue employee and identify the targeted laptop that could leak billions if not shut down. You are that team. Good luck.

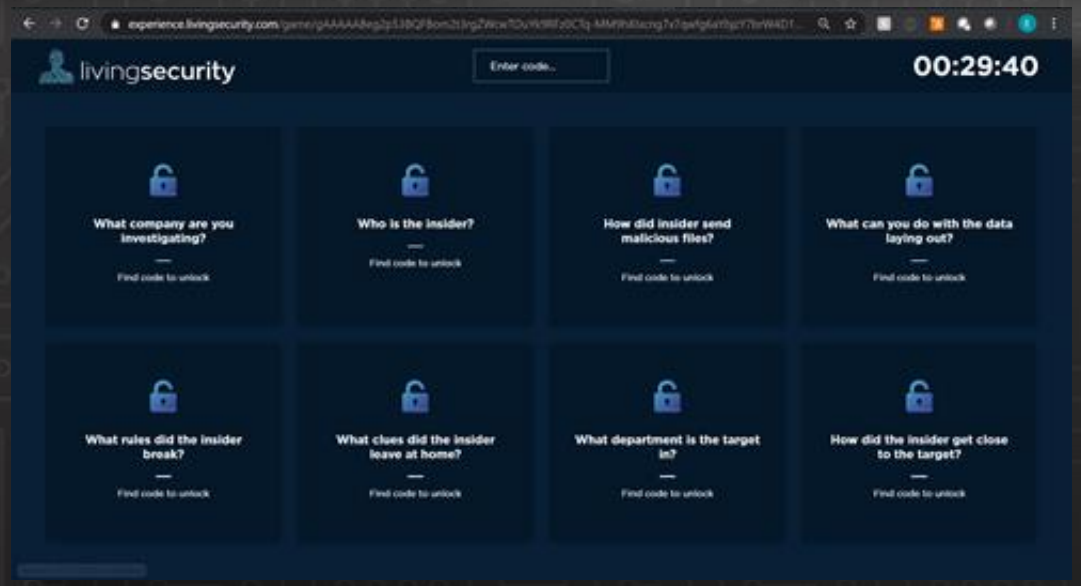
WHAT IS HAPPENING?

