Federal Information Security Educators (FISSEA)

Winter Forum

February 14, 2023

1:00pm – 4:00pm ET

#FISSEA2023 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Welcome and Opening Remarks

Kendra Henthorne

FISSEA Co-Chair
IT Cybersecurity Specialist
Social Security Administration

Get Involved

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

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

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

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

Keynote

Why Social Engineering Should Be Part of The Cybersecurity Education Discourse

Dr. Aunshul Rege

Associate Professor/ Director of the Cybersecurity in Application, Research, and Education (CARE) Lab
Temple University

Why Social Engineering Should Be Part of The Cybersecurity Education Discourse

Dr. Aunshul Rege
Director, CARE Lab
rege@temple.edu

Acknowledgements

NSF

TEMPLE UNIVERSITY
Office of the Vice President for Research

Temple University
Office of Enterprise Risk Management
College of Liberal Arts Marketing Team

CISA NICE PBGC ATT&CK® AARP® SentinelOne

Google DUO TREND MICRO | education

The CARE Lab

- CARE = Cybersecurity in **A**pplication, **R**esearch, and **E**ducation

Aunshul Rege

@prof_rege

Katorah Williams

@KatorahW

Rachel Bleiman

@rab1928

Gabrielle Spence

@drspenceloading

- Human, socio-behavioral focus
- Funded by NSF + DoE/INL
- Critical infrastructure, ransomware, privacy, surveillance, disinformation, social engineering (SE), cybersecurity education

Agenda

- Why teach students Social Engineering (SE)?
- What does SE education look like?
- What are the challenges in (and responses to) teaching SE?
- (How) does SE education benefit students?
- So… why teach students SE?

Why teach students Social Engineering (SE)?

Current training for next generation workforce

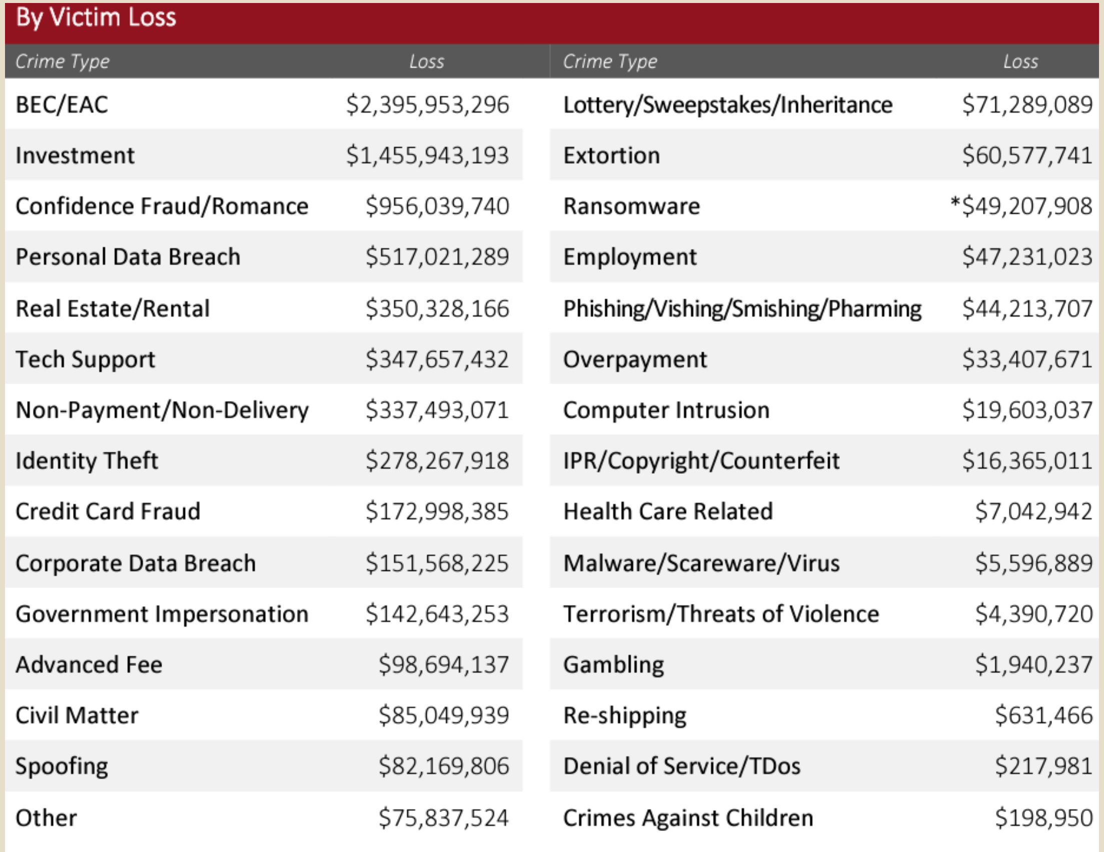
- Global cybersecurity workforce shortage
  - 3.4 million workers needed
- Computer science & engineering already investing heavily
  - Hands-on/experiential learning
  - Capture the flag (CTF) competitions
- Too *small* and *homogenous* for holistic solutions
  - Enlarge & diversify to foster creative potential
  - Human factor in cyberattacks/security

What is social engineering (SE)?

- Manipulating human behavior/psychology to get individuals to:
    - Reveal information
    - Provide access
    - Perform an action

Why address SE?

- Consequences[1]:
    - Direct financial loss
    - Recovery cost
    - Productivity loss
    - Operation disruption
    - Reputation damage



By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$337,493,071	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

[1] https://www.graphus.ai/blog/the-five-agonies-of-social-engineering-cyber-attacks/

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

What does SE education look like?

In the classroom

CARE Lab’s efforts to teach SE

- This educator’s concern
  - Liberal arts students feel they can’t contribute to cybersecurity
  - Computer science students not exposed to human aspects
- Several SE projects mapped to NICE Framework
  - Pretexting, OSINT, privacy, shoulder surfing
  - https://sites.temple.edu/care/social-engineering/course-projects/
- Ethics
  - IRB approved; student training
- > 1,000 downloads worldwide
  - Educators, students, industry, government

What is shoulder surfing?

- Using direct observation
  - Looking over individuals' shoulders at their device
  - Surfing with them without their knowledge or consent
- Gather sensitive information for malicious purposes
  - Personal information/conversations
  - Passwords
  - PINs

Shoulder surfing

1

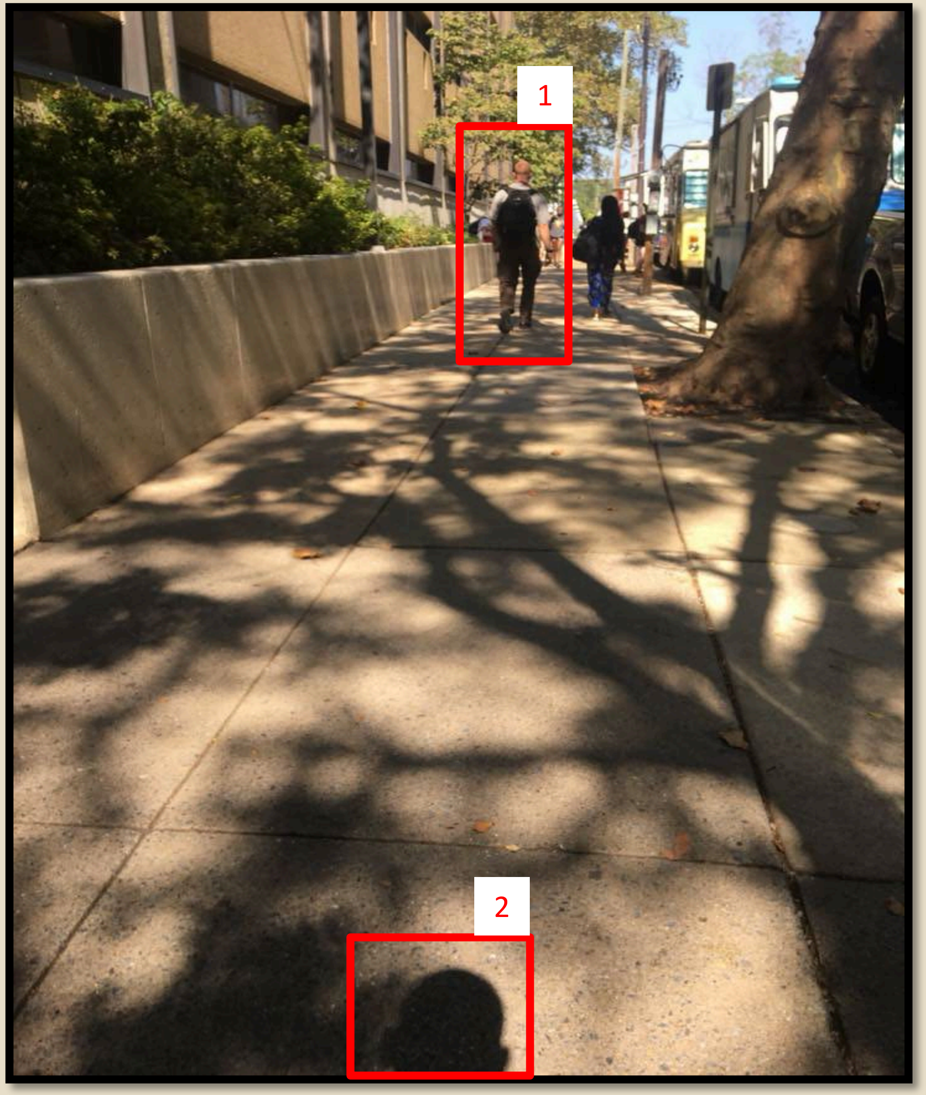
2

Rege, A., Mendlein, A. (+) & Williams, K. (+) (2019). "Security and Privacy Education for STEM Undergraduates: A Shoulder Surfing Course Project". Proceedings of the IEEE Frontiers in Education.

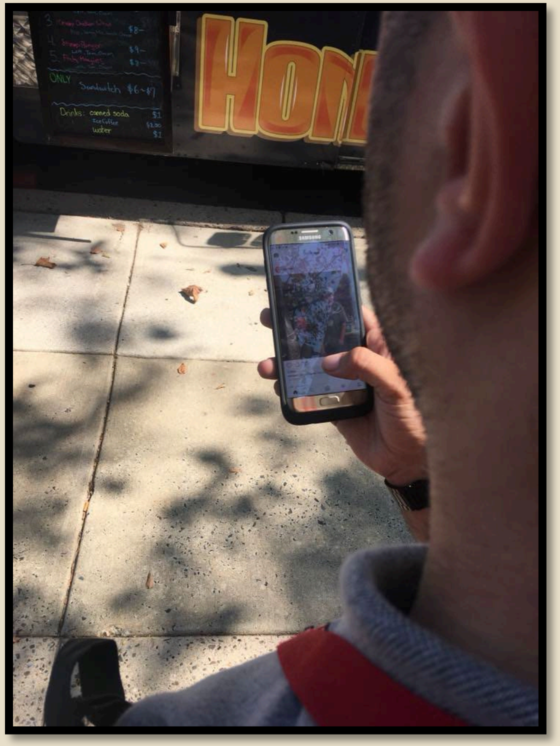
Shoulder surfing: Student thoughts

- Strategies (Offense)
  - In Class
    - Remember seating arrangement & what devices used
    - Honeypots
  - Outside Class
    - Follow rival team members after class persistence
      - Keep a good distance (10-15 feet minimum)
      - Blend in (hats, sunglasses, etc.); remain stealthy
    - Cross-reference rival team members for shared classes
  - Overall
    - Patience, quick action

Shoulder surfing: Persistence

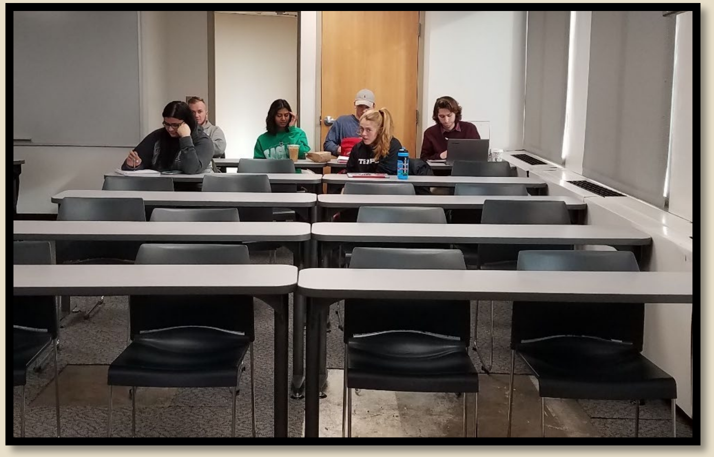


- Followed rival team member
- 20 minutes
- Persistence paid off!



Shoulder surfing: Student thoughts

- Strategies (Defense)
  - High alert
  - Turn off devices
  - Sabotage (photobombing)
  - Change seating location (back, by walls) and position (sideways)

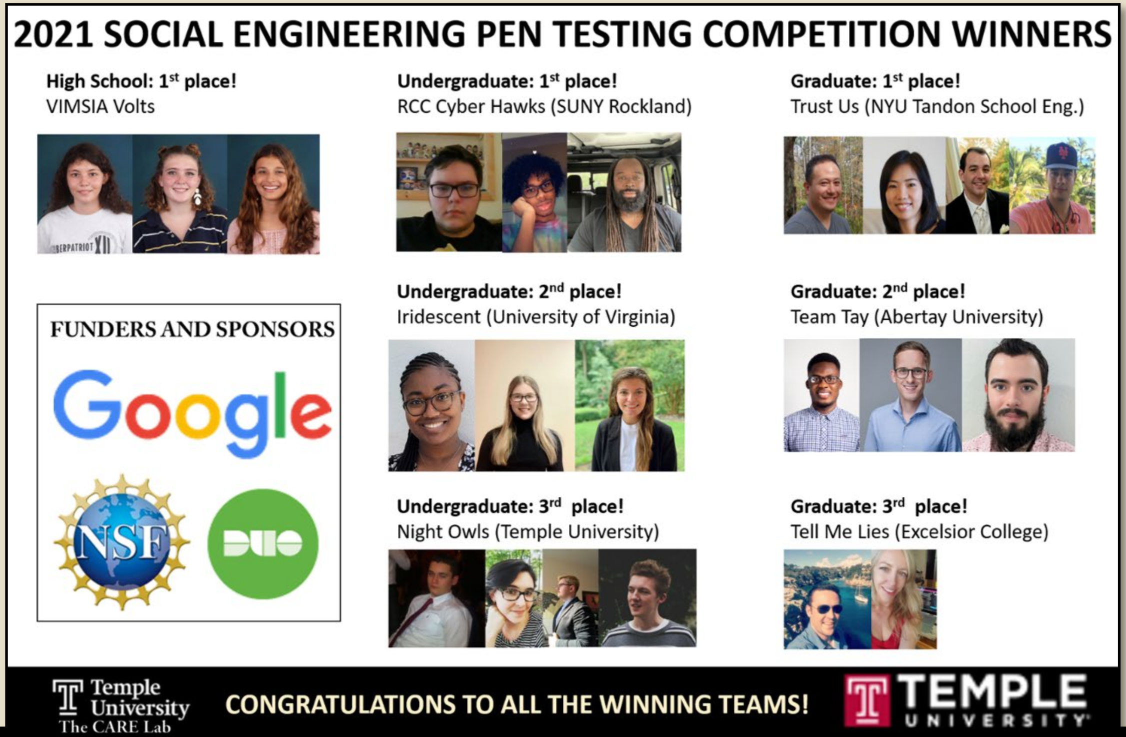


What does SE education look like?

Beyond the classroom

2021: SE penetration test

- The CARE Lab “hired” student teams to conduct a SE pen test on the CARE Lab and its employees
- OSINT, phishing, and vishing
- Formal report: findings + security recommendations



2021 SOCIAL ENGINEERING PEN TESTING COMPETITION WINNERS

High School: 1st place!
VIMSIA Volts

Undergraduate: 1st place!
RCC Cyber Hawks (SUNY Rockland)

Graduate: 1st place!
Trust Us (NYU Tandon School Eng.)

FUNDERS AND SPONSORS

Undergraduate: 2nd place!
Iridescent (University of Virginia)

Graduate: 2nd place!
Team Tay (Abertay University)

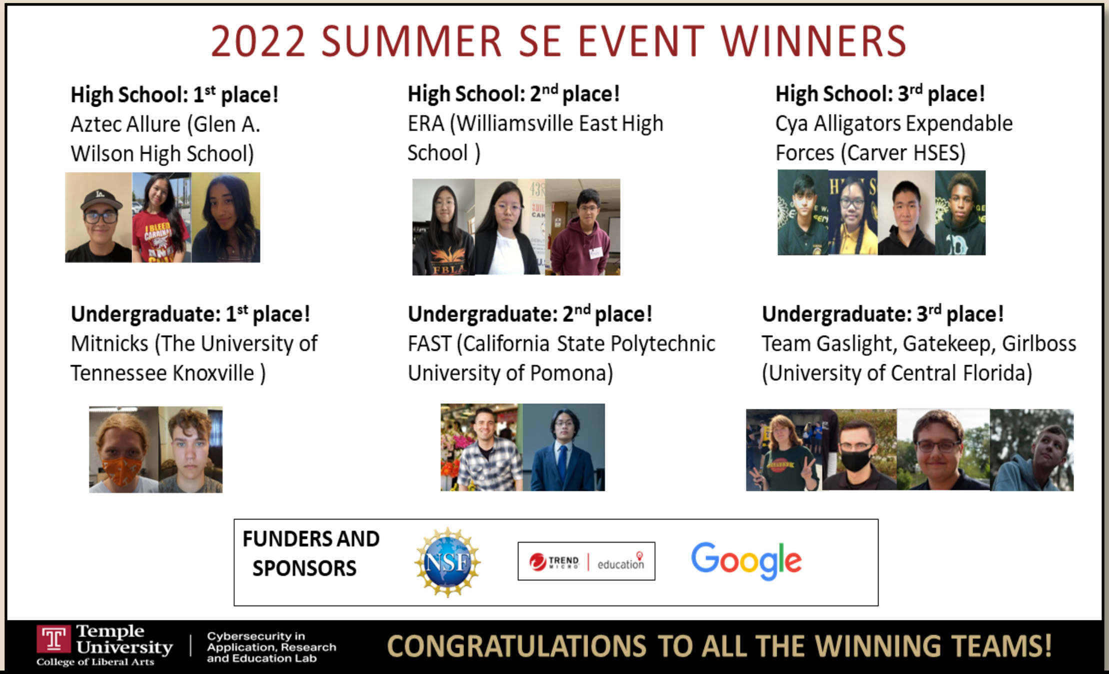
Undergraduate: 3rd place!
Night Owls (Temple University)

Graduate: 3rd place!
Tell Me Lies (Excelsior College)

CONGRATULATIONS TO ALL THE WINNING TEAMS!

2022: Ransomware and SE

- The CARE Lab was hit with ransomware and “hired” student teams to serve as negotiators
- Interface with client + negotiate with ransomware group
- Formal report: negotiation summary + outcome/standing + security recommendations



2022 SUMMER SE EVENT WINNERS

High School: 1st place!
Aztec Allure (Glen A. Wilson High School)

High School: 2nd place!
ERA (Williamsville East High School)

High School: 3rd place!
Cya Alligators Expendable Forces (Carver HSES)

Undergraduate: 1st place!
Mitnicks (The University of Tennessee Knoxville)

Undergraduate: 2nd place!
FAST (California State Polytechnic University of Pomona)

Undergraduate: 3rd place!
Team Gaslight, Gatekeep, Girlboss (University of Central Florida)

FUNDERS AND SPONSORS

NSF
TREND MICRO | education
Google
Temple University College of Liberal Arts | Cybersecurity in Application, Research and Education Lab

CONGRATULATIONS TO ALL THE WINNING TEAMS!

2023: Romance scams and SE

- Inspired FTC Report
  - 2021 ~ $547 million[1]
  - 2022: $1.3 billion[2]
- CARE Lab has been brought in to help the elderly who are falling victim to catfishing scams
  - 70+: individual median loss $9,000
  - Intergenerational emphasis
- Registration opens today!
  - CISA, NICE, AARP, PBGC
  - G: May 19-21 | UG: June 2-4 | HS: June 9-11
  - https://sites.temple.edu/socialengineering/

[1] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

[2] https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

What are the challenges in (and responses to) teaching SE?

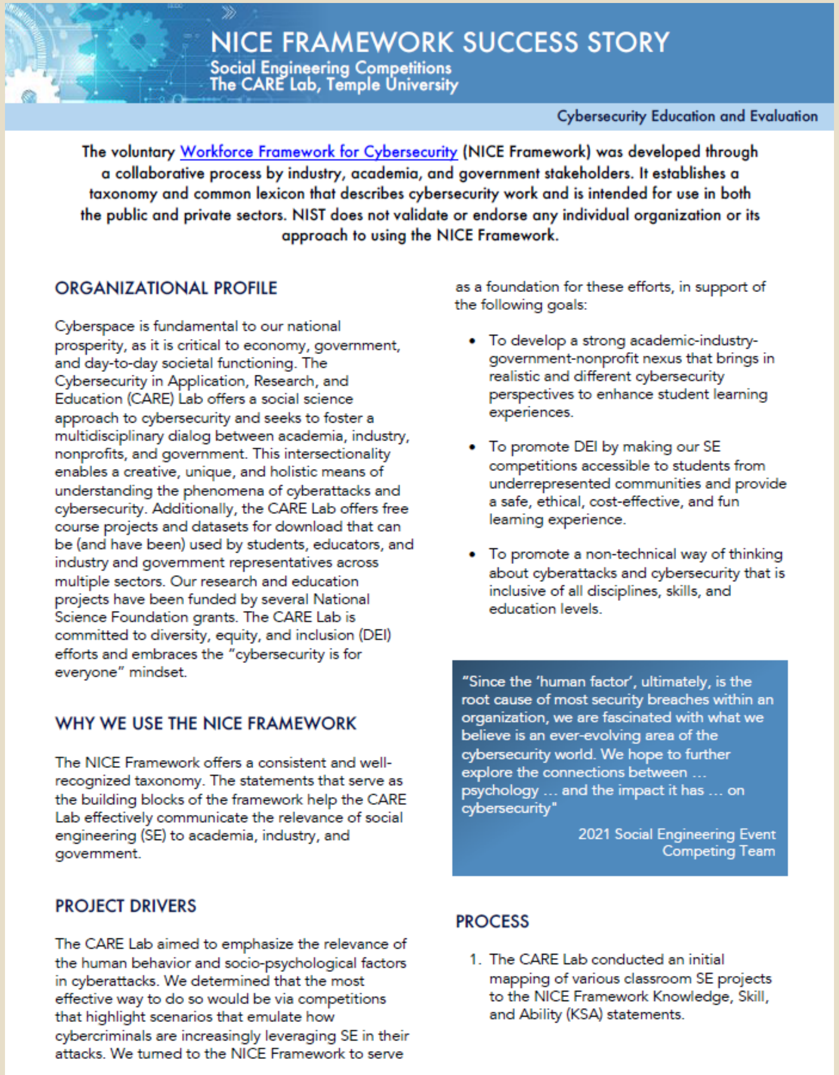
Challenges: Deception & ethics

- “Aren’t you teaching students how to deceive others?”
- “Isn’t what you’re doing ethically wrong?”