livingsecurity

EVIDENCE
LOCKER



PUZZLE
PAGE



EXPERIENCE
MANAGER

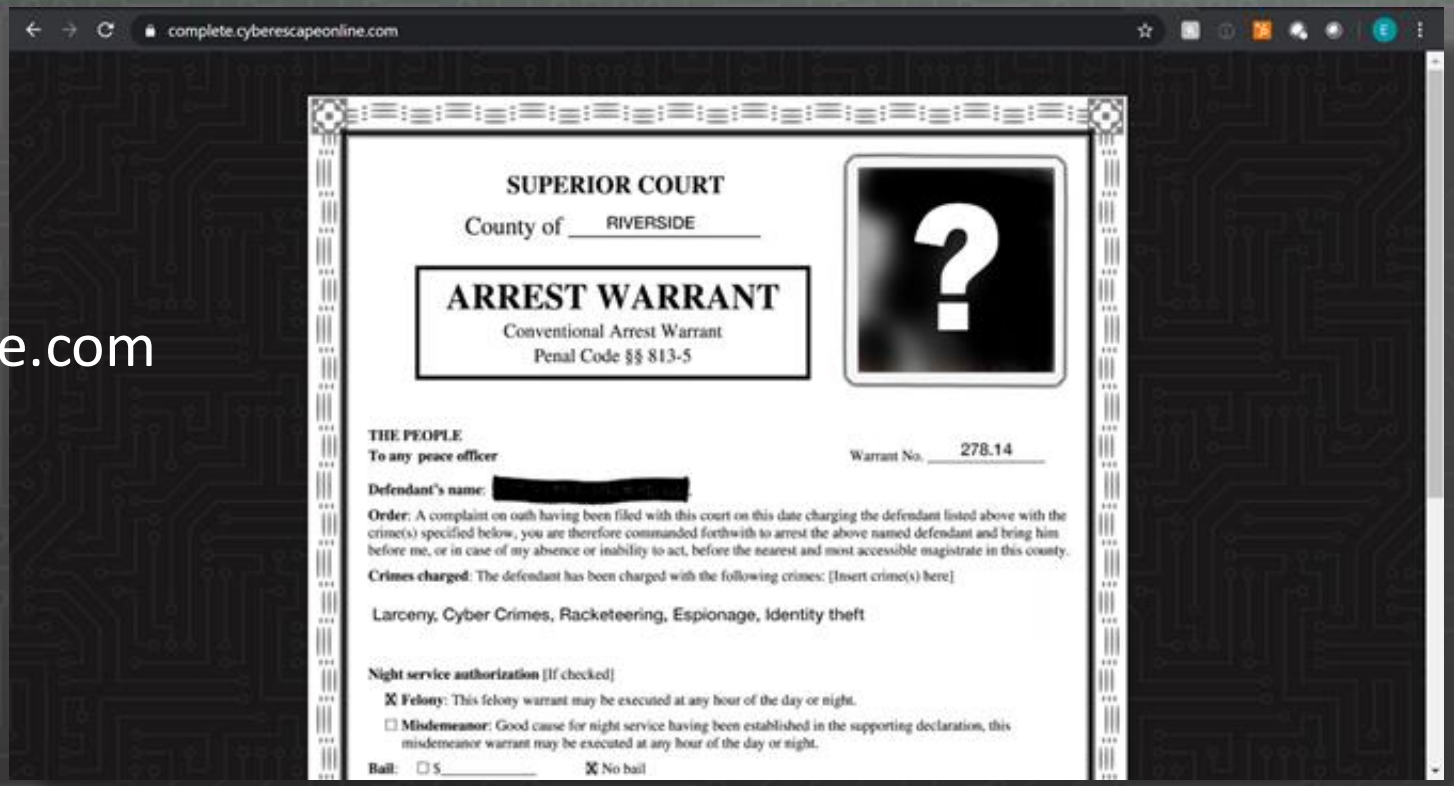
CYBERESCAPE ONLINE
A TEAM TRAINING EXPERIENCE

WHAT IS HAPPENING?

livingsecurity

PUZZLE PAGES

• • • • • • • • • • • .cyberescapeonline.com



ONLY ONE PERSON

SHOULD HAVE THE CURRENT PUZZLE OPEN AT ANY GIVEN TIME! YOUR MODERATOR WILL ENGAGE EVERYONE IN THE ROOM TO GET INVOLVED!

WHAT IS HAPPENING?

livingsecurity

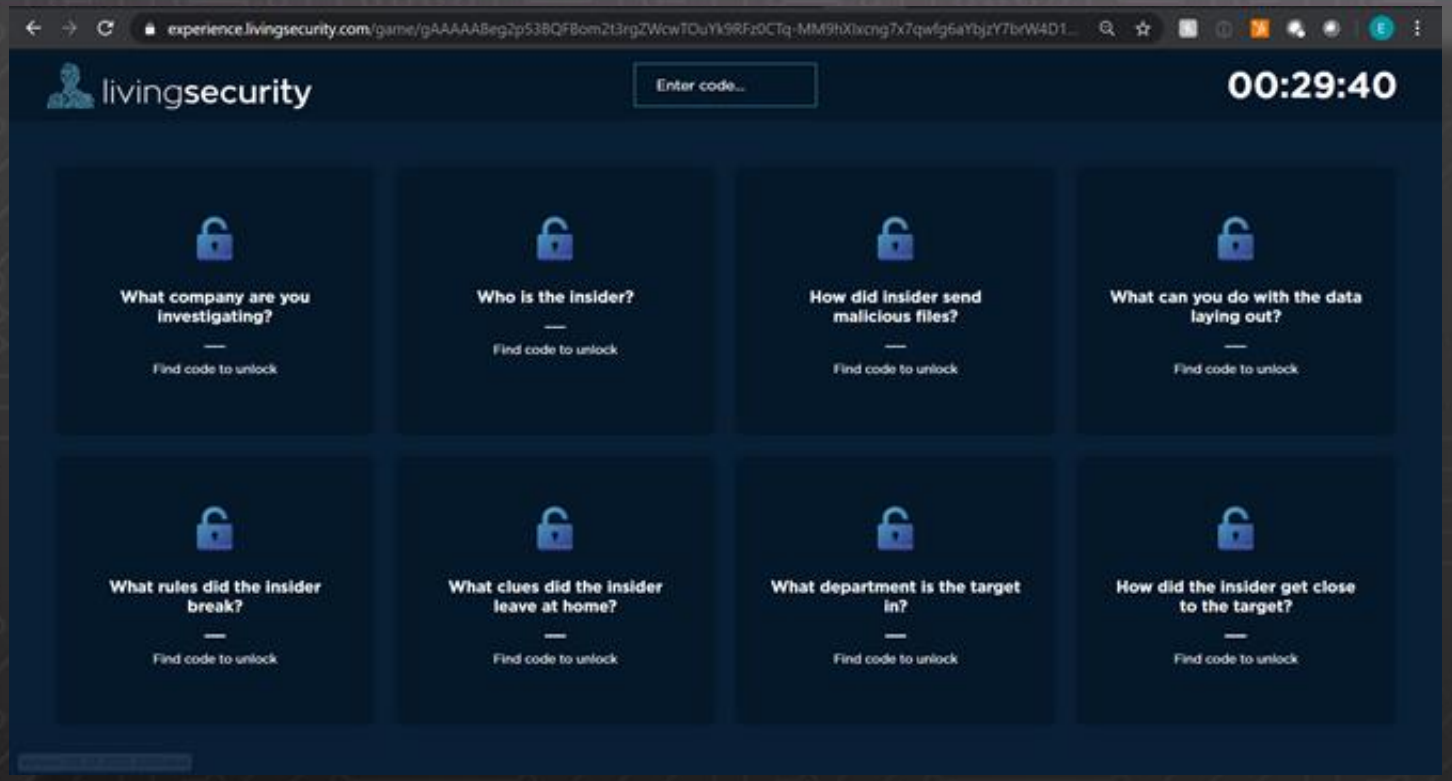
EVIDENCE LOCKER

EVERYONE

SHOULD HAVE THE EVIDENCE LOCKER OPEN DURING GAMEPLAY!!

WHAT IS HAPPENING?