Responses

- Hacking CTFs
- Not teaching it is worse
- Best defense is a good offense
- Ethics & code of conduct
- NICE framework success story
- Broadening participation in STEM

NICE Framework Success Story



NICE FRAMEWORK SUCCESS STORY

Social Engineering Competitions
The CARE Lab, Temple University

Cybersecurity Education and Evaluation

The voluntary Workforce Framework for Cybersecurity (NICE Framework) was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE

Cyberspace is fundamental to our national prosperity, as it is critical to economy, government, and day-to-day societal functioning. The Cybersecurity in Application, Research, and Education (CARE) Lab offers a social science approach to cybersecurity and seeks to foster a multidisciplinary dialog between academia, industry, nonprofits, and government. This intersectionality enables a creative, unique, and holistic means of understanding the phenomena of cyberattacks and cybersecurity. Additionally, the CARE Lab offers free course projects and datasets for download that can be (and have been) used by students, educators, and industry and government representatives across multiple sectors. Our research and education projects have been funded by several National Science Foundation grants. The CARE Lab is committed to diversity, equity, and inclusion (DEI) efforts and embraces the "cybersecurity is for everyone" mindset.

WHY WE USE THE NICE FRAMEWORK

The NICE Framework offers a consistent and well-recognized taxonomy. The statements that serve as the building blocks of the framework help the CARE Lab effectively communicate the relevance of social engineering (SE) to academia, industry, and government.

PROJECT DRIVERS

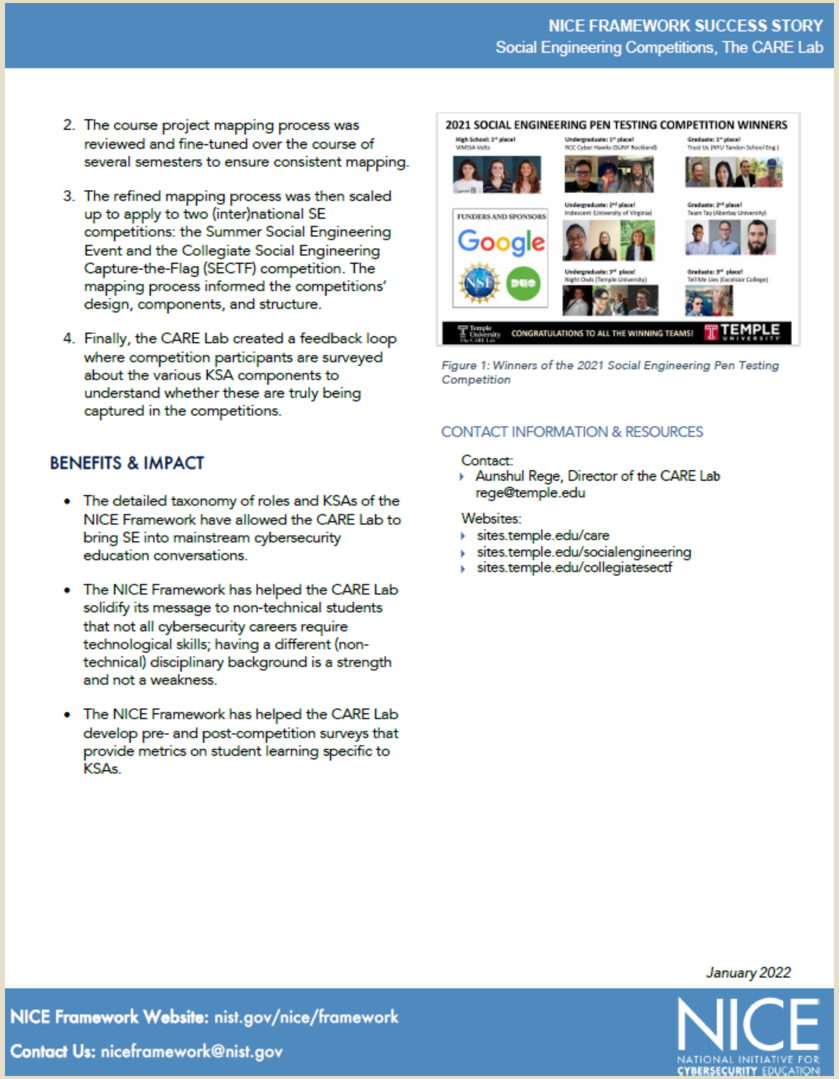
The CARE Lab aimed to emphasize the relevance of the human behavior and socio-psychological factors in cyberattacks. We determined that the most effective way to do so would be via competitions that highlight scenarios that emulate how cybercriminals are increasingly leveraging SE in their attacks. We turned to the NICE Framework to serve as a foundation for these efforts, in support of the following goals:

- To develop a strong academic-industry-government-nonprofit nexus that brings in realistic and different cybersecurity perspectives to enhance student learning experiences.
- To promote DEI by making our SE competitions accessible to students from underrepresented communities and provide a safe, ethical, cost-effective, and fun learning experience.
- To promote a non-technical way of thinking about cyberattacks and cybersecurity that is inclusive of all disciplines, skills, and education levels.

> "Since the 'human factor', ultimately, is the root cause of most security breaches within an organization, we are fascinated with what we believe is an ever-evolving area of the cybersecurity world. We hope to further explore the connections between … psychology … and the impact it has … on cybersecurity"
>
> 2021 Social Engineering Event Competing Team

PROCESS

1. The CARE Lab conducted an initial mapping of various classroom SE projects to the NICE Framework Knowledge, Skill, and Ability (KSA) statements.



NICE FRAMEWORK SUCCESS STORY
Social Engineering Competitions, The CARE Lab

2. The course project mapping process was reviewed and fine-tuned over the course of several semesters to ensure consistent mapping.
3. The refined mapping process was then scaled up to apply to two (inter)national SE competitions: the Summer Social Engineering Event and the Collegiate Social Engineering Capture-the-Flag (SECTF) competition. The mapping process informed the competitions' design, components, and structure.
4. Finally, the CARE Lab created a feedback loop where competition participants are surveyed about the various KSA components to understand whether these are truly being captured in the competitions.

BENEFITS & IMPACT

- The detailed taxonomy of roles and KSAs of the NICE Framework have allowed the CARE Lab to bring SE into mainstream cybersecurity education conversations.
- The NICE Framework has helped the CARE Lab solidify its message to non-technical students that not all cybersecurity careers require technological skills; having a different (non-technical) disciplinary background is a strength and not a weakness.
- The NICE Framework has helped the CARE Lab develop pre- and post-competition surveys that provide metrics on student learning specific to KSAs.

2021 SOCIAL ENGINEERING PEN TESTING COMPETITION WINNERS

FUNDERS AND SPONSORS

CONGRATULATIONS TO ALL THE WINNING TEAMS!

Figure 1: Winners of the 2021 Social Engineering Pen Testing Competition

CONTACT INFORMATION & RESOURCES

Contact:
- Aunshul Rege, Director of the CARE Lab
rege@temple.edu

Websites:
- sites.temple.edu/care
- sites.temple.edu/socialengineering
- sites.temple.edu/collegiatesectf

January 2022

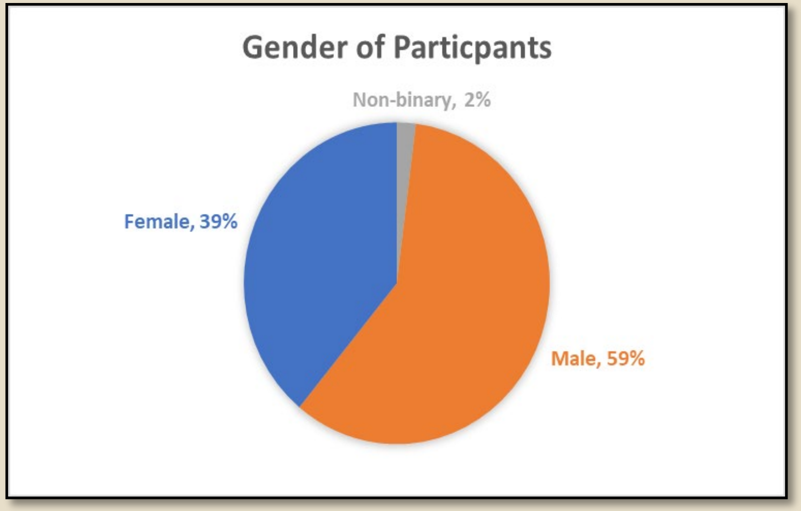
NICE Framework Website: nist.gov/nice/framework
Contact Us: niceframework@nist.gov

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

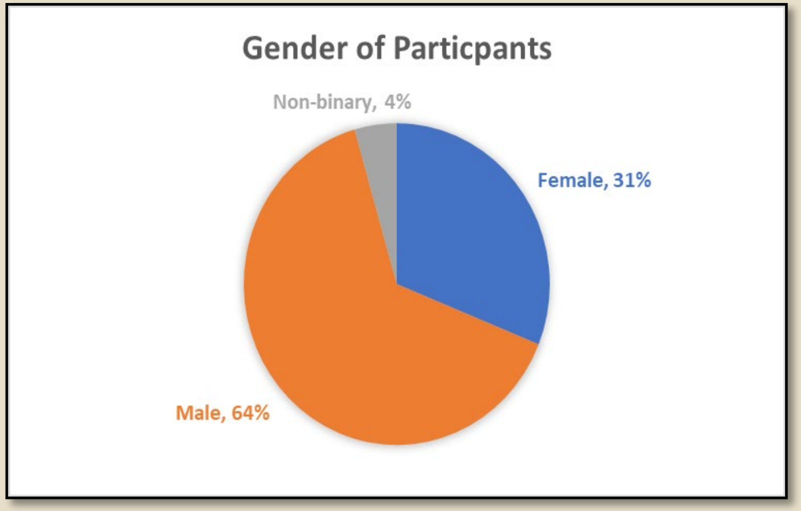
https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-success-story-social

Broadening participation: Gender

2021

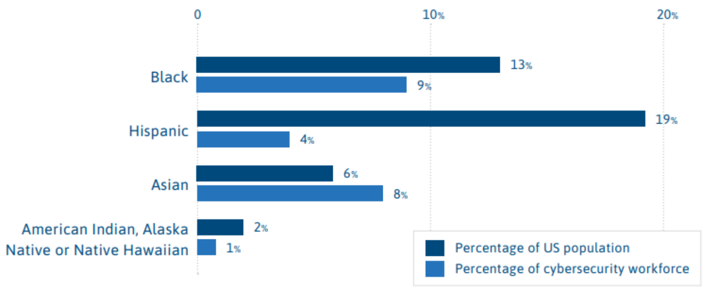


2022



Broadening participation: Race & ethnicity

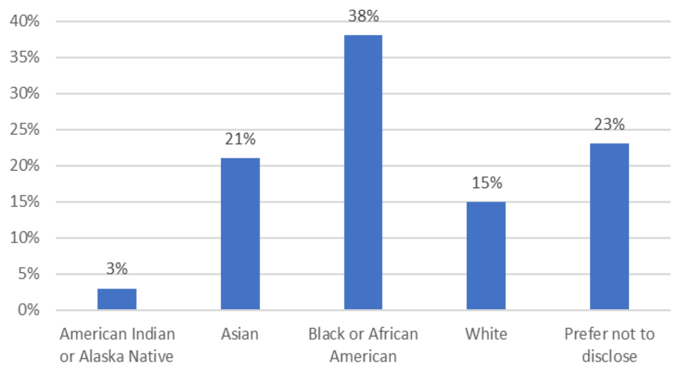
Racial and Ethnic Diversity in the Cybersecurity Workforce



Sources: Jason Reed and Jonathan Acosta-Rubio, "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," Frost & Sullivan, 2019, https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx; United States Population Estimates, 2019," US Census Bureau, accessed July 18, 2021, https://www.census.gov/quickfacts/fact/table/US/SBO050212.

2021

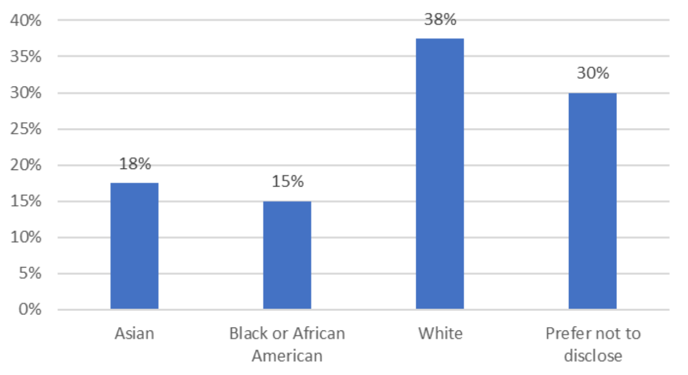
Race of Participants



Hispanic: 5%
Not Hispanic: 66%
Prefer not to disclose: 29%

2022

Race of Participants



Hispanic: 7%
Not Hispanic: 65%
Prefer not to disclose: 28%

Strategic partners

Why diversity (gender, race, ethnicity) matters

- Innovative thinking & different perspectives that cater to a global threat landscape
- Adversaries aren’t homogenous, so our workforce shouldn’t be either.

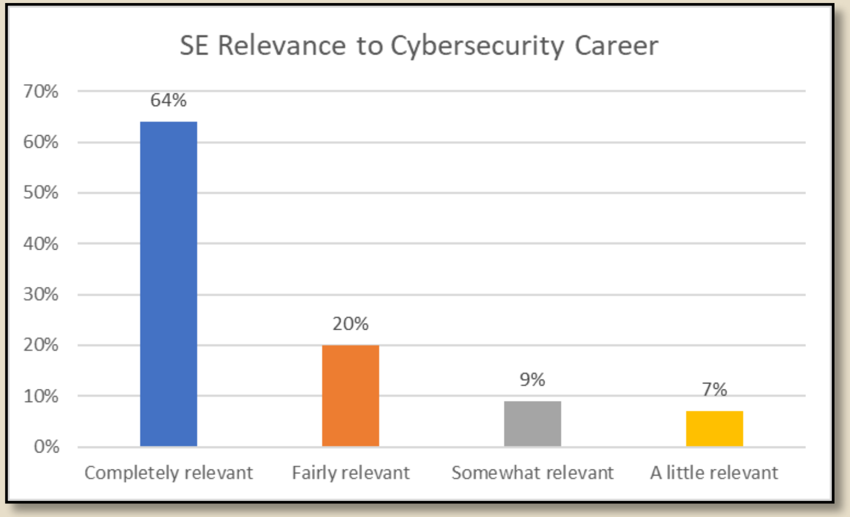
(How) does SE education benefit students?

What are we measuring?

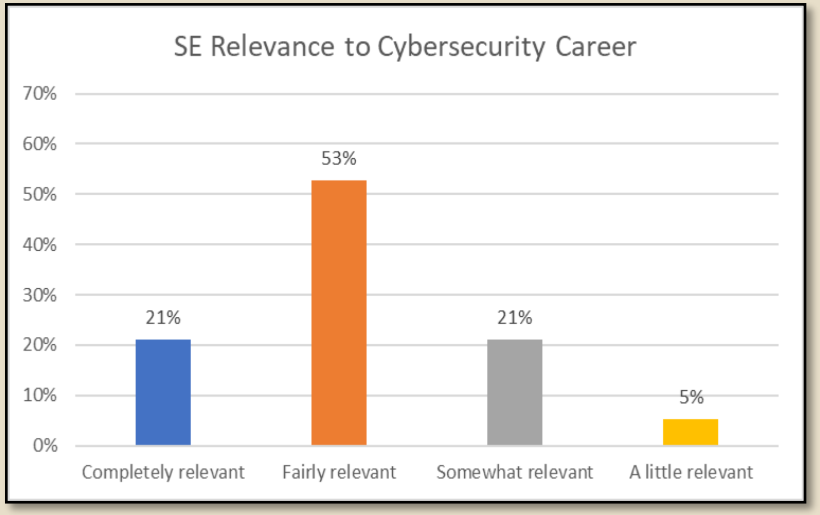
- Relevance of SE to cybersecurity career
- Confidence in SE ability pre-post event
- A supplementary take on diversity, equity, and inclusion (DEI)

Relevance of SE to cybersecurity career

2021

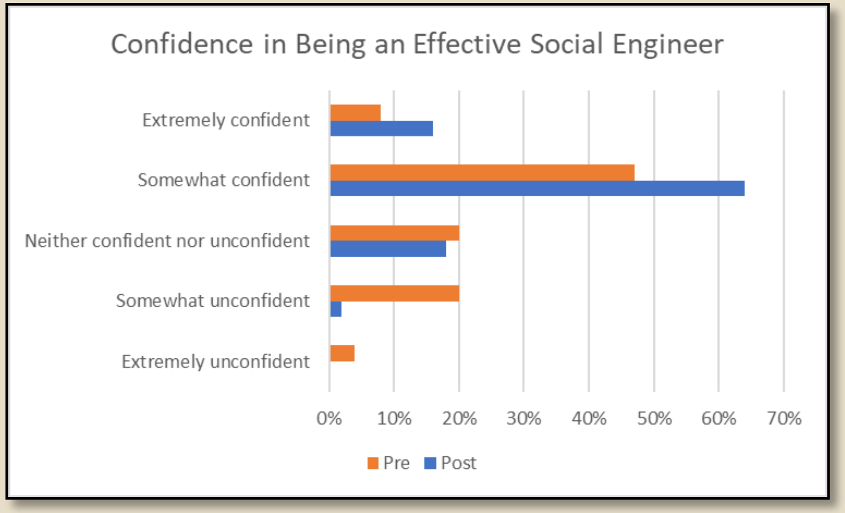


2022

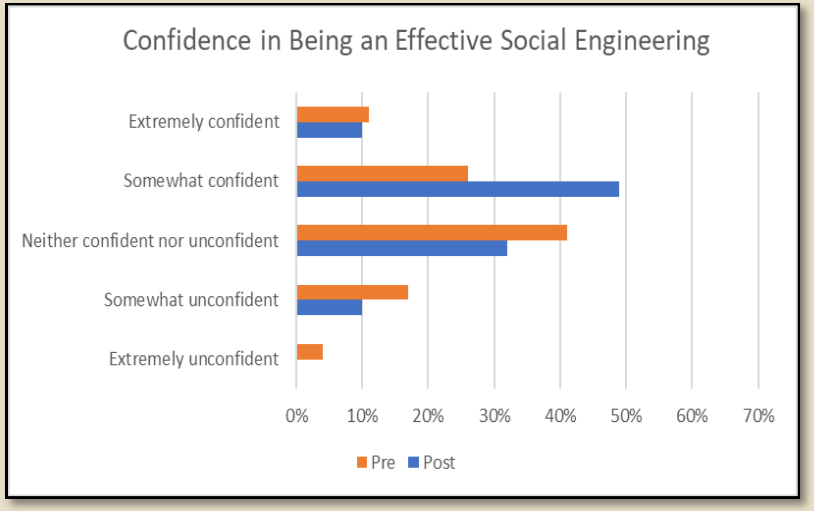


Confidence in being an effective SE pre/post

2021



2022



Diversity, equity and inclusion

- Diversity
  - A different way of thinking/approaching cybersecurity

> "It doesn't matter how much we are hardening our technical systems. If we still haven't [addressed the] human element… then the system will still be weak.
>
> You learn how to do the offense, and when you learn that, you learn about the defense, and you learn that people are susceptible to [SE]".

- Competition participant

Diversity, **equity** and inclusion

- Skills equity = Relatability
  - Everyone has experienced SE

> *"Cybersecurity is something that everyone can do and be aware of and it doesn't have to be super technical. It can be psychological and emotional manipulation"*
>
> ***- Competition participant***

Diversity, equity and **inclusion**

- Inclusion: all disciplines are welcomed <u>and</u> valued
  - Not about conversion!

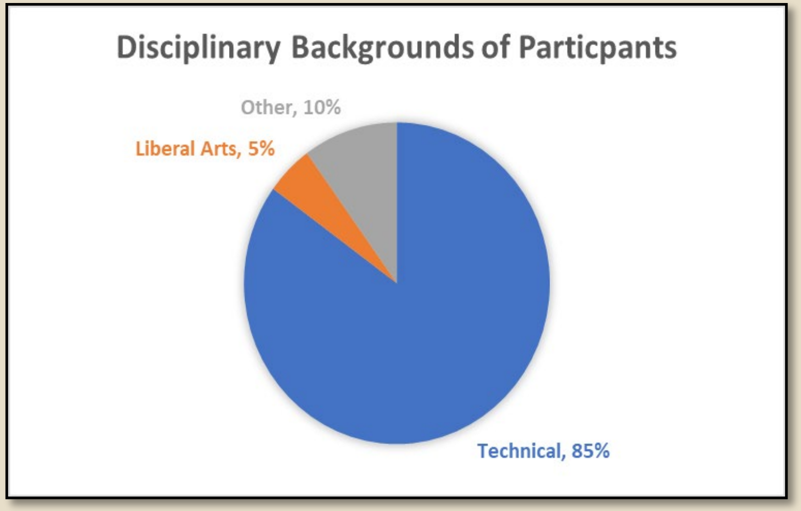
*"[one team member] studies …**Chemistry** , [which] will help us to come up with **scientific-based solutions when we are faced with a challenge**… studies in Nursing and … minor in psychology [would help them] figure out how the … lab employees [thought, and another team member's] background in Global Studies & Italian [would help them] come up with persuasive language that … lab [employees would] respond well to.*

*The **<u>interdisciplinary nature of [our] team [was] a strength</u>** that [would] help us throughout the competition."*

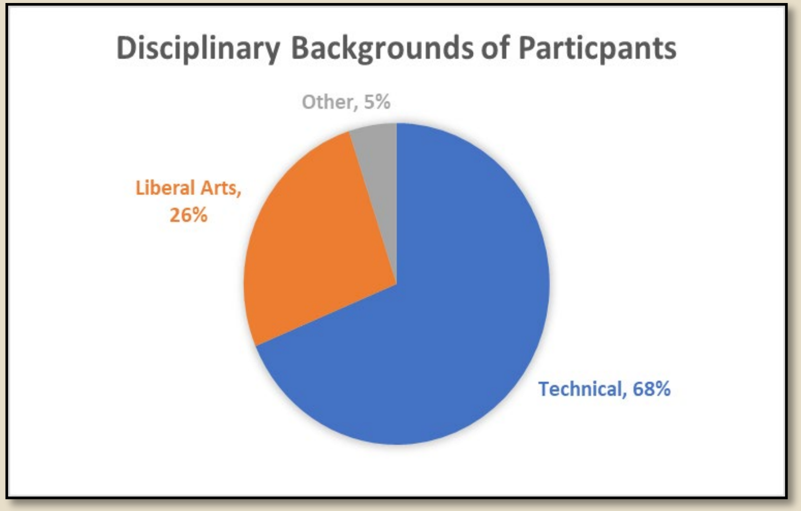
- Competition participant

Disciplinary backgrounds of participants

2021



2022



So… why teach students SE?

Closing thoughts

Why teach SE?

- Cybersecurity >> hard sciences
- Exposure to an often-downplayed attack vector
- Ethics and cyber hygiene
- Well-rounded next generation workforce
  - For social science
    - Empower | change mindset → they CAN contribute
  - For hard science
    - Better designer | Better defender
  - For all
    - Break silo-based thinking
    - Holistic and multidisciplinary | Respect + value other perspectives
- Employers want SE as part of their employees' skills set
  - Nonprofits, industry, government

Nonprofits: Why teach SE?