livingsecurity

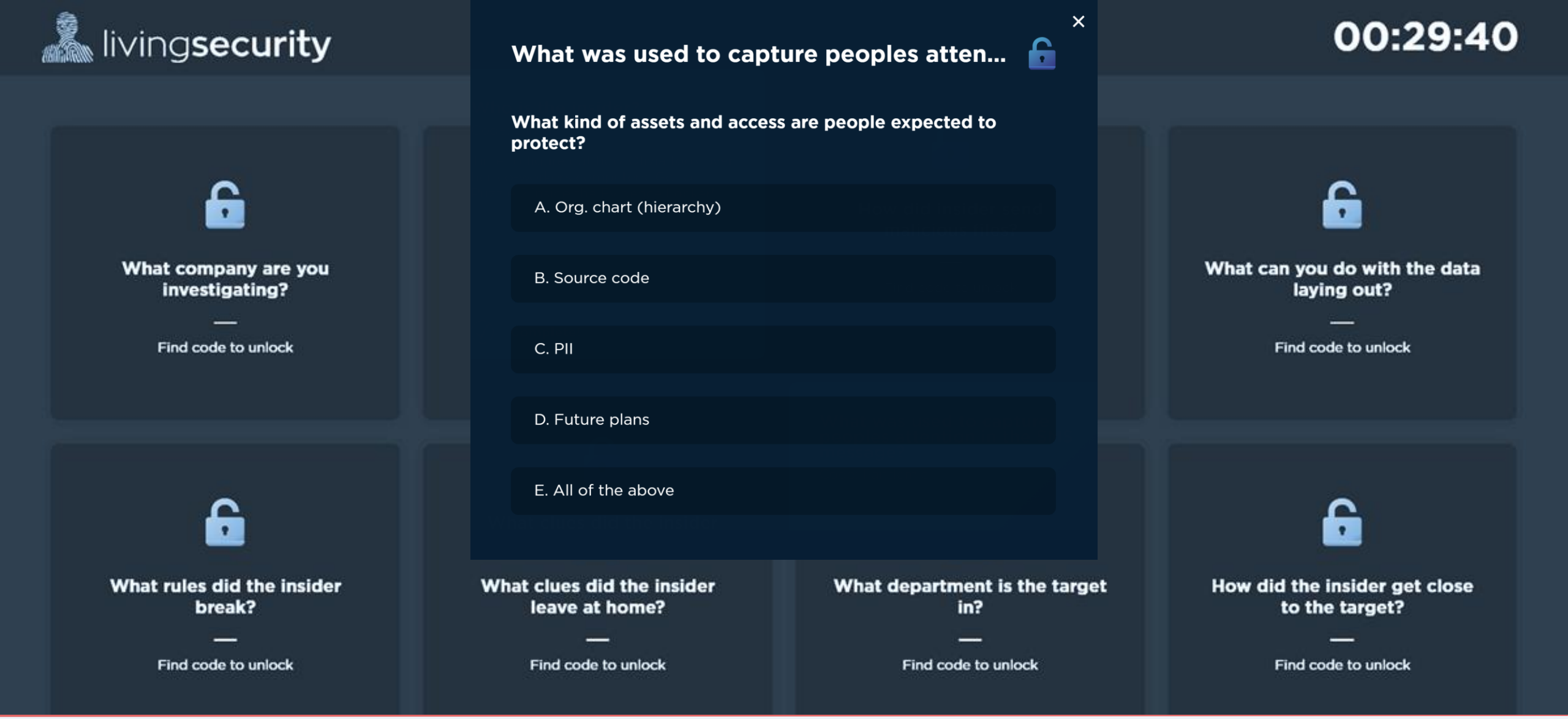


EXPERIENCE MANAGER

ONLY THE HOST

WILL OPERATE THE EXPERIENCE MANAGER DURING GAMEPLAY!!

CYBERESCAPE ONLINE
A TEAM TRAINING EXPERIENCE



CYBERESCAPE ONLINE

A TEAM TRAINING EXPERIENCE

Training Integration

FORENSICS REPORT

livingsecurity

1.

PUZZLE: COMPLETE
PROCEDURE: We found evidence of the ***INSIDER THREAT***
RESULT: We linked suspect, **OLIVIA GRAY**, to insider activity

2.

PUZZLE: FLAGS
PROCEDURE: We identified red flags in ***PHISHING*** and ***SPEAR-PHISHING*** emails
RESULT: We analyzed suspicious emails sent from Olivia Gray's personal account

3.

PUZZLE: CLASSIFY
PROCEDURE: We used ***DATA CLASSIFICATION*** techniques to sort public & private data
RESULT: We discovered, in Olivia's file cabinet, that she was hoarding private data

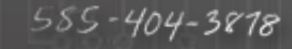
4.

PUZZLE: UNSCRAMBLE
PROCEDURE: We reviewed 10 ***SECURITY AWARENESS POLICY FUNDAMENTALS***
RESULT: We used the policy statements to figure out what rules Olivia broke

5.

PUZZLE: HOTSPOT
PROCEDURE: We identified 7 deadly sins of ***WORKING FROM HOME***
RESULT: We got a warrant to search Olivia's home and discovered work data on personal devices

6.



PUZZLE: CALLFIRE
PROCEDURE: We uncovered evidence of a ***SMS-PHISHING (SMISHING)*** campaign
RESULT: We investigated a phone number on Olivia's scribble pad and found another clue

7.

PUZZLE: VISHING
PROCEDURE: We learned how Olivia used ***VOICE-PHISHING (VISHING)*** tactics to gain access to company finances
RESULT: We followed the breadcrumbs to two of Olivia's targets

8.

PUZZLE: FEED
PROCEDURE: We used ***DEFAULT CREDENTIALS*** to gain access to an unprotected ***IoT*** video feed
RESULT: We used intel from the investigative team to find Olivia's target (CFO) and shut down the laptop

CYBERESCAPE ONLINE
A TEAM TRAINING EXPERIENCE

END GAME

livingsecurity

Congratulations!

You successfully completed the Living Security Escape Room.

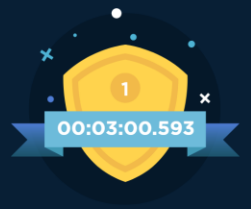
Unlocked Clues:	3
Incorrect Answers:	1
Initial Time:	00:06:26.340
Penalty Time:	00:01:00
Final Time:	**00:07:26.340**
	00:06:26.340 + 00:01:00

See Leaderboard | Add picture

CyberEscape Competi... - Leaderboard

https://experience.livingsec... Copy Link

Test800
Online



Test123
Online

Anonymous
Somewhere in the universe

Rank	Team	Location	Start date	Time completed
1	Test123	Online	May 18, 2020	00:03:00.593
2	Test800	Online	Jun 18, 2020	00:07:26.340

CYBERESCAPE ONLINE
A TEAM TRAINING EXPERIENCE

REPORTING

livingsecurity

Living security at Event Demos: CyberEscape Online

Date created: 06.04.2020 Storyline: Critical Mass: Remote

Export Report

View participants ▸

Filter

06/04/2020 — 06/18/2020

Sessions distributed by location:

Search location

- [ ] 2800 Opryland Dr, Nashville, TN, 37214
- [ ] Dallas
- [ ] Houston
- [ ] London Conference Room 2
- [ ] Manhattan Beach, CA
- [ ] Online
- [ ] test
- [ ] UK

Submit

7 Sessions scheduled	**5** Sessions completed	**6** Average number of participants in each completed sessions
0/0 0% Sign up/Invited	**28/40** 70% Actually played/Max capacity	**28/0** 100% Actually played/Sign up

% Questions answered correct first time 100%

% Questions answered correct after 1st wrong guess 0%

Leaderboard

1	eg	0%	15s
2	dfg	0%	36s
3	InternationalTeam	100%	25m 40s
4	Winnerz - Totally Better than the Rest!	100%	27m 36s
5	Team Awesome!	100%	DID NOT FINISH

Questions

Based on correct answeres for the 1st time

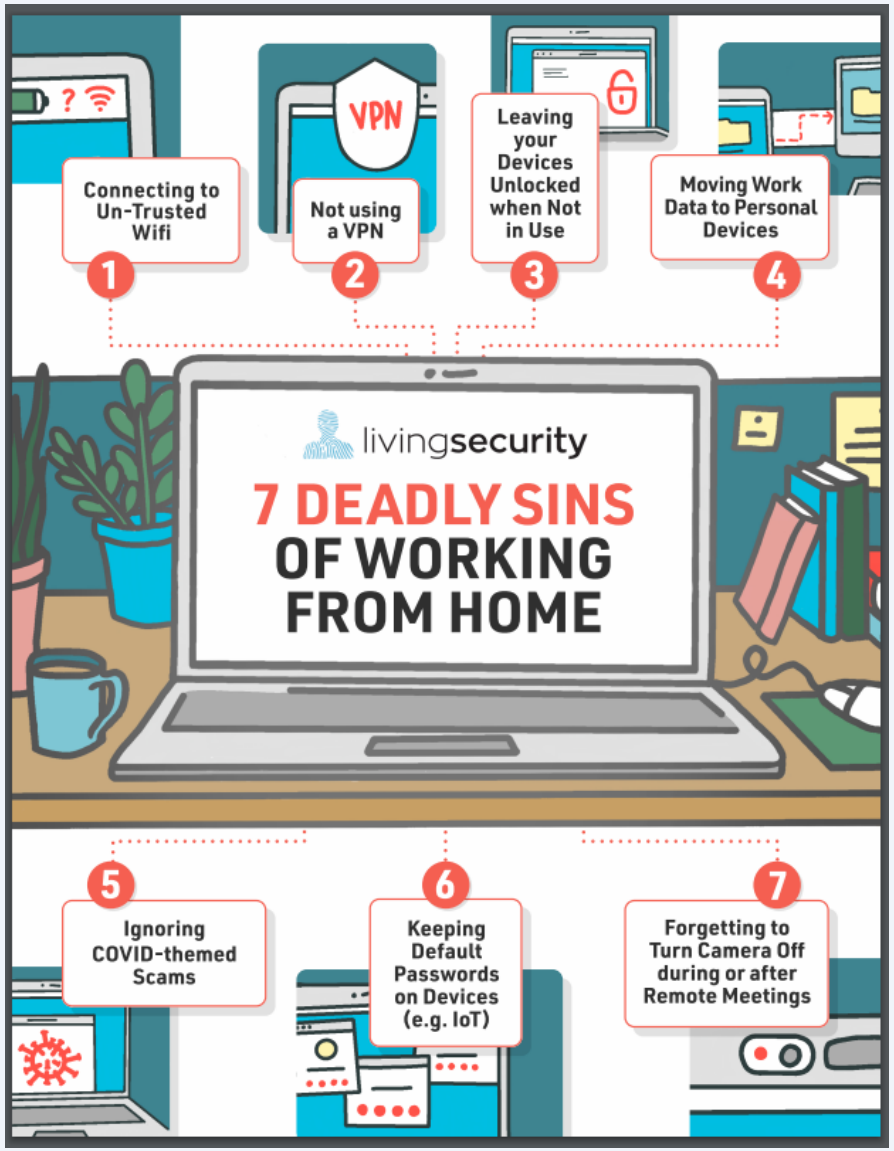
From strong to w...