“The more eyes we can get on this problem, and the more thoughts we can put into this [SE] space, maybe we can produce something [that is meaningful]… cybersecurity is a shared problem… when you see how the real world works, you realize it’s all connected. You can either play in your silo and lose the battle or you can open up to new ideas and realize you can’t solve the problem by yourself”

Industry: Why teach SE?

“Social engineering has definitely gotten picked up more and more; higher profile targets have been attacked via social engineering and I think it’s a big blind spot that a lot of schools and companies don’t think about as much; they are concerned with the technical controls and not with the people controls”

Government: Why teach SE?

"Social engineering is a part of our everyday lives and we are seeing a huge uptick in misinformation and disinformation… and we don't have a grasp on [SE] yet… and if you don't understand it, you're going to get hit by it"

"I recognized that hardly anyone is doing [SE]… it's rare to be able to exercise and practice this skill ethically… [it] is hard to teach… it needs to happen, we need more of it"

Shared responsibility

- Educators
  - Think outside the box
  - Experiential learning with application value
- Subject matter experts
  - Government: CISA, NICE (NIST), PBGC
  - Non-profit: MITRE (ATT&CK), AARP
  - Industry: SentinelOne
- Sponsors

  Google DUO TREND MICRO | education

- Validation that SE is relevant

Why Social Engineering Should Be Part of The Cybersecurity Education Discourse

Thank you.
Comments/Questions?

Dr. Aunshul Rege
Director, CARE Lab
rege@temple.edu

Q&A

Are There Any Questions?

Security Anime Training

Dr. Stephanie Carter

Principal

Coalfire Systems

Security Anime Training

Dr. Stephanie Carter
Principal, Coalfire Systems

Workforce Statistics By Age

Age Groups	Total Population (noninstitutionalized)	Total of Total Population in the Workforce	Percent of Total Population for each Age Group in Workforce	Percent Of Total Population Employed of all Age Groups
16-19	263,973	164,287	62.2%	51%
20-24	20,886	14,817	70.9%	4.6%
25-54	127,162	104,837	82.4%	32.5%
55-64	42,145	27,460	65.2%	8.5%
65 and over	56,710	10,897	19.2%	3.4%
All Age Groups	510,876	322,298	63.1%	100%

- The Baby Boomer Generation (1946 – 1964) – ages 58 to 76
- Generation X (1965 – 1979) – ages 43 to 57
- Millennials (1980-1994) – ages 28 to 42
- Generation Z (1995 – 2012) – ages 10 to 27
- Gen Alpha (2013 – 2025) – ages 0 - 9

**US Bureau of Labor Statistics*

Incorporate Various Learning Styles in Security Training

Learning Styles

- Visual (seeing)
- Aural (hearing, listening)
- Verbal (talking, reading)
- Physical (touching, doing)
- Logical (thinking, figuring out)
- Social (focus groups)
- Solitary (self-learning)

*Training Humans to be Machines, Dr. S. Carter

Elements to Effective Learning

Effective Learning

- Attention and Focus
  - Cognition
  - Concentration
  - Critical Thinking
- Connections and Associations
  - Relevant
  - Relatable
  - Real
- Emotions
  - Agility
  - Reward
  - Ethical Principles
- Innovation
  - Room to grow
  - Room to contribute
  - Room to express
- Diversity
  - Differences
  - Norms
  - Inclusion

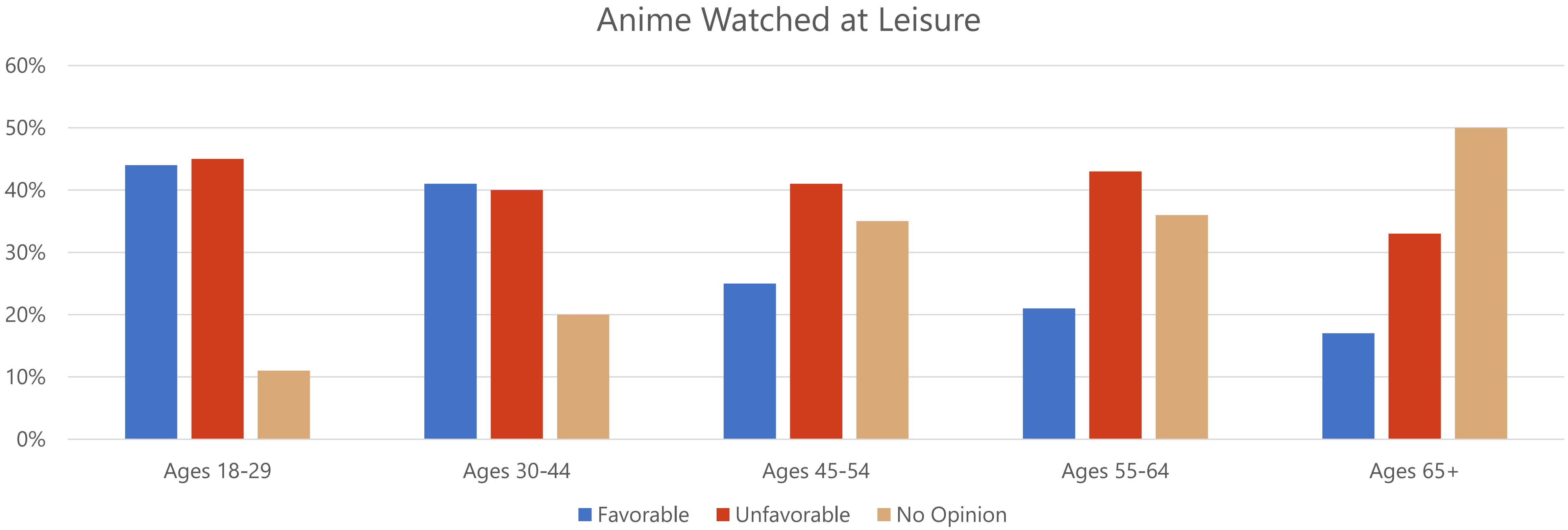
Roadblocks to Learning

Mirrored Mentalities

When you look alike, think alike, feel alike, you also share all perceptions in common to include:

- Biases
- Blind spots
- All or nothing thinking errors
- In the box thinking and performance
- No change
- No innovation
- No perspective
- No diversity

Statistics on Anime

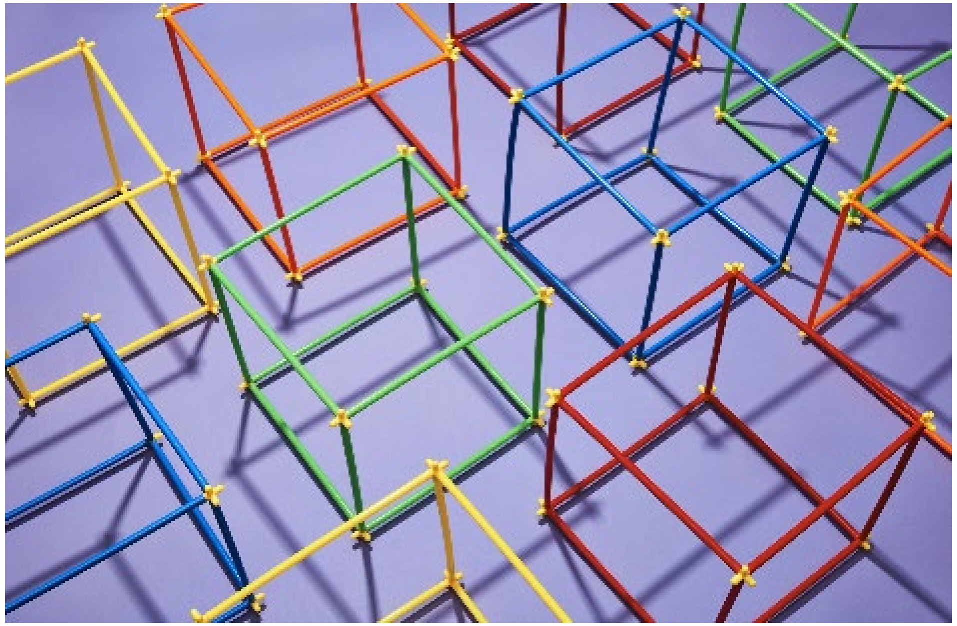


*statista.com

What Can Be Learned From Anime

Study conducted in 2020 for Capella University showed the following themes relating to Anime:

- Engagement
- Academic Success Strategies
- Transition Adaptability
- Resilience Building
- Attention to Detail
- Flexibility
- Open Mindedness
- Positivity
- Facing Obstacles
- Self Advocacy



Traits Needed to Promote Security in the Workplace:

- Engagement
- Resilience Building
- Attention to Detail
- Flexibility
- Open Mindedness
- Positivity

Lessons Learned from Anime that Supports a Security Culture

- Engagement – maturity, real-world relation, manages stress, personally relate

- Resilience Building – learn to advocate for self, characters imitate real-world for them and made them stronger to face those situations, learned to offer understanding, learned "how" to explain things

- Attention to Detail – learned how to set priorities, looked at things differently, learned to not be afraid to ask questions for clarity, asking questions are important, learn to do what is needed to succeed

- Flexibility – do not have to conform to a one size fits all

- Open Mindedness – if something I like is a part of something we all have in common (school) I am more open to share ideas

- Positivity – easier to connect to what is being talked about by showing a clip of anime, would grab their attention and keep them watching, lessons are real in anime despite characters are not, a lot of anime show characters working together even if they don't like each other to accomplish a common goal

Summary

Anime is a tool to use to grab the attention and focus of the younger professionals that make up most of the workforce today.

Security training, to be effective, must be relatable to the intended audience; since the audience will vary greatly, there must be a balance of tools used to present the training.

Everyone digests information drastically different depending on the generation they grew up in.

Learning styles should always be incorporated into all trainings, regardless of additional tools used such as anime, video games, etc.

Security doesn't have to be boring; it can be fun.

Incorporating fun does not automatically weed out significance and importance.

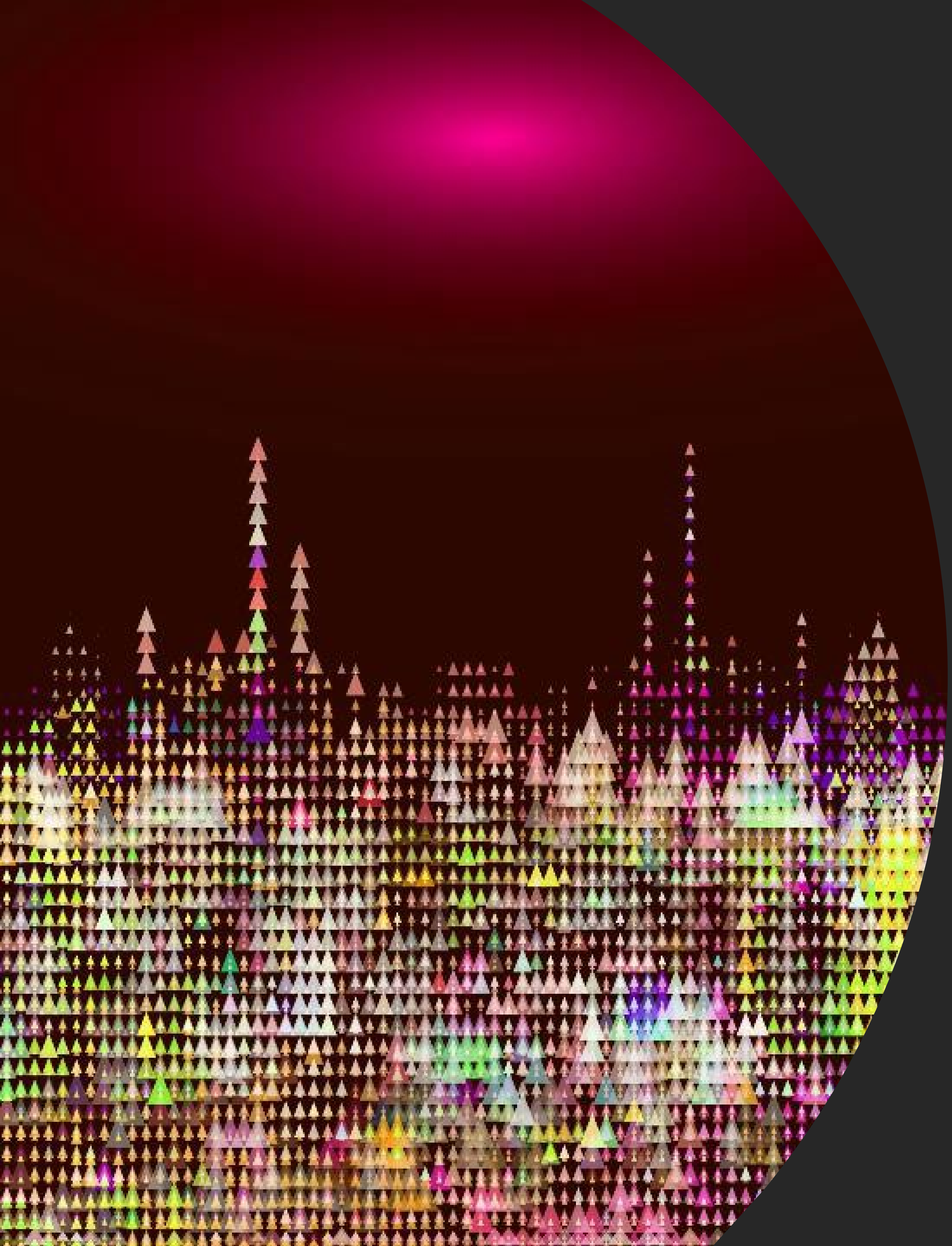
Questions

FISSEA Ignite

How to Build Safer Proto-Metaverses with Conversational AI & Extended Reality

Dr. Tania Peitzker

Adjunct Professor of Metaverses and Interfaces
University of Silicon Valley



How to build safer proto-metaverses with Conversational AI & Extended Reality

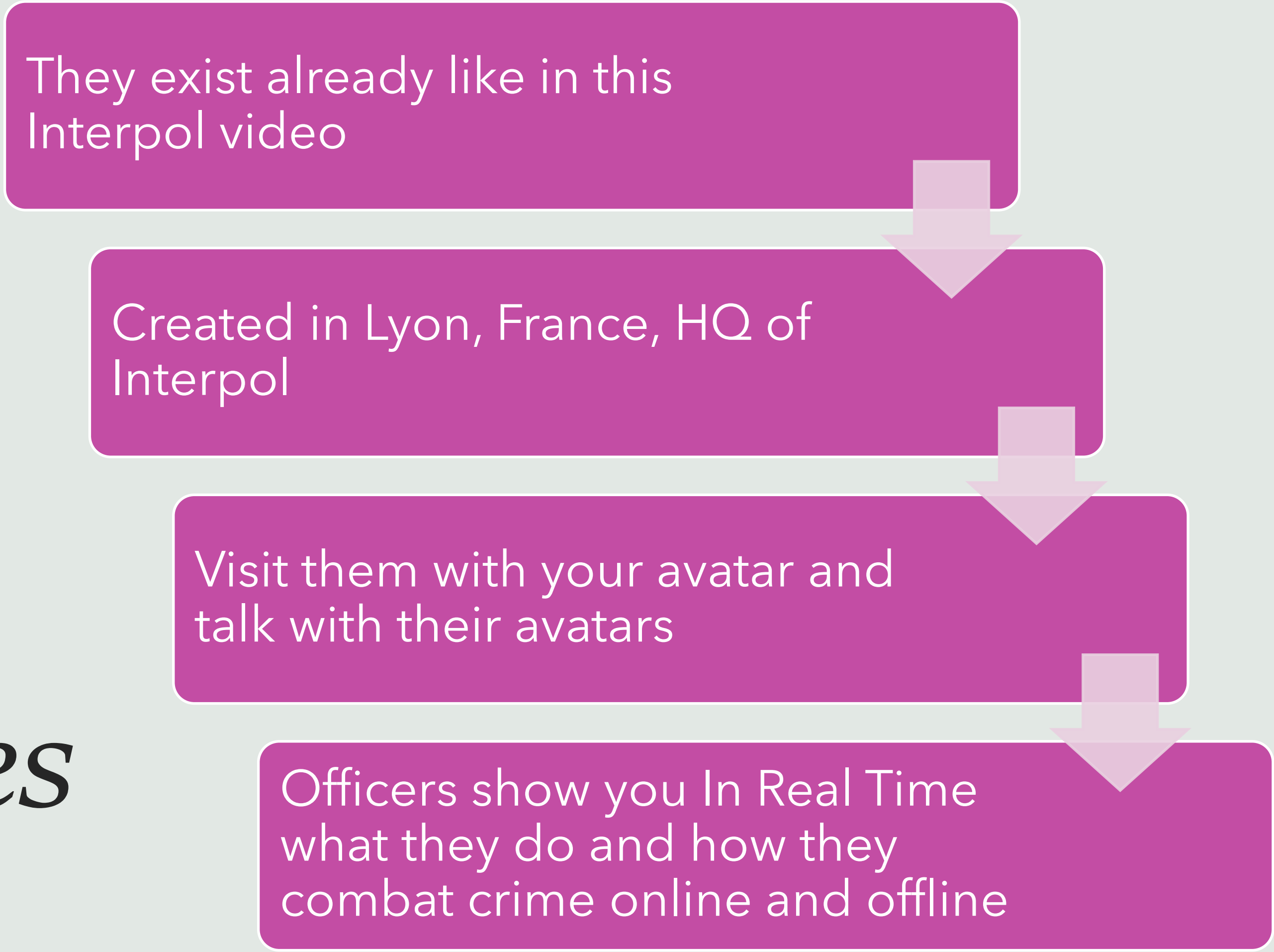
A brief overview of current and potential measures

Dr. phil. Tania Peitzker, Adjunct Prof. Uni Silicon Valley (Cogswell College)

□ *metaverses*
“The Metaverse”
XR - Extended Reality (VR/AR)
Conversational AI (artificial intelligence apps)
cognitive interfaces

Questions you might be asking yourself:

- What are proto-metaverses?
- Why could they be unsafe?
- Does this affect me now or in the near future?



They exist already like in this Interpol video

Created in Lyon, France, HQ of Interpol

Visit them with your avatar and talk with their avatars

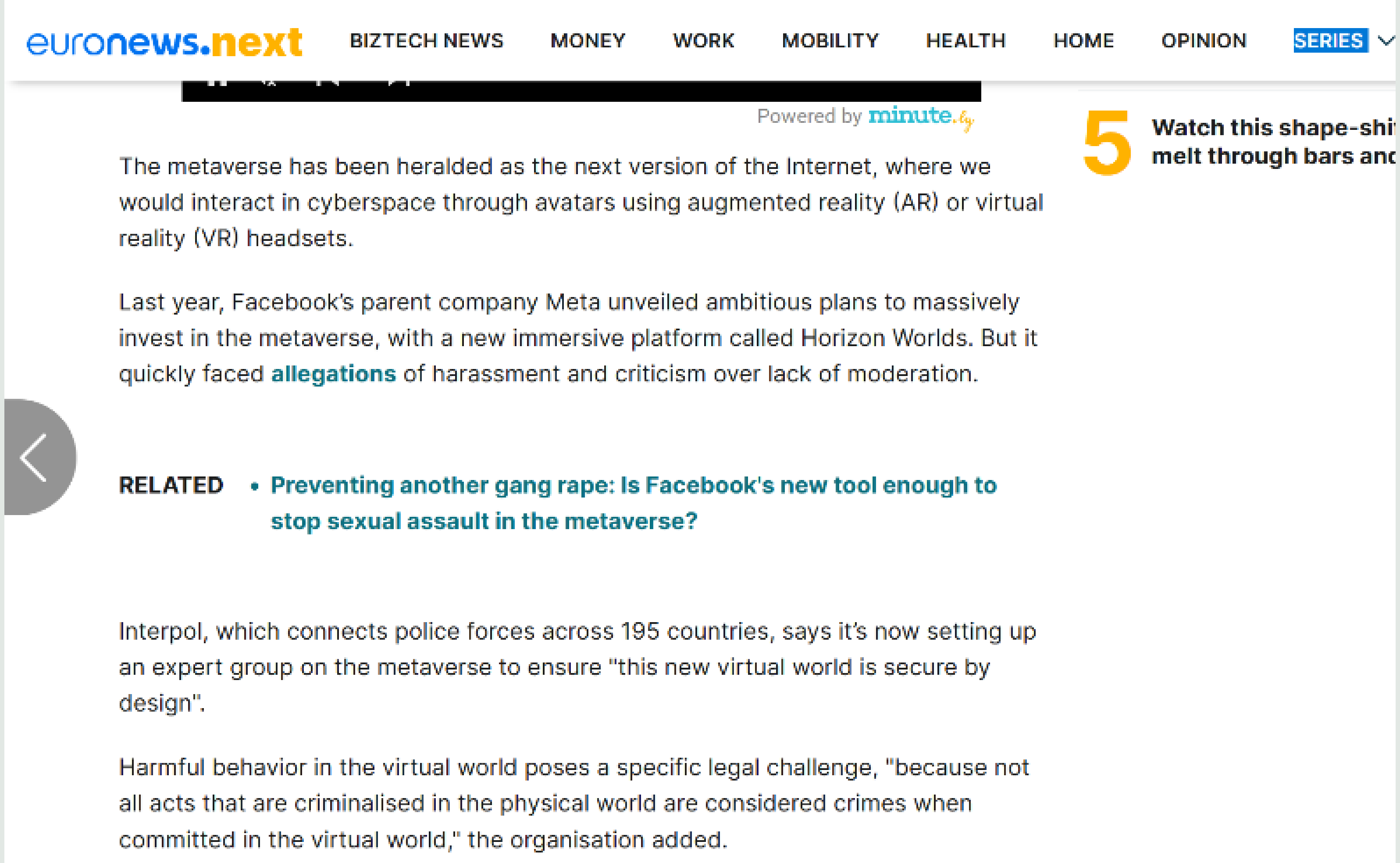
Officers show you In Real Time what they do and how they combat crime online and offline

Proto-metaverses? Immersive platforms you enter with or without VR headsets

Rise of cybercrime

“As the number of metaverse users grows, more possible crimes will emerge, Interpol said, citing "crimes against children, data theft, money laundering, financial fraud, counterfeiting, ransomware, phishing, and sexual assault and harassment".

Cybercrime, from ransomware to online child sexual exploitation and abuse, is expected to rise in the coming years, according to its latest Global Crime Trend report.”



The metaverse has been heralded as the next version of the Internet, where we would interact in cyberspace through avatars using augmented reality (AR) or virtual reality (VR) headsets.