Malicious insiders are typically...	17%
What does VPN stand for?	11%
Which of the following is a cybersecurity violation?	11%
What kind of assets and access are people expected to protect?	11%

livingsecurity

FREE RESOURCES

- Living Security Resource Page: https://livingsecurity.com/resources/
- **NCSAM Training Kit**
- Security Feud Game
- Cybersecurity Cards Game
- 7 Deadly Sins of Working From Home Poster
- Cyber Hygiene Webinar



livingsecurity

Let's Connect!

Ashley Rose, CEO Living Security

ashley-rose-11678463/

AshleyRose_ATX

Livingsecurity.com

Register for FREE!!!!

www.breakingsecurityawareness.com


Q
&
A

THANK YOU!

Rodney Petersen
NICE Program Director

Sarah Moffat
FISSEA Program Chair

Kristina Rigopoulos
ITL Communications Director

Keri Bray
FISSEA Coordinator

Amber Crutchfield
FISSEA Logistics Coordinator

Calvin Watson
NICE Group Office Manager

STAY IN TOUCH

CONTACT US

fissea@nist.gov

@NISTcyber | #FISSEA2020 #NICEatNIST

JOIN US FOR THE NEXT WEBINAR

CyberRap, Music, Dance, Gamification, and Fun in Cybersecurity Training

July 20, 2020 1:00PM-2:30PM

A new generation of cybersecurity leaders is on the rise. They think cybersecurity education and training should be fun and entertaining. They are ready to inject their fun personalities and creative styles to educate and train organizational workers and members of the public using music, songs, dancing, and cybersecurity games. They are putting out their own brand of cybersecurity education and training and changing organizational culture while building their own personal brands and demonstrating leadership. They call themselves the Cybersecurity Divas and they teach cybersecurity and lead and mentor others in their own unique ways. This session shares their insights, ideas, and unique presentation styles that have won them a large global following already!

Presenters:
- Katia Dean
- Elena Healing
- Katoria Henry
- Naalphatu Toure
- Anye Biamby
- Tomiko Evans
- Dr. Mansur Hasib, Panel moderator and Coach

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

NIST CYBER

fissea FEDERAL

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

NIST CYBER

fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Register Today for the FISSEA Summer Series 2020

July 20, 2020, 1:00-2:30 pm

"CyberRap, Music, Dance, Gamification, and Fun in Cybersecurity Training"

Featuring: Preparing for National Cyber Security Awareness Month presented by the National Cyber Security Alliance

August 24, 2020, 1:00-2:30 pm

"Adaptive Learning: Utilizing AI and Social Collaboration for User-Centric Training Results"

Featuring: Presentation of the FISSEA Security Awareness and Training Contest Winners

September 21, 2020, 1:00-2:30 pm

Topic to be announced

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

NIST CYBER

fissea
FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Save the Date

FISSEA 2021

June 16-17, 2021
NIST Campus
Gaithersburg, Maryland