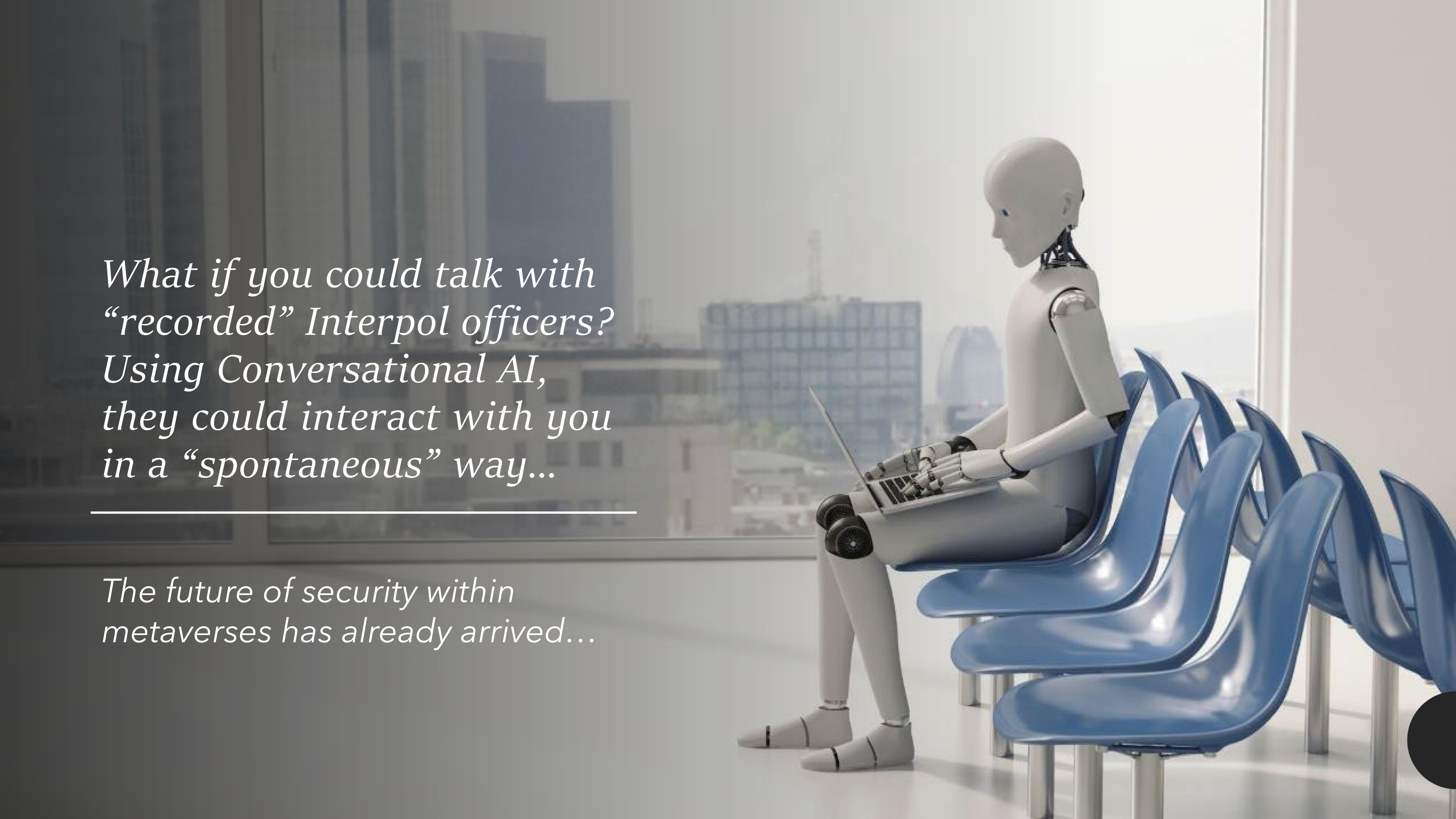
Last year, Facebook's parent company Meta unveiled ambitious plans to massively invest in the metaverse, with a new immersive platform called Horizon Worlds. But it quickly faced **allegations** of harassment and criticism over lack of moderation.

RELATED
- **Preventing another gang rape: Is Facebook's new tool enough to stop sexual assault in the metaverse?**

Interpol, which connects police forces across 195 countries, says it's now setting up an expert group on the metaverse to ensure "this new virtual world is secure by design".

Harmful behavior in the virtual world poses a specific legal challenge, "because not all acts that are criminalised in the physical world are considered crimes when committed in the virtual world," the organisation added.

https://www.euronews.com/next/2022/10/20/interpol-sets-up-its-own-metaverse-to-learn-how-to-police-the-virtual-world

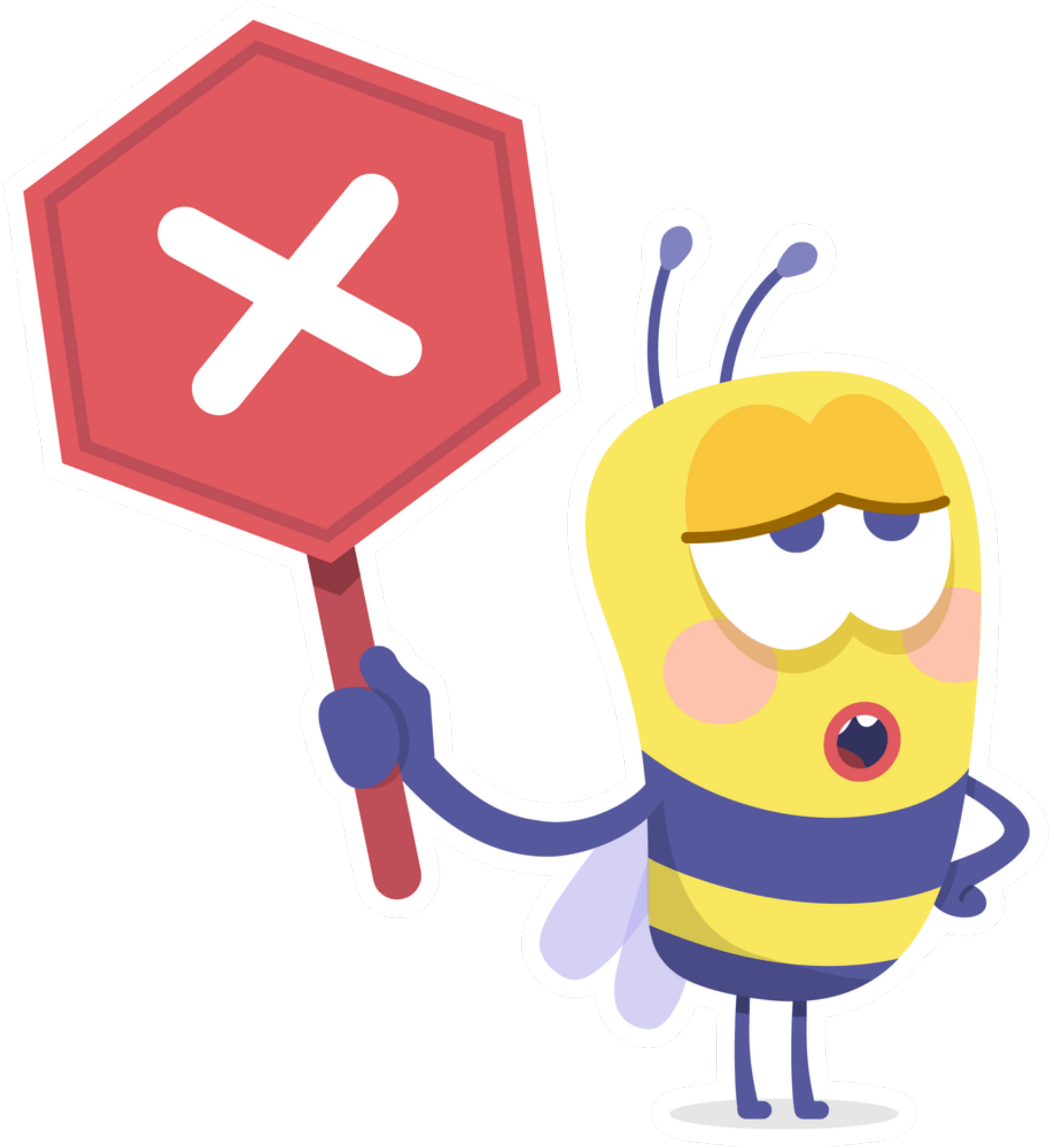


What if you could talk with “recorded” Interpol officers? Using Conversational AI, they could interact with you in a “spontaneous” way...

The future of security within metaverses has already arrived…

Gaming examples   inworld.ai

THE WALT DISNEY COMPANY EXPLORES THE FUTURE OF IMMERSIVE EXPERIENCES AT 2022 DISNEY ACCELERATOR DEMO DAY (prnewswire.com)



Potential for live interactive "policing" or "community officers" avatars to create safe metaverses

Conversational AI to the rescue!

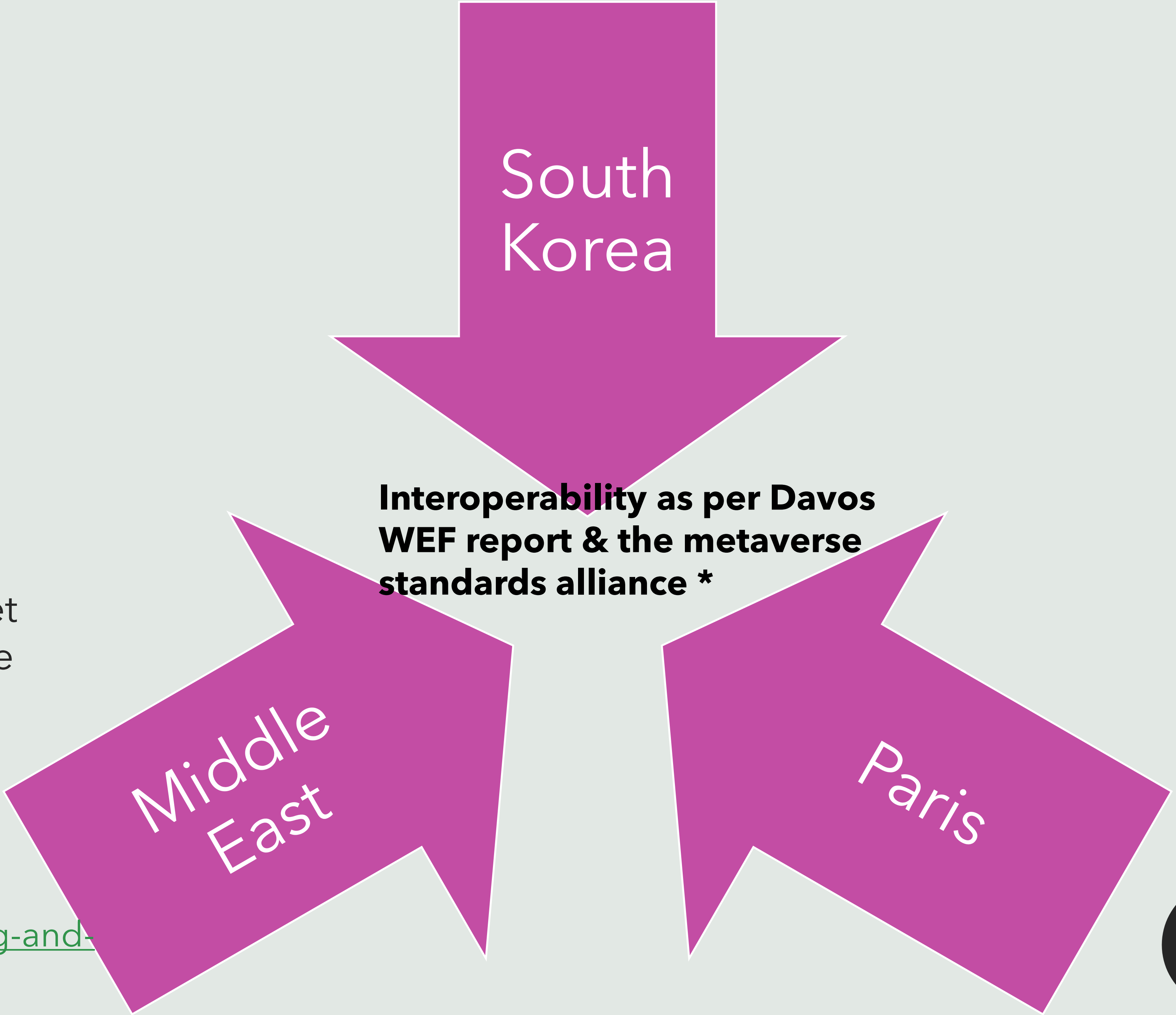
Potential for XR to regulate the proto-metaverse building over the next 5-10 years

Niantic – Meet You Out There & Campfire VR/MR UX

Magic Leap extension with Augmented Reality

We are immersing ourselves

In New Technologies – let's get the foundation right and make sure the infrastructure serves the ideals & visions of the "builders" of Web 4.0



Interoperability as per Davos WEF report & the metaverse standards alliance *

* https://initiatives.weforum.org/defining-and-building-the-metaverse/home

Leading Standards Organizations and Companies Unite to Drive Open Metaverse Interoperability

https://metaverse-standards.org/news/press-releases/leading-standards-organizations-and-companies-unite-to-drive-open-metaverse-interoperability/

中文 / 日本語

Metaverse Standards Forum to foster the development of open standards for the metaverse; Membership is free and open to any organization. Founding members include: 0xSenses, Academy Software Foundation, Adobe, Alibaba, Autodesk, Avataar, Blackshark.ai, CalConnect, Cesium, Daly Realism, Disguise, the Enosema Foundation, Epic Games, the Express Language Foundation, Huawei, IKEA, John Peddie Research, Khronos, Lamina1, Maxon, Meta, Microsoft, NVIDIA, OpenAR Cloud, the Open Geospatial Consortium, Otoy, Perey Research and Consulting, Qualcomm Technologies, Ribose, Sony Interactive Entertainment, Spatial Web Foundation, Unity, VerseMaker, Wayfair, the Web3D Consortium, the World Wide Web Consortium, and the XR Association (XRA)

June 21st, 2022 – Announced today, **The Metaverse Standards Forum** brings together leading standards organizations and companies for industry-wide cooperation on interoperability standards needed to build the open metaverse. The Forum will explore where the lack of interoperability is holding back metaverse deployment and how the work of Standards Developing Organizations (SDOs) defining and evolving needed standards may be coordinated and accelerated. Open to any organization at no cost, the Forum will focus on pragmatic, action-based projects such as implementation prototyping, hackathons, plugfests, and open-source tooling to accelerate the testing and adoption of metaverse standards, while also developing consistent terminology and deployment guidelines.

The metaverse is motivating the novel integration and deployment of diverse technologies for collaborative spatial computing, such as interactive 3D graphics, augmented and virtual reality, photorealistic content authoring, geospatial systems, end-user content tooling, digital twins, real-time collaboration, physical simulation, online economies, multi-user gaming, and more – at new levels of scale and

If we can agree on metaverse safety standards, then we will succeed in creating a better web for all – the "evolution of the internet"

www.linktr.ee/taniapeitzker

Interoperability	Safety	(Cyber) Security – stop hacking	Identity – stop theft	Governance – private + public sectors	International Standards
Child Protection	Protection of minors & vulnerable people of all ages	Anti-sexual harassment/assaults	Law Enforcement	Anti-money laundering	Anti-fraud and other financial crimes
Stopping phishing	Data protection	Privacy like the GDPR	Right to be forgotten	Privacy by Design	Privacy by Default

Federal Information Security Educators (FISSEA) Winter Forum

BREAK

The Forum will resume at 2:45pm ET

#FISSEA2023 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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

Welcome Back!

Brooke Crisp

IT Cybersecurity Specialist
Social Security Administration

How to Spruce Up Your Cybersecurity Awareness Program

Christopher M. Schmigel

Vice President

M&T Bank

How to Spruce Up your Cybersecurity Awareness Program

February 14, 2023

First: The Numbers* …

2022:   1,802 Data Breaches Reported in US
Impacting 440 million individuals

* BankInfoSecurity, "Reported Data Breaches in US Reach Near-Record Highs", 1/25/23

M&T Bank

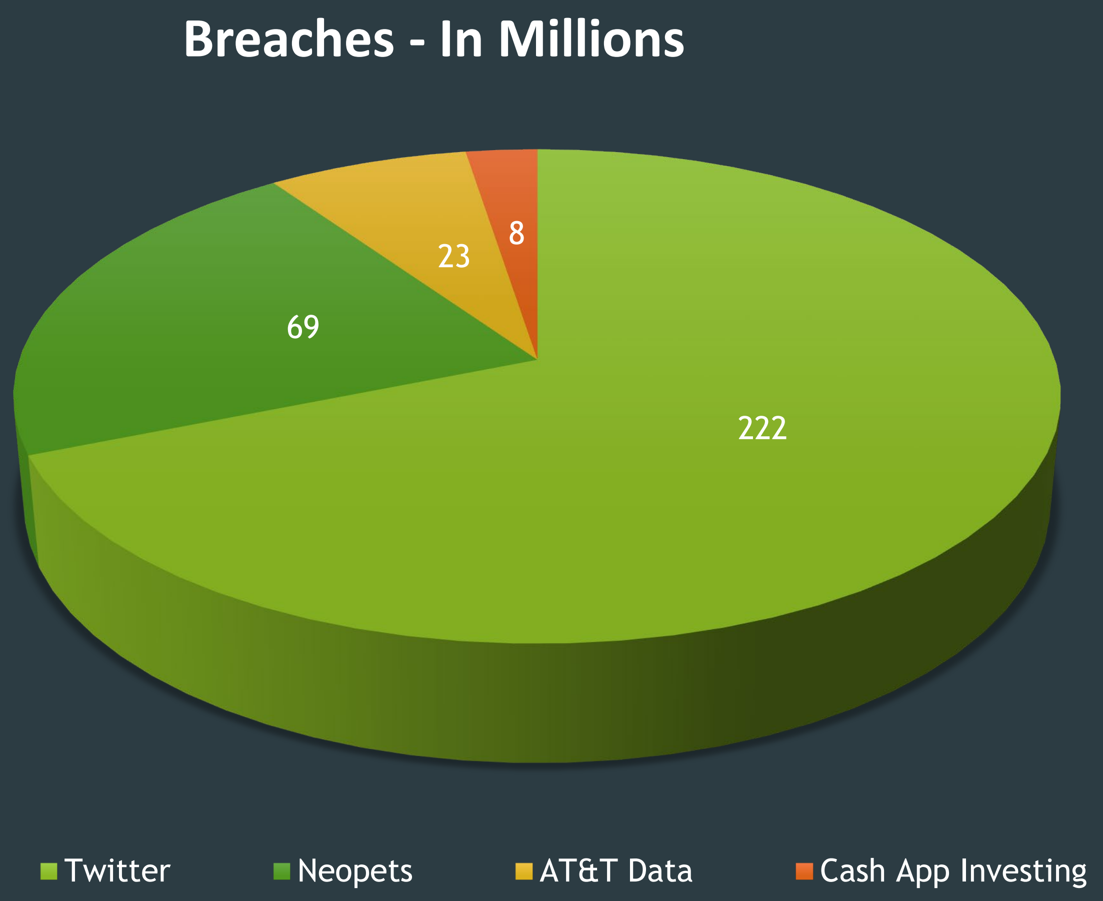
First: The Numbers*…

2022: 1,802 Data Breaches Reported in US
Impacting 440 million individuals

2021: 1,862 breach notifications in US
60 breaches higher than 2022

* BankInfoSecurity, "Reported Data Breaches in US Reach Near-Record Highs", 1/25/23

Now, The Targets…



Cybersecurity Awareness Training

Isn't it like doing laundry?

M&T Bank

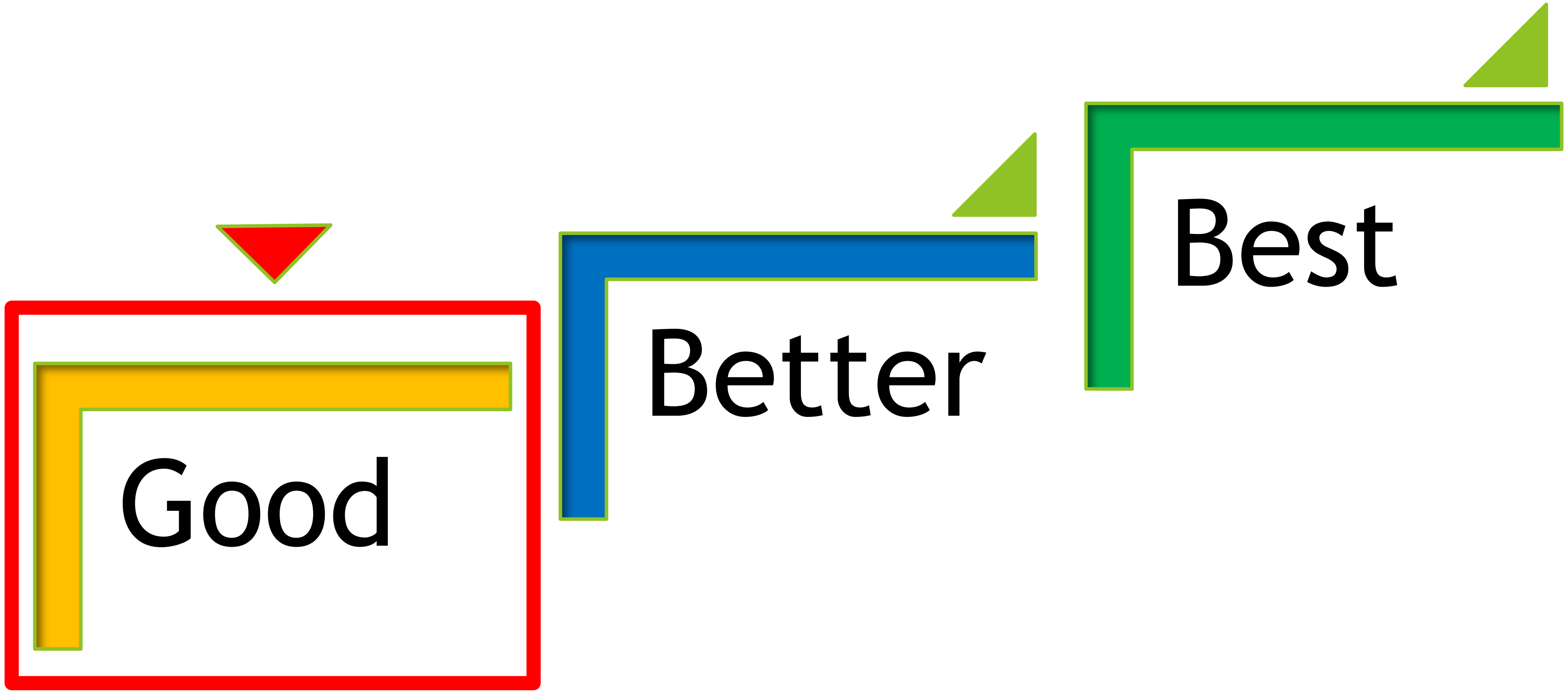
Training Journey...

Good

Better

Best

Training Program: Maturity Progression



Good

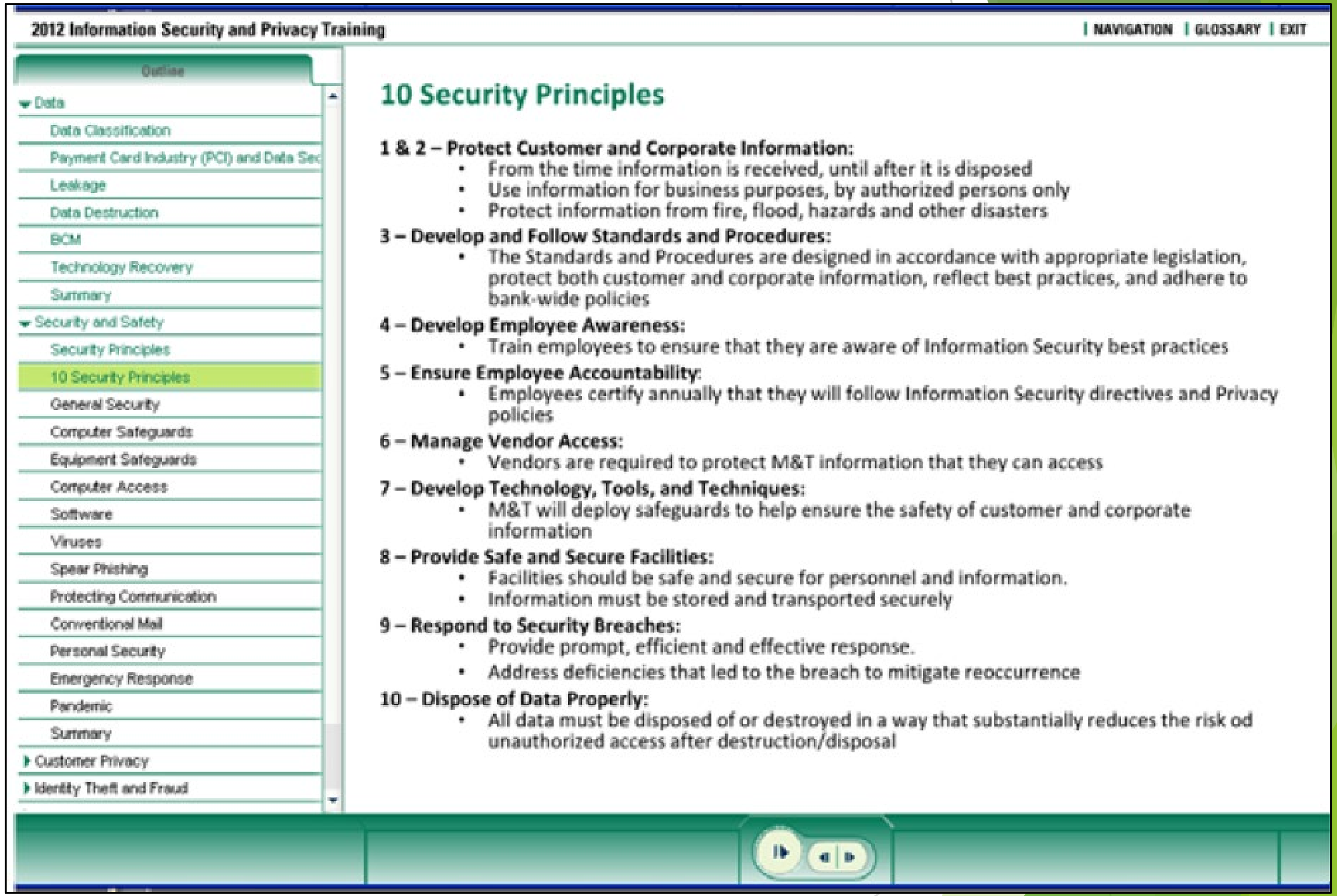
Training

Simulated Phishing

Good

Training:

- ✓ Once a Year
- ✓ Compliance Based
- 👎 Lengthy, dry & non-interactive



2012 Information Security and Privacy Training

10 Security Principles

1 & 2 – Protect Customer and Corporate Information:
- From the time information is received, until after it is disposed
- Use information for business purposes, by authorized persons only
- Protect information from fire, flood, hazards and other disasters

3 – Develop and Follow Standards and Procedures:
- The Standards and Procedures are designed in accordance with appropriate legislation, protect both customer and corporate information, reflect best practices, and adhere to bank-wide policies

4 – Develop Employee Awareness:
- Train employees to ensure that they are aware of Information Security best practices

5 – Ensure Employee Accountability:
- Employees certify annually that they will follow Information Security directives and Privacy policies

6 – Manage Vendor Access:
- Vendors are required to protect M&T information that they can access

7 – Develop Technology, Tools, and Techniques:
- M&T will deploy safeguards to help ensure the safety of customer and corporate information

8 – Provide Safe and Secure Facilities:
- Facilities should be safe and secure for personnel and information.
- Information must be stored and transported securely

9 – Respond to Security Breaches:
- Provide prompt, efficient and effective response.
- Address deficiencies that led to the breach to mitigate reoccurrence

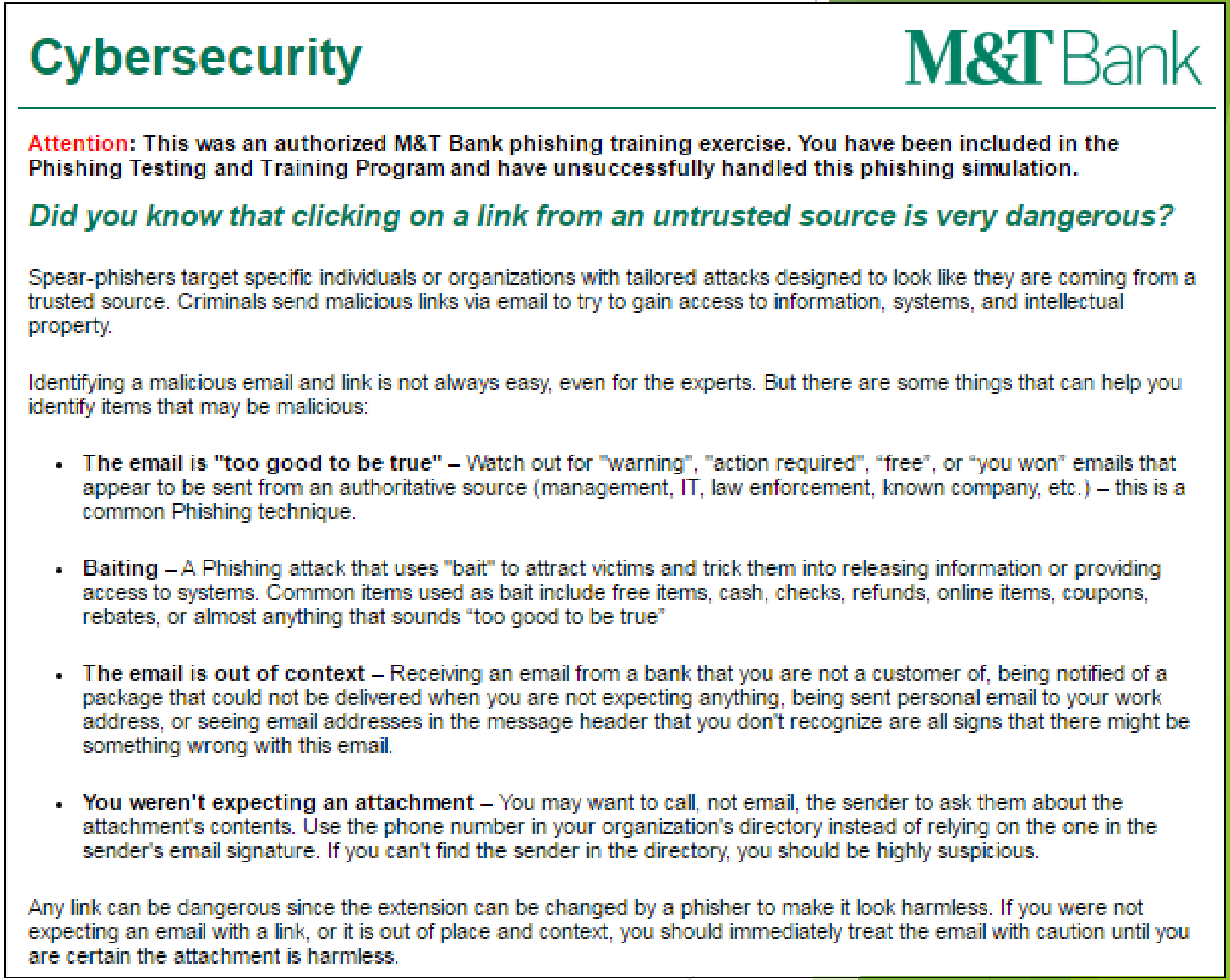
10 – Dispose of Data Properly:
- All data must be disposed of or destroyed in a way that substantially reduces the risk od unauthorized access after destruction/disposal

M&T Bank

Good

Simulated Phishing:

- ✓ Periodic
- 👎 Manual processes involved
- 👎 Wordy Education pages



Cybersecurity

M&T Bank

Attention: This was an authorized M&T Bank phishing training exercise. You have been included in the Phishing Testing and Training Program and have unsuccessfully handled this phishing simulation.

Did you know that clicking on a link from an untrusted source is very dangerous?

Spear-phishers target specific individuals or organizations with tailored attacks designed to look like they are coming from a trusted source. Criminals send malicious links via email to try to gain access to information, systems, and intellectual property.

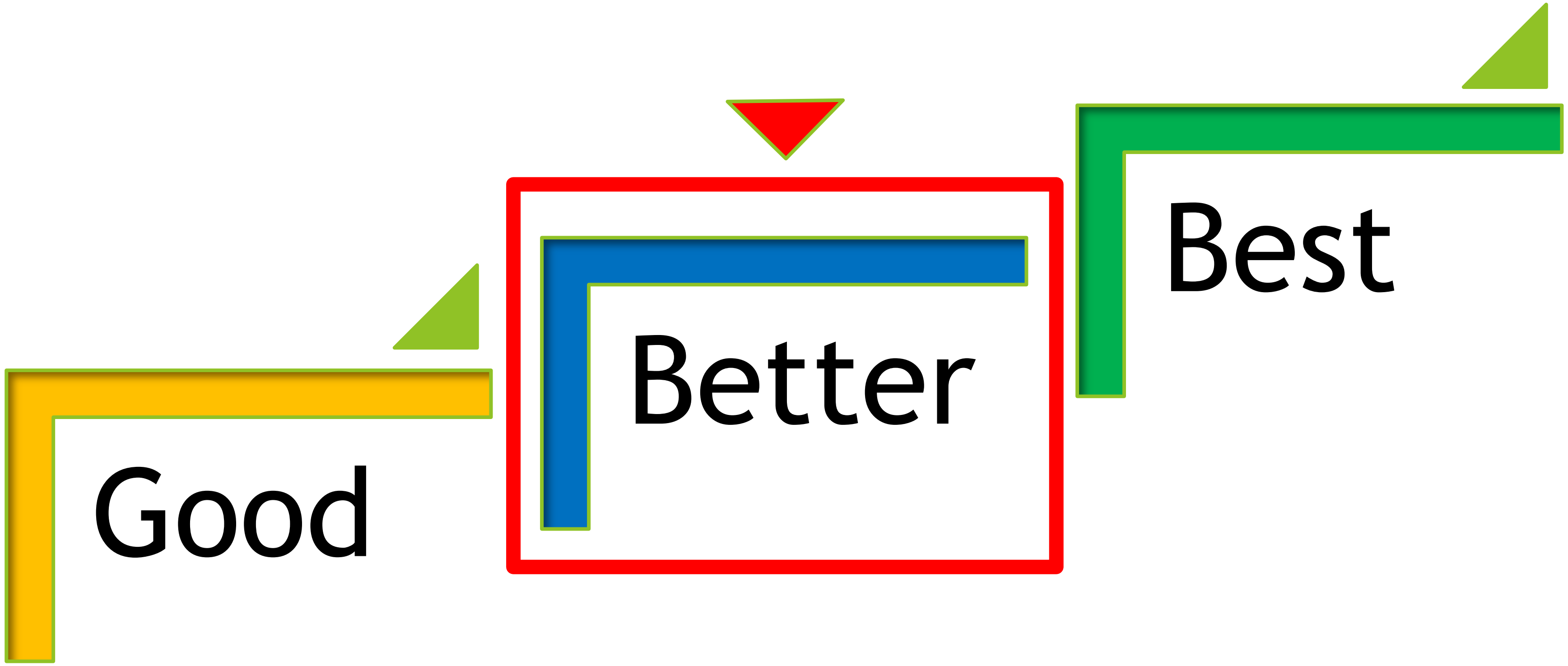
Identifying a malicious email and link is not always easy, even for the experts. But there are some things that can help you identify items that may be malicious:

- **The email is "too good to be true"** – Watch out for "warning", "action required", “free”, or “you won” emails that appear to be sent from an authoritative source (management, IT, law enforcement, known company, etc.) – this is a common Phishing technique.
- **Baiting** – A Phishing attack that uses "bait" to attract victims and trick them into releasing information or providing access to systems. Common items used as bait include free items, cash, checks, refunds, online items, coupons, rebates, or almost anything that sounds “too good to be true”
- **The email is out of context** – Receiving an email from a bank that you are not a customer of, being notified of a package that could not be delivered when you are not expecting anything, being sent personal email to your work address, or seeing email addresses in the message header that you don't recognize are all signs that there might be something wrong with this email.
- **You weren't expecting an attachment** – You may want to call, not email, the sender to ask them about the attachment's contents. Use the phone number in your organization's directory instead of relying on the one in the sender's email signature. If you can't find the sender in the directory, you should be highly suspicious.

Any link can be dangerous since the extension can be changed by a phisher to make it look harmless. If you were not expecting an email with a link, or it is out of place and context, you should immediately treat the email with caution until you are certain the attachment is harmless.

M&T Bank

Training Program: Maturity Progression



M&T Bank

Better

Training IMPROVED

Simulated Phishing IMPROVED

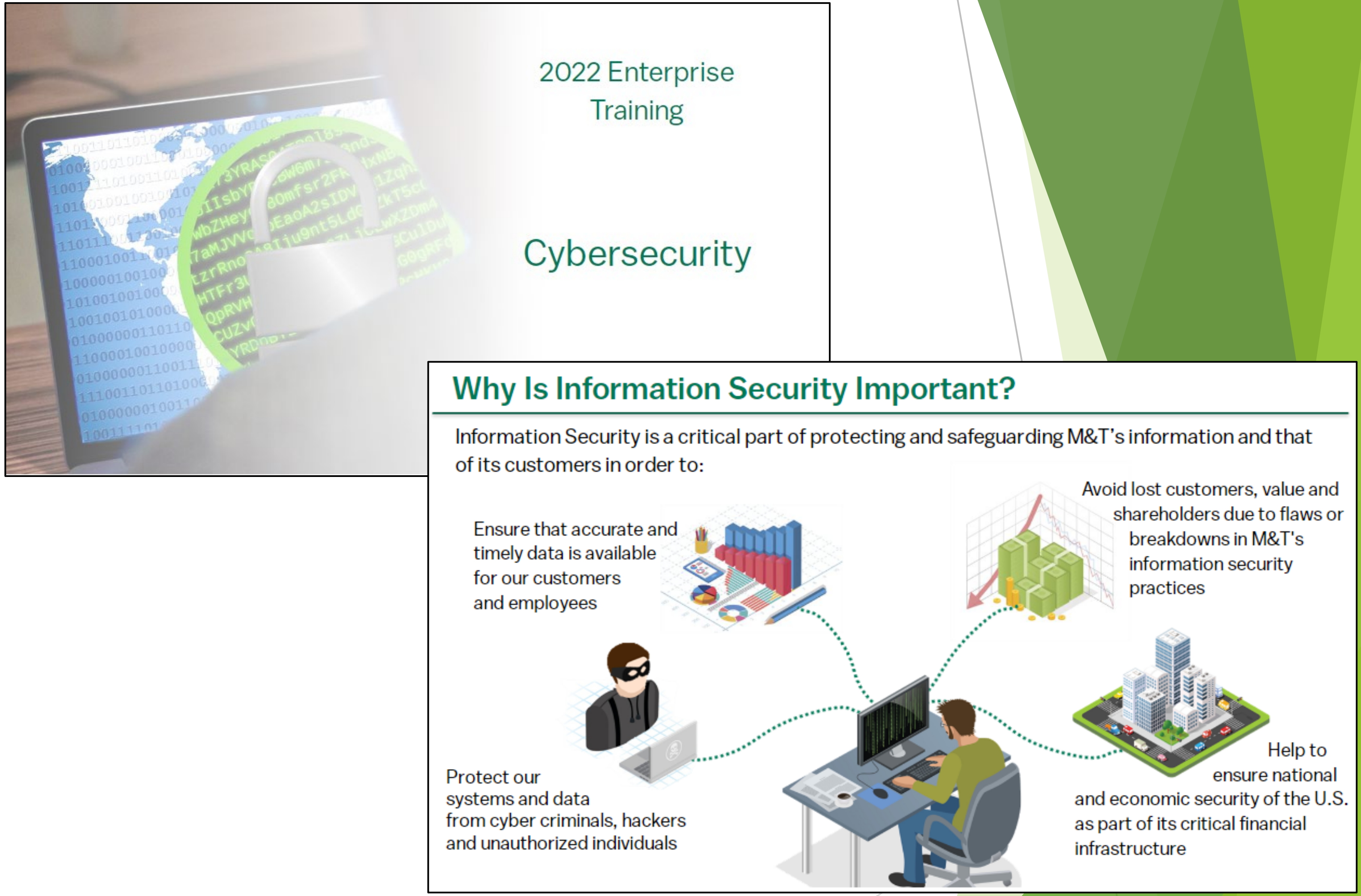
Cybersecurity Awareness Month NEW!

M&T Bank

Better

Training:

- ✓ Once a Year
- ✓ Compliance Based
- ✓ Rebranded
- ✓ Less text
- ✓ Better presentation



2022 Enterprise Training

Cybersecurity

Why Is Information Security Important?

Information Security is a critical part of protecting and safeguarding M&T's information and that of its customers in order to:

Ensure that accurate and timely data is available for our customers and employees

Avoid lost customers, value and shareholders due to flaws or breakdowns in M&T's information security practices

Protect our systems and data from cyber criminals, hackers and unauthorized individuals

Help to ensure national and economic security of the U.S. as part of its critical financial infrastructure

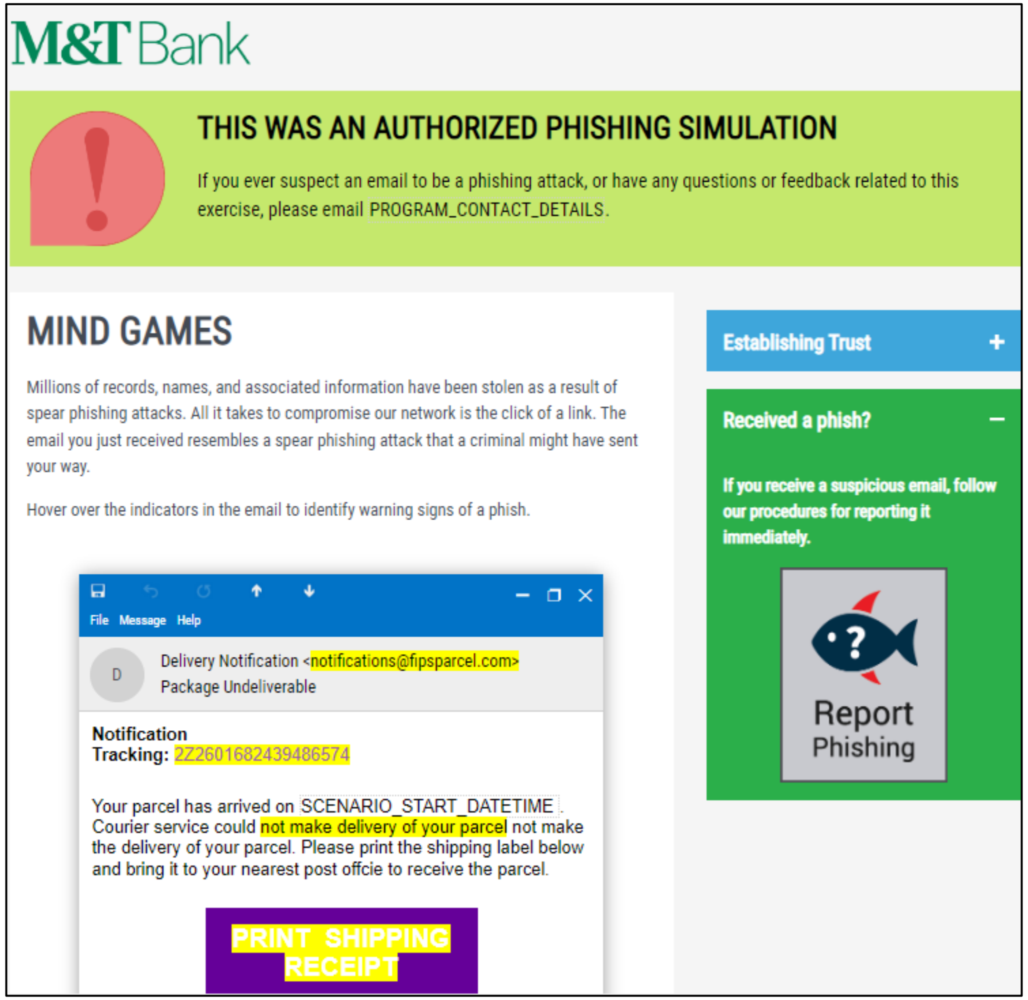
M&T Bank

Better

TLP: GREEN

Simulated Phishing:

- ✓ Increased phishing cadence
- ✓ Added targeted groups
- ✓ Improved education pages
- ✓ Better metrics & reporting
- ✓ Remedial training on 3 hits



M&T Bank

THIS WAS AN AUTHORIZED PHISHING SIMULATION

If you ever suspect an email to be a phishing attack, or have any questions or feedback related to this exercise, please email PROGRAM_CONTACT_DETAILS.

MIND GAMES

Millions of records, names, and associated information have been stolen as a result of spear phishing attacks. All it takes to compromise our network is the click of a link. The email you just received resembles a spear phishing attack that a criminal might have sent your way.

Hover over the indicators in the email to identify warning signs of a phish.

Delivery Notification <notifications@fipsparcel.com>
Package Undeliverable

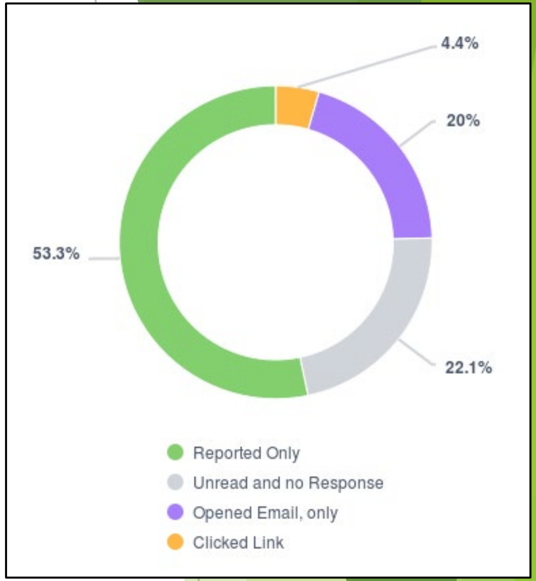
Notification
Tracking: 2Z2601682439486574

Your parcel has arrived on SCENARIO_START_DATETIME . Courier service could not make delivery of your parcel not make the delivery of your parcel. Please print the shipping label below and bring it to your nearest post offcie to receive the parcel.

Establishing Trust +

Received a phish? –

If you receive a suspicious email, follow our procedures for reporting it immediately.



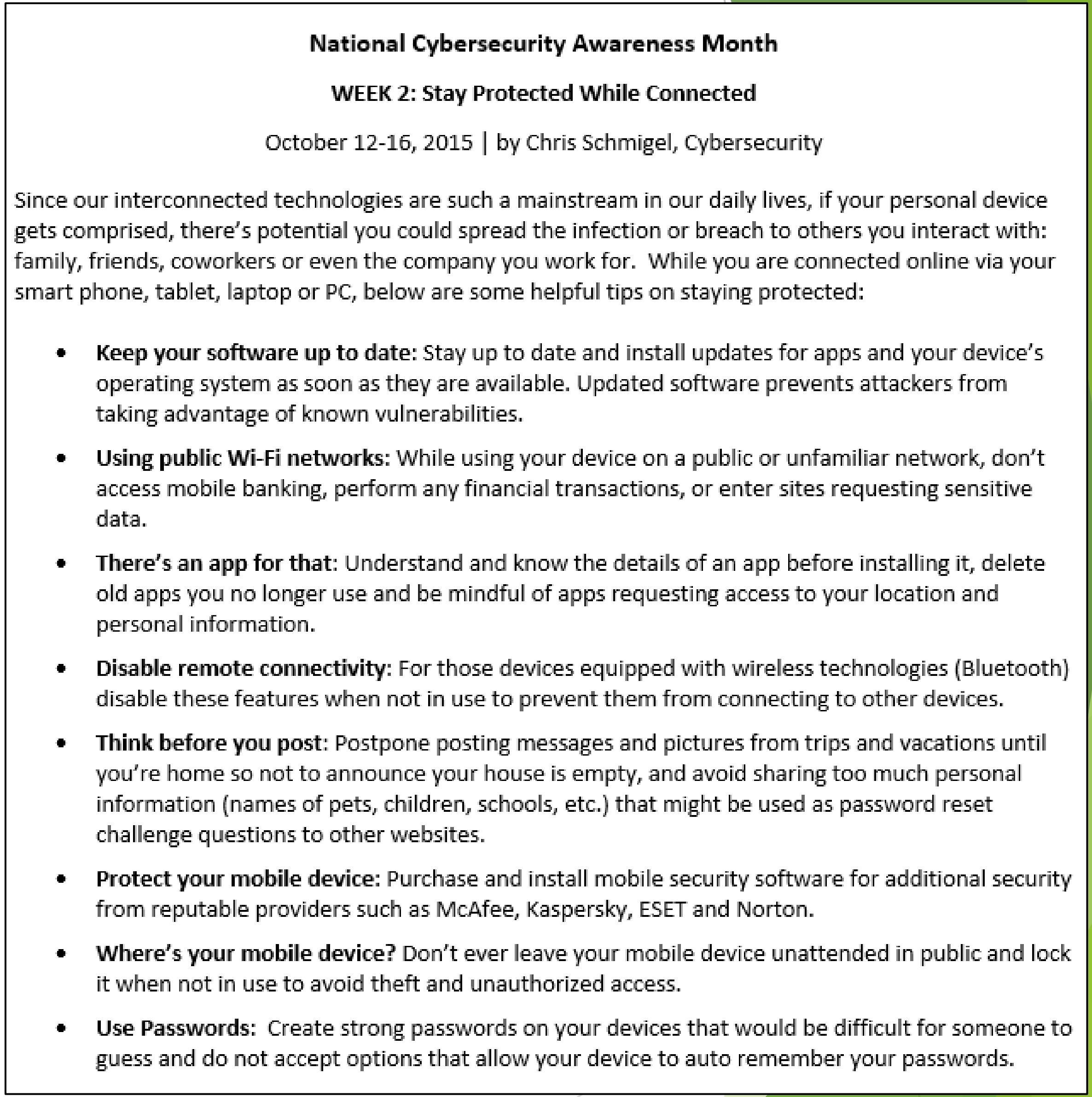
Recipient Response	%
Susceptible 0 Times	87.6%
Susceptible 1 Time	10.4%
Susceptible 2 Times	1.6%
Susceptible 3 Times	0.3%
Susceptible 4 Times	0.1%
Susceptible 5+ Times	0.0%
Grand Total	**100.0%**

M&T Bank

Better

Cybersecurity Awareness Month:

- ✓ Weekly articles
- ✓ Hosted on our intranet site
- 👎 Nice idea, but no one knew of them
- 👎 Tips good, but too much and wordy



National Cybersecurity Awareness Month

WEEK 2: Stay Protected While Connected

October 12-16, 2015 | by Chris Schmigel, Cybersecurity

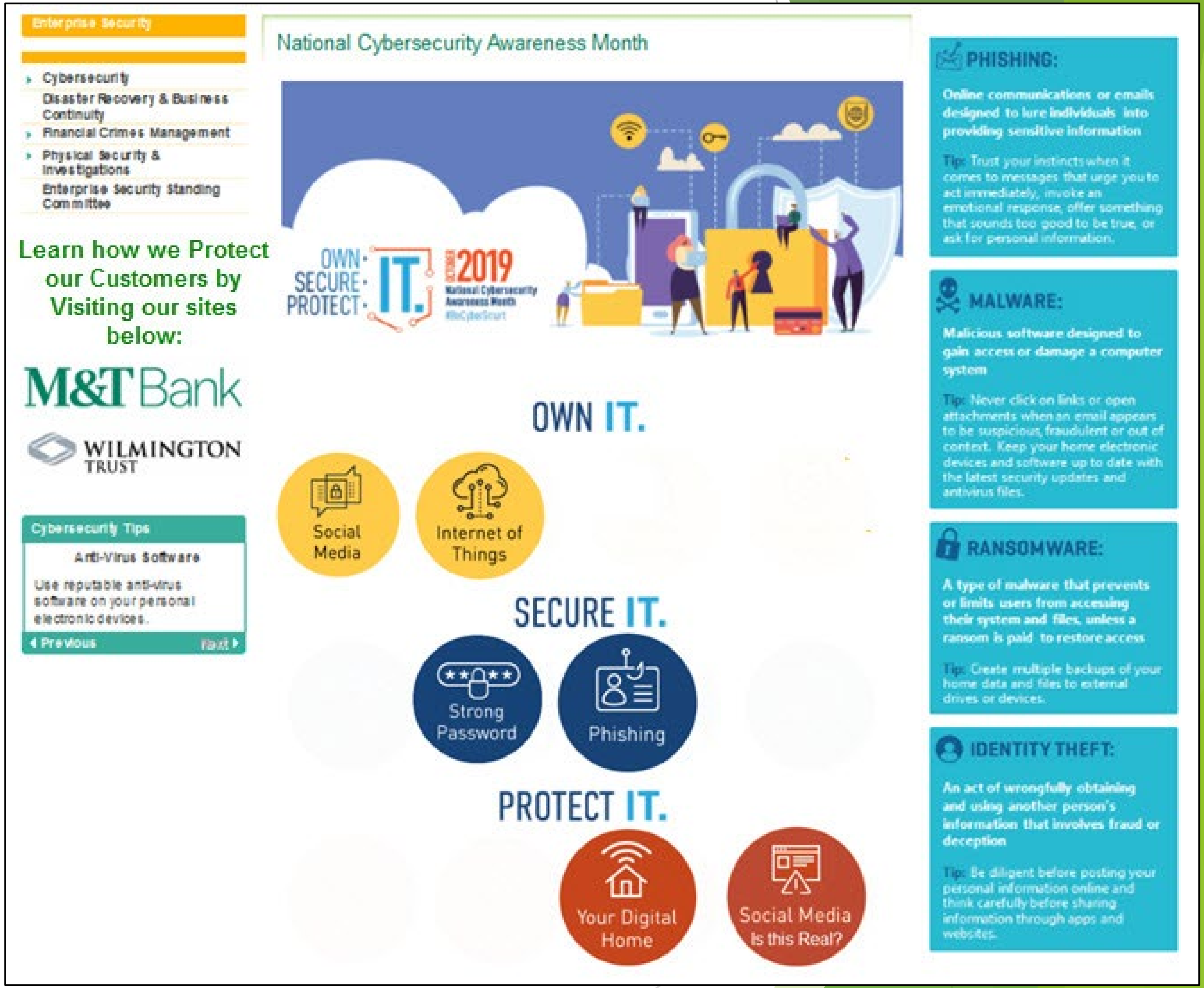
Since our interconnected technologies are such a mainstream in our daily lives, if your personal device gets comprised, there's potential you could spread the infection or breach to others you interact with: family, friends, coworkers or even the company you work for. While you are connected online via your smart phone, tablet, laptop or PC, below are some helpful tips on staying protected:

- **Keep your software up to date:** Stay up to date and install updates for apps and your device's operating system as soon as they are available. Updated software prevents attackers from taking advantage of known vulnerabilities.
- **Using public Wi-Fi networks:** While using your device on a public or unfamiliar network, don't access mobile banking, perform any financial transactions, or enter sites requesting sensitive data.
- **There's an app for that**: Understand and know the details of an app before installing it, delete old apps you no longer use and be mindful of apps requesting access to your location and personal information.
- **Disable remote connectivity:** For those devices equipped with wireless technologies (Bluetooth) disable these features when not in use to prevent them from connecting to other devices.
- **Think before you post**: Postpone posting messages and pictures from trips and vacations until you're home so not to announce your house is empty, and avoid sharing too much personal information (names of pets, children, schools, etc.) that might be used as password reset challenge questions to other websites.
- **Protect your mobile device:** Purchase and install mobile security software for additional security from reputable providers such as McAfee, Kaspersky, ESET and Norton.
- **Where's your mobile device?** Don't ever leave your mobile device unattended in public and lock it when not in use to avoid theft and unauthorized access.
- **Use Passwords:** Create strong passwords on your devices that would be difficult for someone to guess and do not accept options that allow your device to auto remember your passwords.

Better

Cybersecurity Awareness Month:

- ✓ Dedicated intranet page
- ✓ Leveraged existing articles
- 👎 Intent was good,
  but not our site's traffic
- 👎 Too busy, long and wordy



Enterprise Security

- Cybersecurity
- Disaster Recovery & Business Continuity
- Financial Crimes Management
- Physical Security & Investigations
- Enterprise Security Standing Committee

Learn how we Protect our Customers by Visiting our sites below:

M&T Bank

WILMINGTON TRUST

Cybersecurity Tips

Anti-Virus Software

Use reputable anti-virus software on your personal electronic devices.

◀ Previous Next ▶

National Cybersecurity Awareness Month

OWN IT.

Social Media

Internet of Things

SECURE IT.

Strong Password

Phishing

PROTECT IT.

Your Digital Home

Social Media Is this Real?

PHISHING:

Online communications or emails designed to lure individuals into providing sensitive information

Tip: Trust your instincts when it comes to messages that urge you to act immediately, invoke an emotional response, offer something that sounds too good to be true, or ask for personal information.

MALWARE:

Malicious software designed to gain access or damage a computer system

Tip: Never click on links or open attachments when an email appears to be suspicious, fraudulent or out of context. Keep your home electronic devices and software up to date with the latest security updates and antivirus files.

RANSOMWARE:

A type of malware that prevents or limits users from accessing their system and files, unless a ransom is paid to restore access

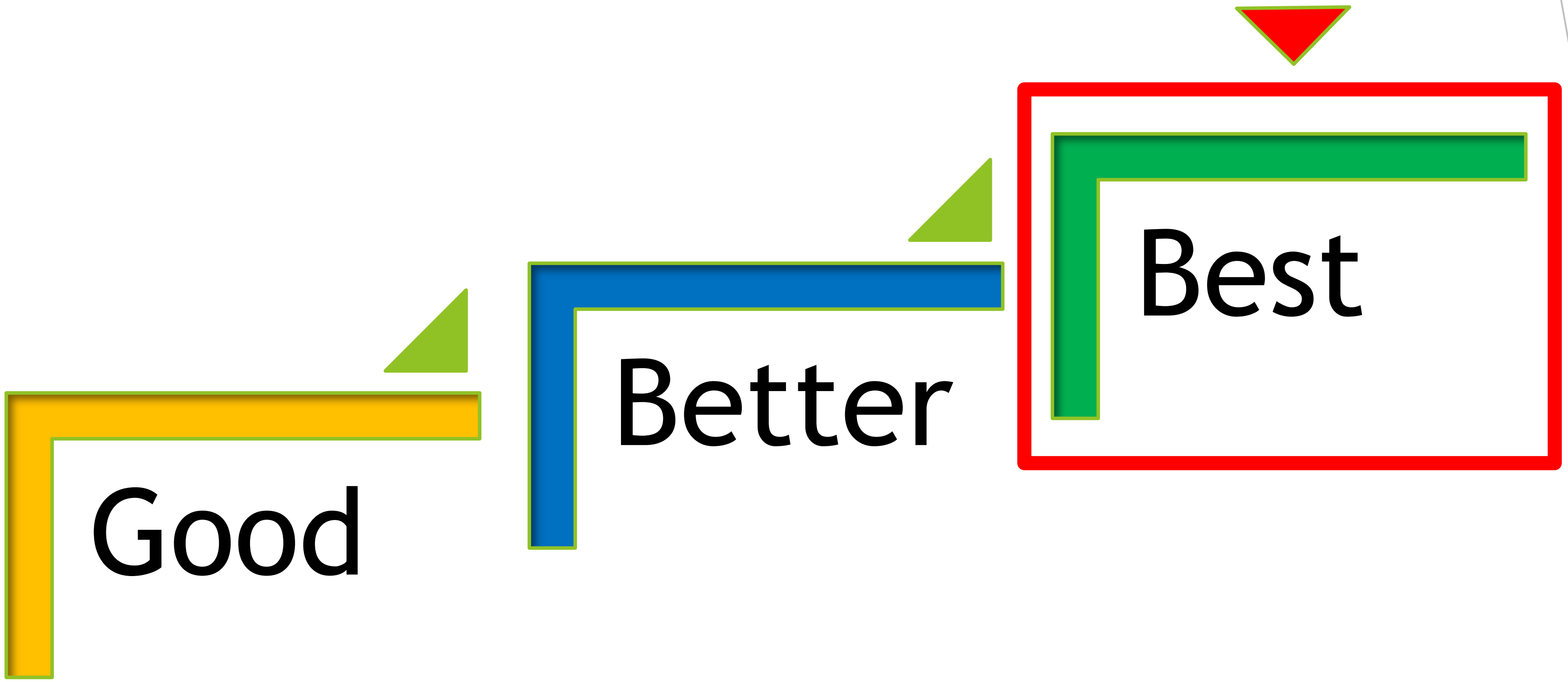
Tip: Create multiple backups of your home data and files to external drives or devices.

IDENTITY THEFT:

An act of wrongfully obtaining and using another person's information that involves fraud or deception

Tip: Be diligent before posting your personal information online and think carefully before sharing information through apps and websites.

Training Program: Maturity Progression



Good

Better

Best

M&T Bank

Best

Training

Targeted Training NEW!

Simulated Phishing IMPROVED

Periodic Awareness NEW!

Cybersecurity Champions NEW!

Cybersecurity Awareness Month IMPROVED

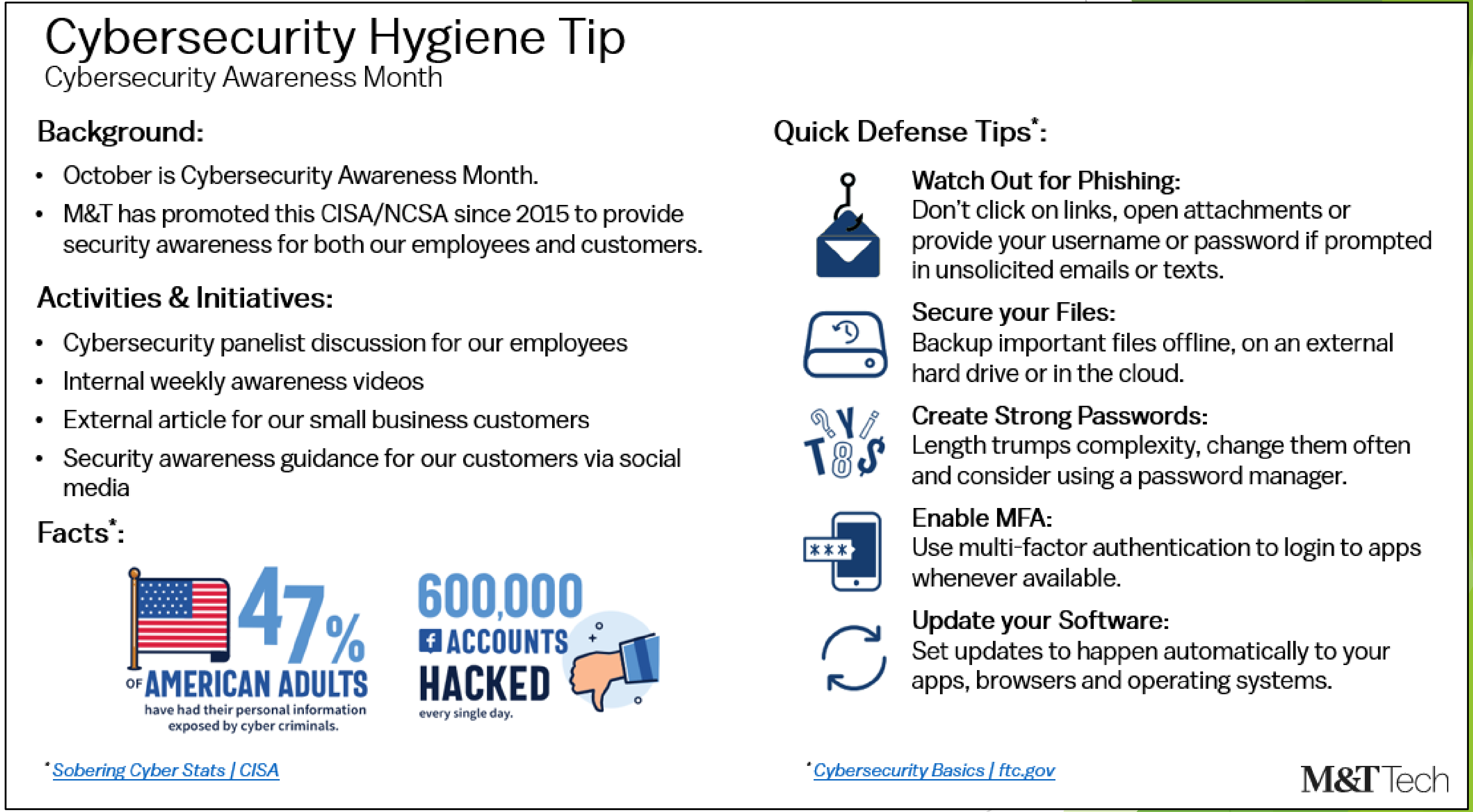
Best

Training:

- ✓ Compliance Based
- ✓ Enterprise wide

Targeted Training:

- ✓ Board of Directors



Cybersecurity Hygiene Tip

Cybersecurity Awareness Month

Background:

- October is Cybersecurity Awareness Month.
- M&T has promoted this CISA/NCSA since 2015 to provide security awareness for both our employees and customers.

Activities & Initiatives:

- Cybersecurity panelist discussion for our employees
- Internal weekly awareness videos
- External article for our small business customers
- Security awareness guidance for our customers via social media

Facts*:

47% OF AMERICAN ADULTS have had their personal information exposed by cyber criminals.

600,000 ACCOUNTS HACKED every single day.

*Sobering Cyber Stats | CISA

Quick Defense Tips*:

Watch Out for Phishing: Don't click on links, open attachments or provide your username or password if prompted in unsolicited emails or texts.

Secure your Files: Backup important files offline, on an external hard drive or in the cloud.

Create Strong Passwords: Length trumps complexity, change them often and consider using a password manager.

Enable MFA: Use multi-factor authentication to login to apps whenever available.

Update your Software: Set updates to happen automatically to your apps, browsers and operating systems.

*Cybersecurity Basics | ftc.gov

M&T Tech

M&T Bank

Best

Training:

- ✓ Compliance Based
- ✓ Enterprise wide

Targeted Training:

- ✓ Board of Directors
- ✓ Privileged Users

Privileged & Elevated Access Training

Cybersecurity

M&T Bank

Did you know?

Because of the access they have, high privileged users have an elevated risk against them. The goal of every cyber attacker is access to data, systems and other resources. The more privileged the victim, the more access attackers have - and the more damage they can do.

Proofpoint, "The Human Factor 2022"

Best

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers

Best

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers

M&T Bank

Best

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers

Best

Phishing: Carrot or the Stick?

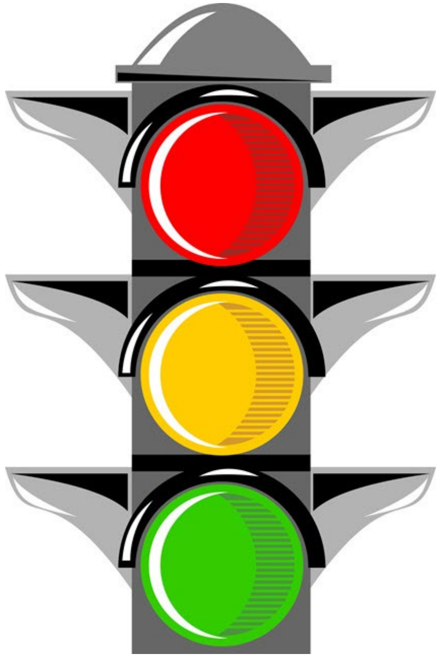
M&T Bank

Best

TLP: GREEN

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers



Recipient Response	%
Susceptible 0 Times	87.6%
Susceptible 1 Time	10.4%
Susceptible 2 Times	1.6%
Susceptible 3 Times	0.3%
Susceptible 4 Times	0.1%
Susceptible 5+ Times	0.0%
Grand Total	**100.0%**

TLP: GREEN

Best

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers
- ✓ Enhanced training reporting

- Remedial phishing training to employees after 3rd click
- Enhanced WBT Reporting & Escalations for Past Due Employees

Recipient Response	%
Susceptible 0 Times	87.6%
Susceptible 1 Time	10.4%
Susceptible 2 Times	1.6%
Susceptible 3 Times	0.3%
Susceptible 4 Times	0.1%
Susceptible 5+ Times	0.0%
Grand Total	**100.0%**

M&T Bank

Best

TLP: GREEN

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers
- ✓ Enhanced training reporting
- ✓ Repeat clicker escalation

- Remedial phishing training to employees after 3rd click
- Enhanced WBT Reporting & Escalations for Past Due Employees

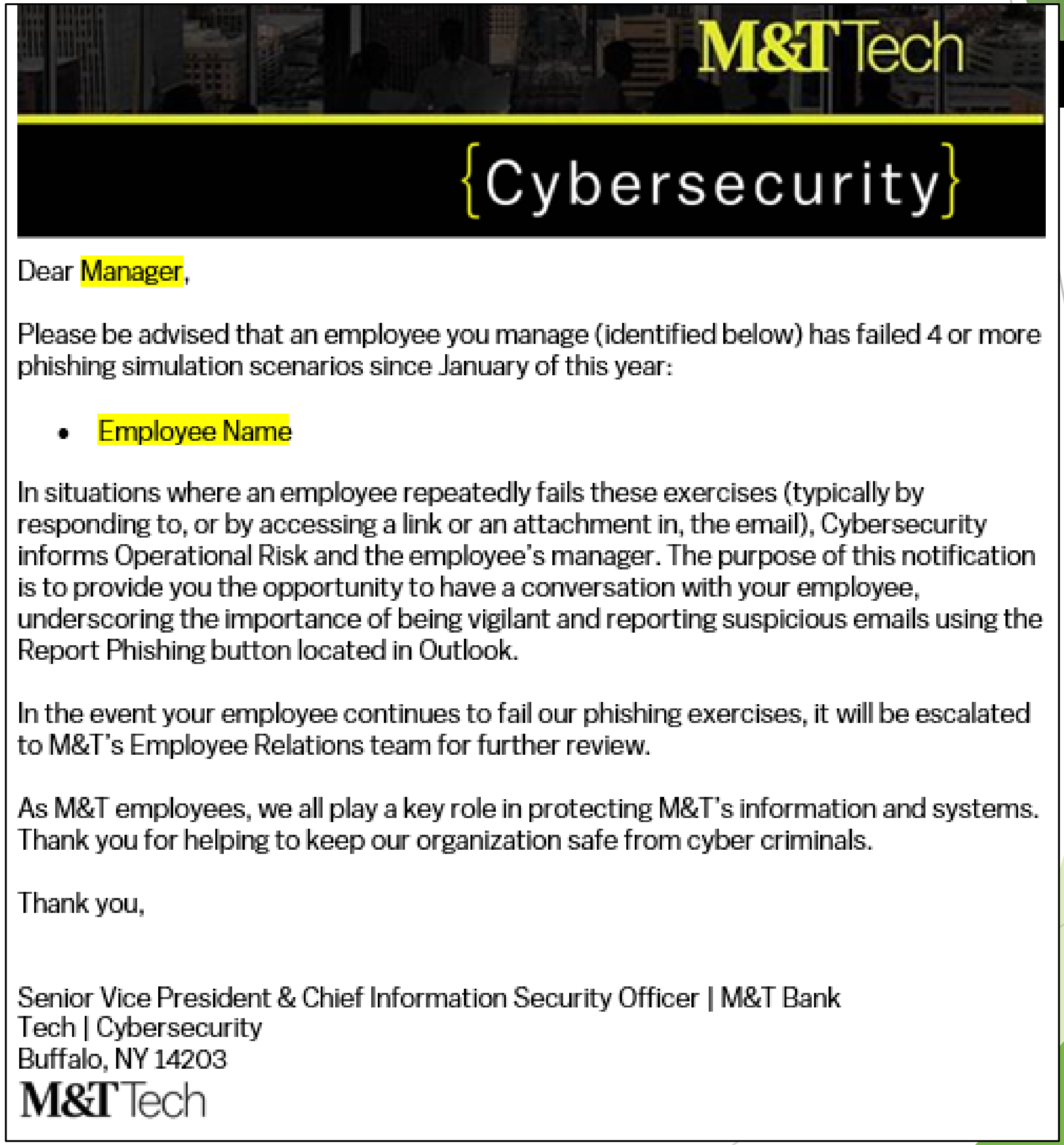
- Share Repeat Clickers with Risk Officers
- CISO email to employee’s supervisor

Recipient Response	%
Susceptible 0 Times	87.6%
Susceptible 1 Time	10.4%
Susceptible 2 Times	1.6%
Susceptible 3 Times	0.3%
Susceptible 4 Times	0.1%
Susceptible 5+ Times	0.0%
Grand Total	**100.0%**

Best

Simulated Phishing:

- ✓ Include contingent workers
- ✓ Annual remedial training refresh
- ✓ Share with Risk Officers
- ✓ Enhanced training reporting
- ✓ Repeat clicker escalation



M&T Tech

{Cybersecurity}

Dear Manager,

Please be advised that an employee you manage (identified below) has failed 4 or more phishing simulation scenarios since January of this year:

- Employee Name

In situations where an employee repeatedly fails these exercises (typically by responding to, or by accessing a link or an attachment in, the email), Cybersecurity informs Operational Risk and the employee's manager. The purpose of this notification is to provide you the opportunity to have a conversation with your employee, underscoring the importance of being vigilant and reporting suspicious emails using the Report Phishing button located in Outlook.

In the event your employee continues to fail our phishing exercises, it will be escalated to M&T's Employee Relations team for further review.

As M&T employees, we all play a key role in protecting M&T's information and systems. Thank you for helping to keep our organization safe from cyber criminals.

Thank you,

Senior Vice President & Chief Information Security Officer | M&T Bank
Tech | Cybersecurity
Buffalo, NY 14203
M&T Tech

TLP: GREEN

TLP: GREEN

Best

Simulated Phishing:

✓ Include contingent workers

✓ Annual remedial training refresh

✓ Share with Risk Officers

✓ Enhanced training reporting

✓ Repeat clicker escalation

✓ Inform HR of offenders

- Remedial phishing training to employees after 3rd click
- Enhanced WBT Reporting & Escalations for Past Due Employees

- Share Repeat Clickers with Risk Officers
- CISO email to employee’s supervisor

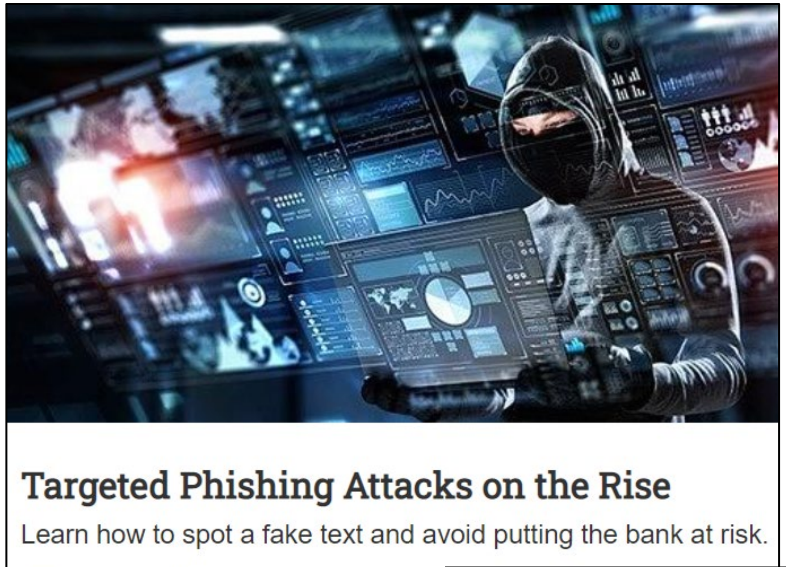
- Employee Relations: Address with Employee & Manager
  - Educate them of the risk
  - Determine if additional training/coaching is required
  - Add to the employee’s Annual Performance Objective

Recipient Response	%
Susceptible 0 Times	87.6%
Susceptible 1 Time	10.4%
Susceptible 2 Times	1.6%
Susceptible 3 Times	0.3%
Susceptible 4 Times	0.1%
Susceptible 5+ Times	0.0%
Grand Total	**100.0%**

Best

Periodic Awareness:

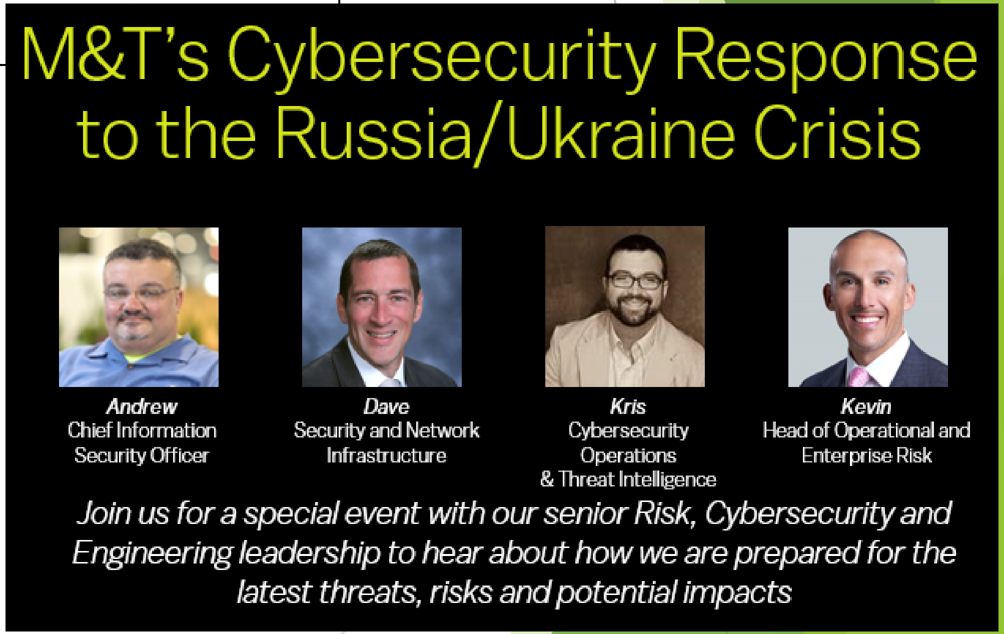
- ✓ Increased the frequency
- ✓ Partnered with Marketing & Communications
- ✓ Expanded the channels
- ✓ Used alternate delivery formats



Targeted Phishing Attacks on the Rise

Learn how to spot a fake text and avoid putting the bank at risk.

C1 CommunityONE
Tuesday, August 16, 2022



M&T's Cybersecurity Response to the Russia/Ukraine Crisis

Andrew
Chief Information Security Officer

Dave
Security and Network Infrastructure

Kris
Cybersecurity Operations & Threat Intelligence

Kevin
Head of Operational and Enterprise Risk

Join us for a special event with our senior Risk, Cybersecurity and Engineering leadership to hear about how we are prepared for the latest threats, risks and potential impacts

Best

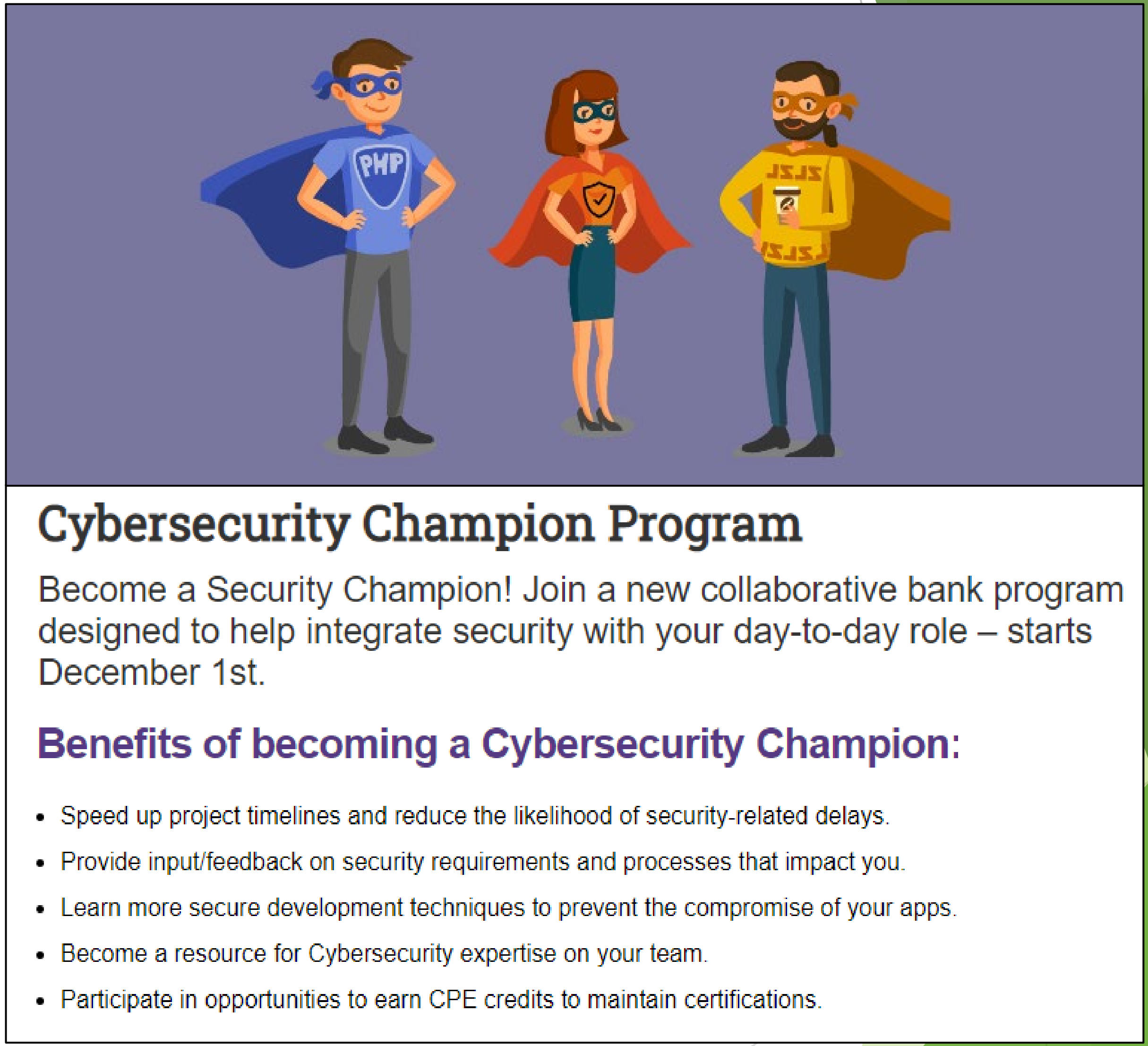
Periodic Awareness:

- ✓ Increased the frequency
- ✓ Partnered with Marketing & Communications
- ✓ Expanded the channels
- ✓ Used alternate delivery formats

Best

Periodic Awareness:

- ✓ Partnered with Marketing & Communications
- ✓ Expanded the channels
- ✓ Used alternate delivery formats
- ✓ Increased the frequency
- ✓ Created Cybersecurity Champions program



Cybersecurity Champion Program

Become a Security Champion! Join a new collaborative bank program designed to help integrate security with your day-to-day role – starts December 1st.

Benefits of becoming a Cybersecurity Champion:

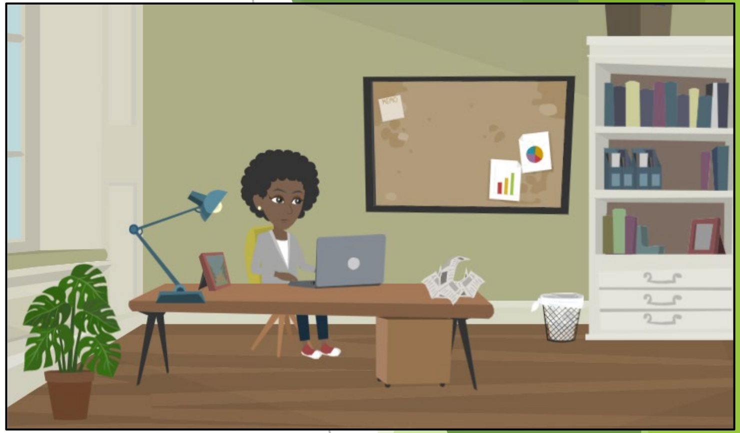
- Speed up project timelines and reduce the likelihood of security-related delays.
- Provide input/feedback on security requirements and processes that impact you.
- Learn more secure development techniques to prevent the compromise of your apps.
- Become a resource for Cybersecurity expertise on your team.
- Participate in opportunities to earn CPE credits to maintain certifications.

Best

Cybersecurity Awareness Month:

- ✓ Acquired licenses for animation software & graphics library
- ✓ Created short weekly 1 ½ minute videos

M&T Bank
CYBERSECURITY AWARENESS MONTH
Protect Yourself from Phishing



Be Careful with Your Assumptions

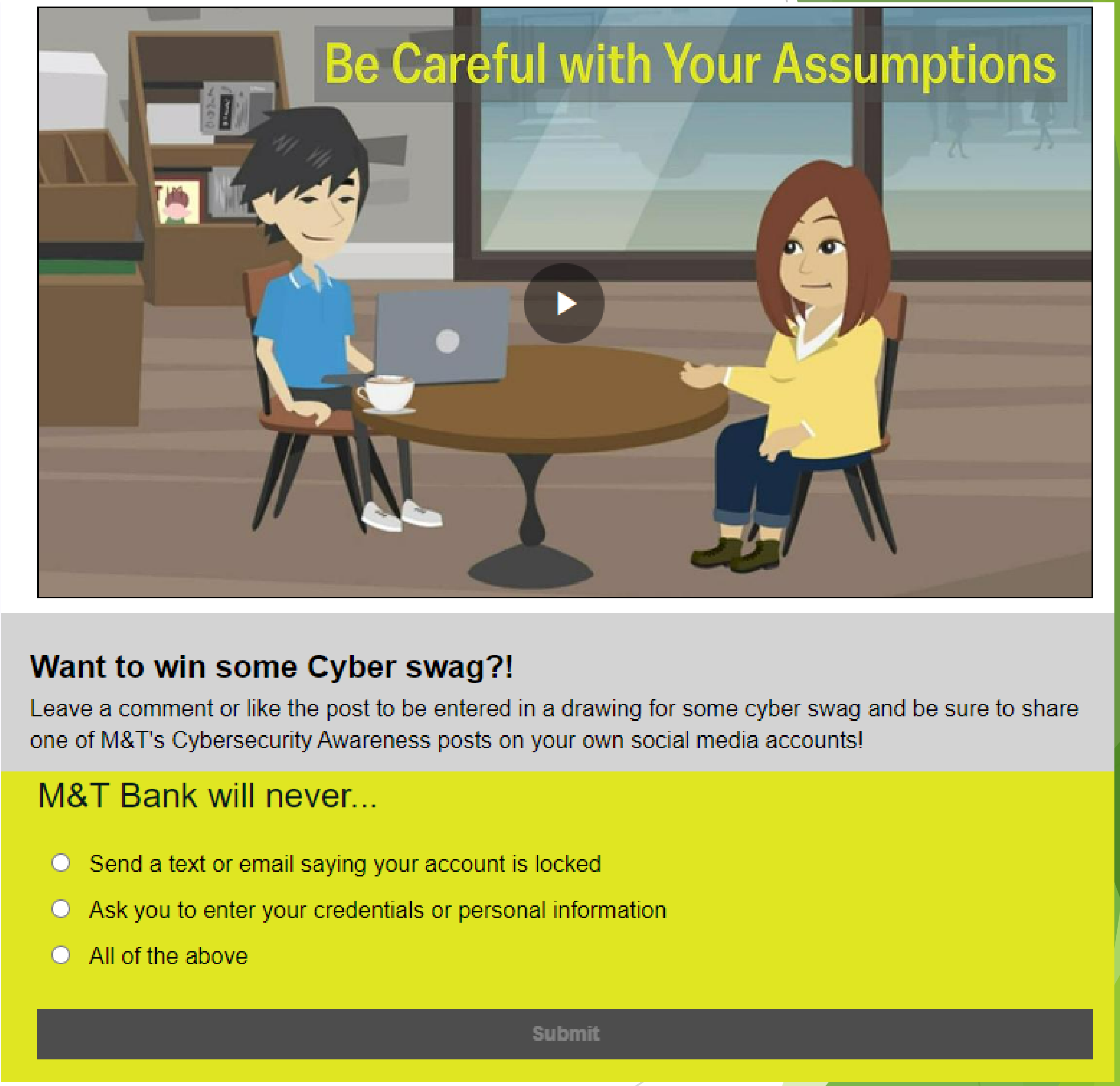
M&T Bank
CYBERSECURITY AWARENESS MONTH
Creating & Safeguarding Your Passwords

M&T Bank

Best

Cybersecurity Awareness Month:

- ✓ Acquired licenses for animation software & graphics library
- ✓ Created short weekly 1 ½ minute videos
- ✓ Launched contest to win swag



Be Careful with Your Assumptions

Want to win some Cyber swag?!

Leave a comment or like the post to be entered in a drawing for some cyber swag and be sure to share one of M&T's Cybersecurity Awareness posts on your own social media accounts!

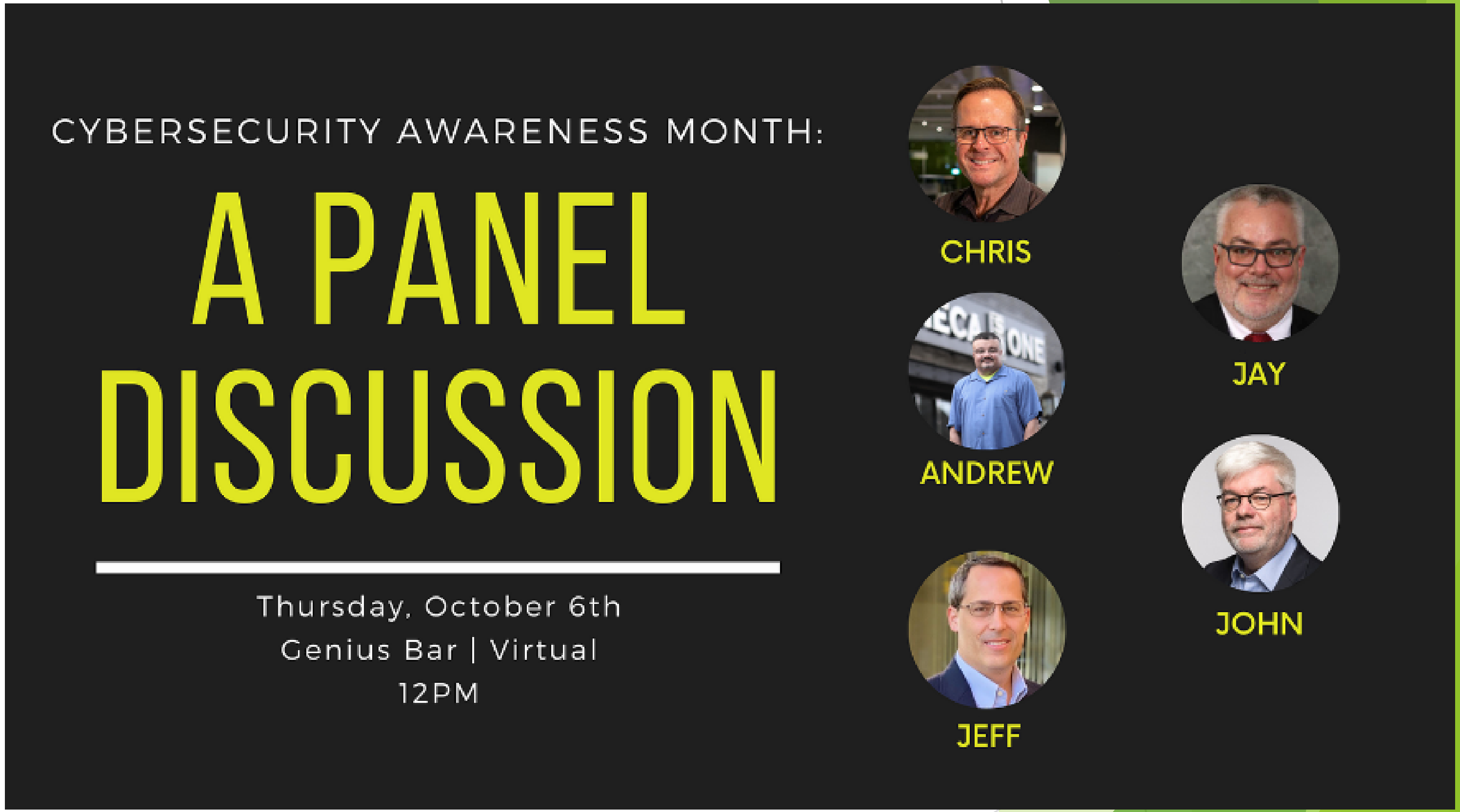
M&T Bank will never...

- ○ Send a text or email saying your account is locked
- ○ Ask you to enter your credentials or personal information
- ○ All of the above

Best

Cybersecurity Awareness Month:

- ✓ Acquired licenses for animation software & graphics library
- ✓ Created short weekly 1 ½ minute videos
- ✓ Launched contest to win swag
- ✓ Hosted live panel discussion



CYBERSECURITY AWARENESS MONTH:

A PANEL DISCUSSION

Thursday, October 6th
Genius Bar | Virtual
12PM

CHRIS

ANDREW

JEFF

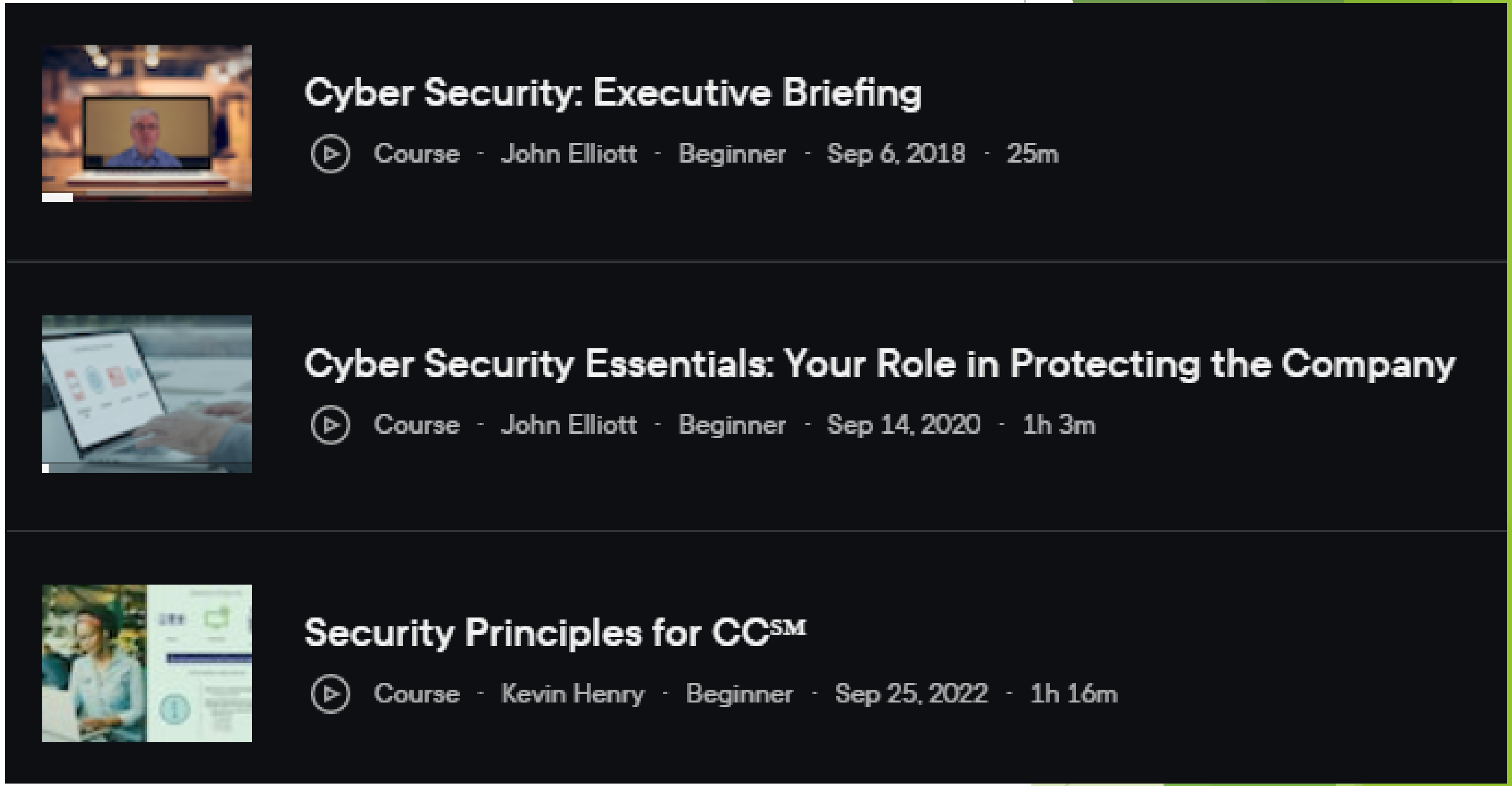
JAY

JOHN

Best

Cybersecurity Awareness Month:

- ✓ Acquired licenses for animation software & graphics library
- ✓ Created short weekly 1 ½ minute videos
- ✓ Launched contest to win swag
- ✓ Hosted live panel discussion



Cyber Security: Executive Briefing

Course · John Elliott · Beginner · Sep 6, 2018 · 25m

Cyber Security Essentials: Your Role in Protecting the Company

Course · John Elliott · Beginner · Sep 14, 2020 · 1h 3m

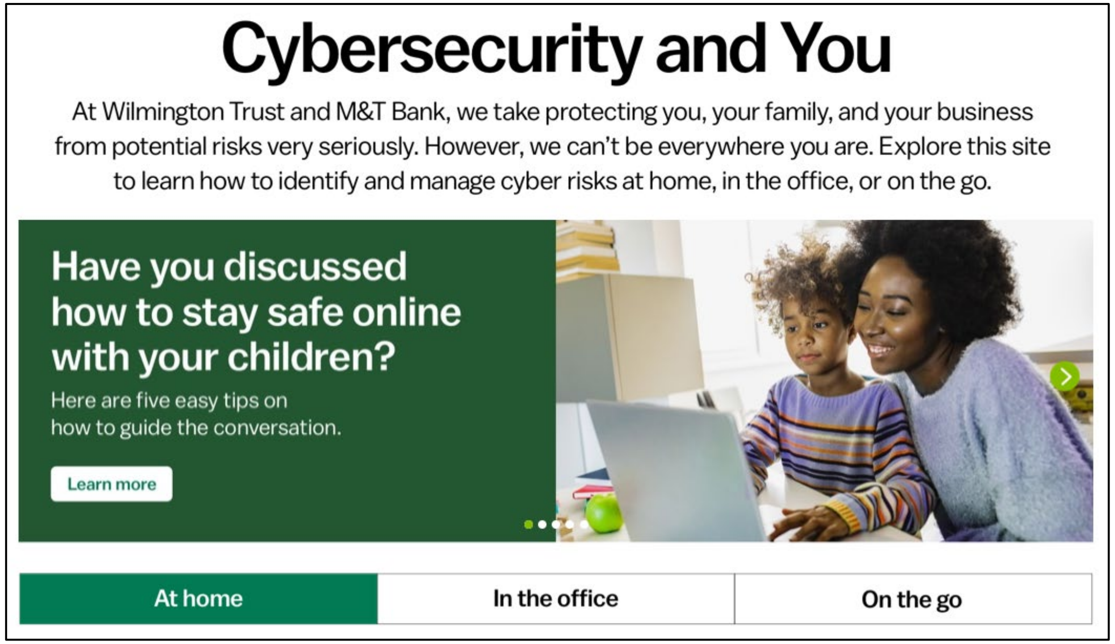
Security Principles for CC℠

Course · Kevin Henry · Beginner · Sep 25, 2022 · 1h 16m

M&T Bank

Best

Customer Awareness Training:



Cybersecurity and You

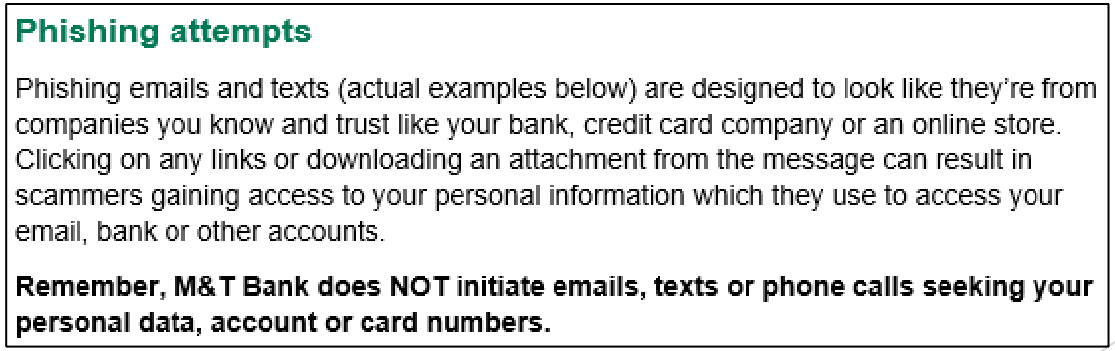
At Wilmington Trust and M&T Bank, we take protecting you, your family, and your business from potential risks very seriously. However, we can't be everywhere you are. Explore this site to learn how to identify and manage cyber risks at home, in the office, or on the go.

Have you discussed how to stay safe online with your children?

Here are five easy tips on how to guide the conversation.

Learn more

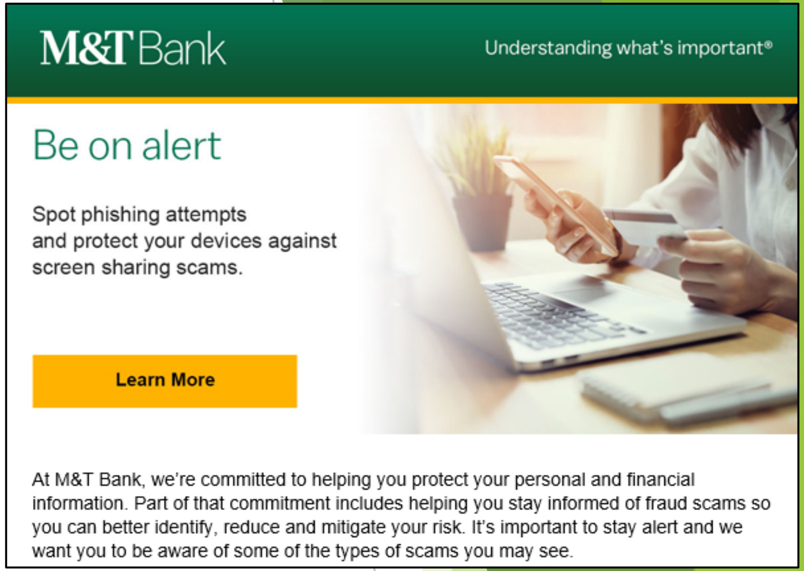
At home	In the office	On the go



Phishing attempts

Phishing emails and texts (actual examples below) are designed to look like they're from companies you know and trust like your bank, credit card company or an online store. Clicking on any links or downloading an attachment from the message can result in scammers gaining access to your personal information which they use to access your email, bank or other accounts.

Remember, M&T Bank does NOT initiate emails, texts or phone calls seeking your personal data, account or card numbers.



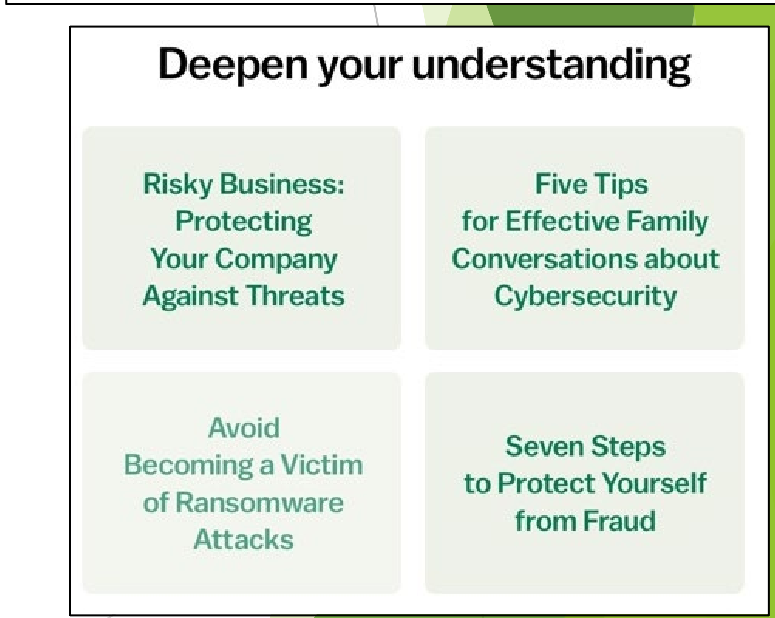
M&T Bank — Understanding what's important®

Be on alert

Spot phishing attempts and protect your devices against screen sharing scams.

Learn More

At M&T Bank, we're committed to helping you protect your personal and financial information. Part of that commitment includes helping you stay informed of fraud scams so you can better identify, reduce and mitigate your risk. It's important to stay alert and we want you to be aware of some of the types of scams you may see.



Deepen your understanding

- Risky Business: Protecting Your Company Against Threats
- Five Tips for Effective Family Conversations about Cybersecurity
- Avoid Becoming a Victim of Ransomware Attacks
- Seven Steps to Protect Yourself from Fraud

M&T Bank

Best

Cybersecurity Awareness Training Summary:

Cybersecurity Training WBT:	All Employees & Contingent Workers, Annual & upon Hire
Targeted Cybersecurity Training & Awareness:	EVPs & Board of Directors, Managers, Privileged Users
Internal Communications:	Periodic Security Awareness Articles Panel Discussions Periodic Video Training
Phishing Simulation Testing & Training Program:	Monthly Enterprise Scenarios, bi-monthly Targeted Scenarios & Remedial Training
Cybersecurity Awareness Month:	Weekly Internal & External Articles, Videos and Social Media Posts
Cybersecurity Champions Program:	Collaboration with Employees of Technology, Product Teams & Cybersecurity
Cybersecurity Intranet & Internet Site Content:	Security Tips, Best Practices , Articles and FAQs
Customer Awareness Training:	Security Center Tips on mtb.com/security & wilmingtontrust.com/security Periodic Customer Emails to Communicate High Risk Threats Customer Training via Email, Webinars and Onsite Meetings

M&T Bank

Best

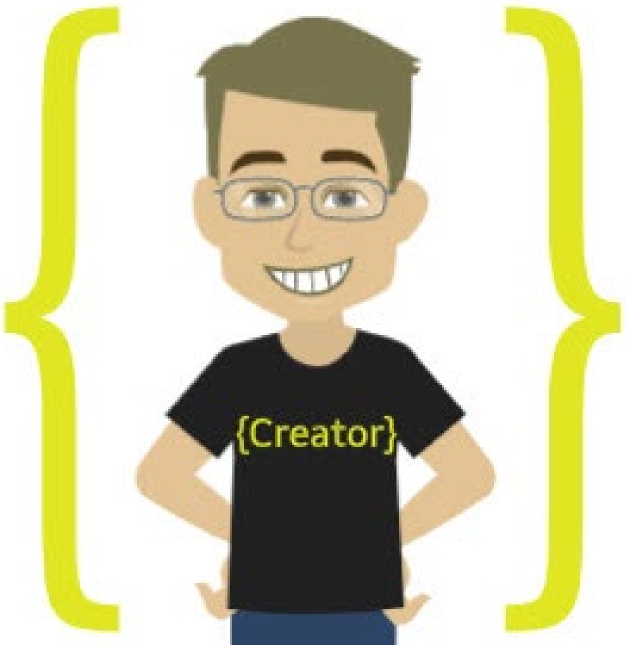
Lessons Learned:

- Think like a Hacker
  - Sell like a Salesperson
    - Market like a Marketer

- BUT -

- Always Think Like your Employees
- People Learn Differently – Switch it Up!
- Less is More
  - Keep it Short and Relevant
  - Make it Fun!

Questions / Comments?



Chris Schmigel
Senior Cybersecurity Risk Analyst
Vice President
M&T Bank

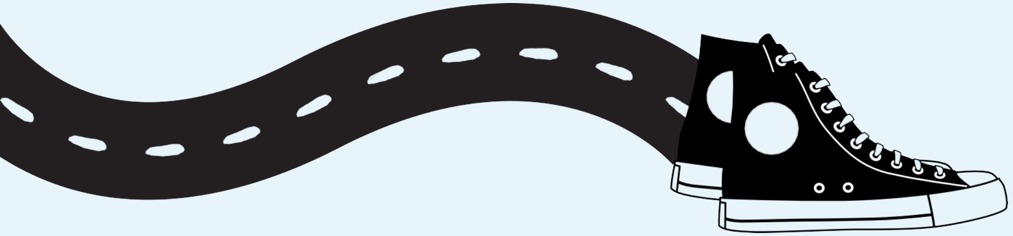
cschmigel@mtb.com

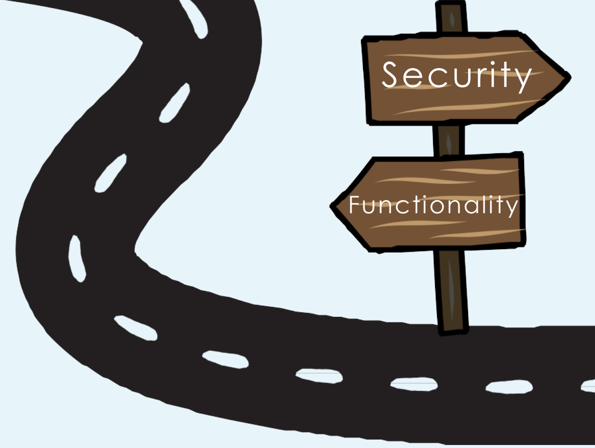
A Mile in the Shoes: Considerations for Developer-centric Security Training and Awareness

Dr. Pranshu Bajpai

Principal Staff Security Architect

Motorola Solutions





A Mile in the Shoes

Considerations for Developer-centric Security Training and Awareness

NIST FISSEA Winter Forum
February 14, 2023

Dr. Pranshu Bajpai

About

PhD, Computer Science, Michigan State University

Principal Security Architect, Motorola Solutions Inc

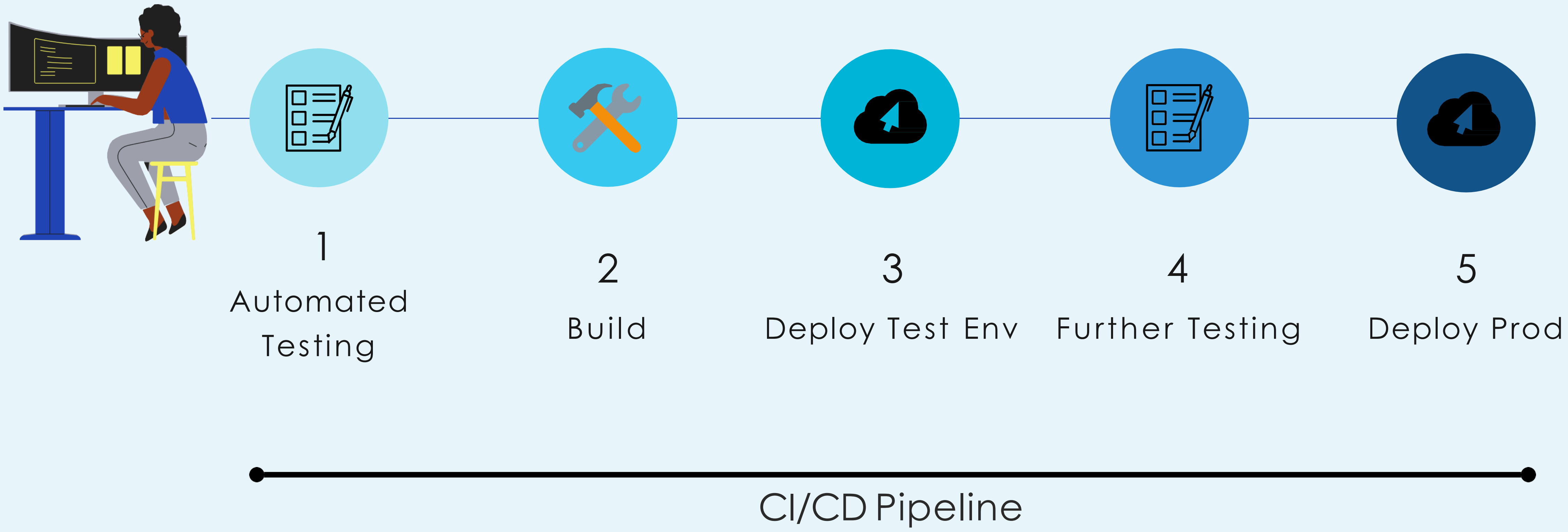
Speaker: Defcon, Grrcon, Toorcon, APWG eCrime, IACP, CascadiaJS, Bsides, IEEE SecDev, Lascon etc.

Research: Malware, Threats, Forensics, Applied Crypto, DevOps, Cloud Security, Data Science

amirootyet.com in/pranshubajpai/ @amirootyet

Modern DevOps

Continuous and Seamless Software Delivery



1 Automated Testing

2 Build

3 Deploy Test Env

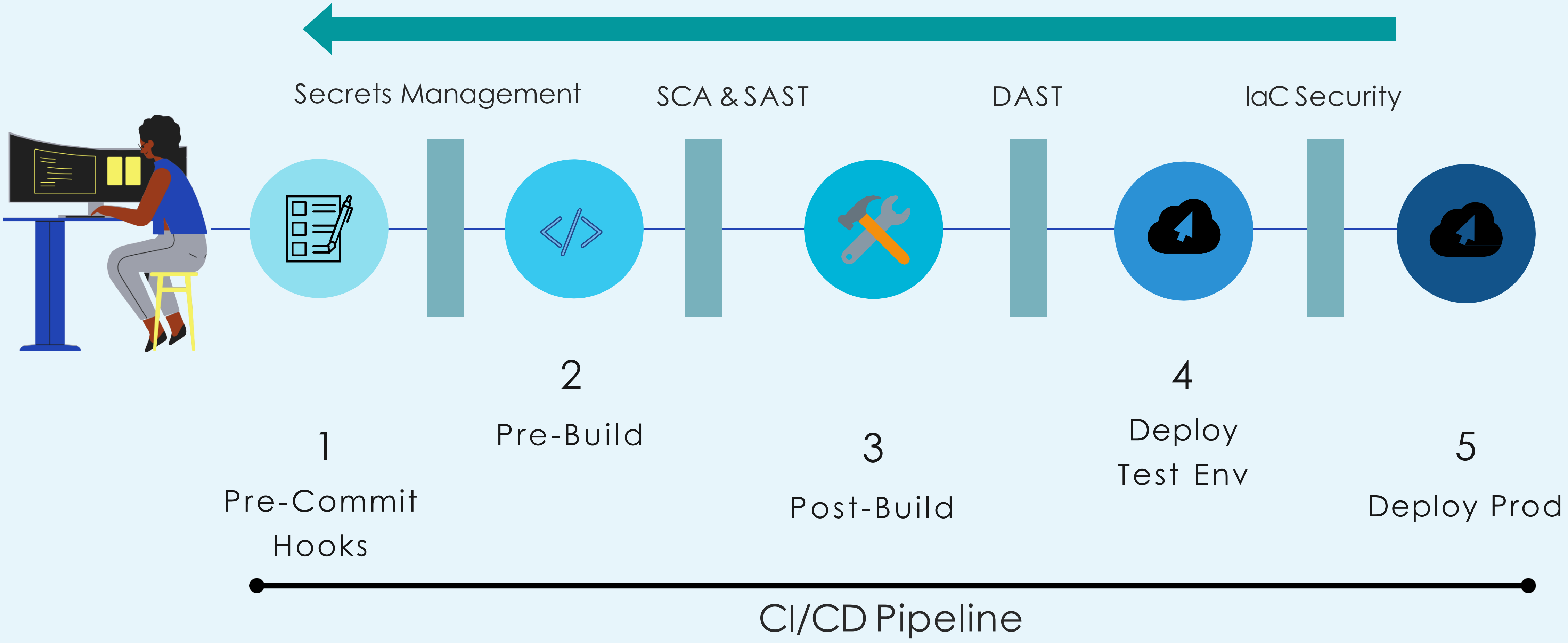
4 Further Testing

5 Deploy Prod

CI/CD Pipeline

Enter DevSecOps

Shift Security Left



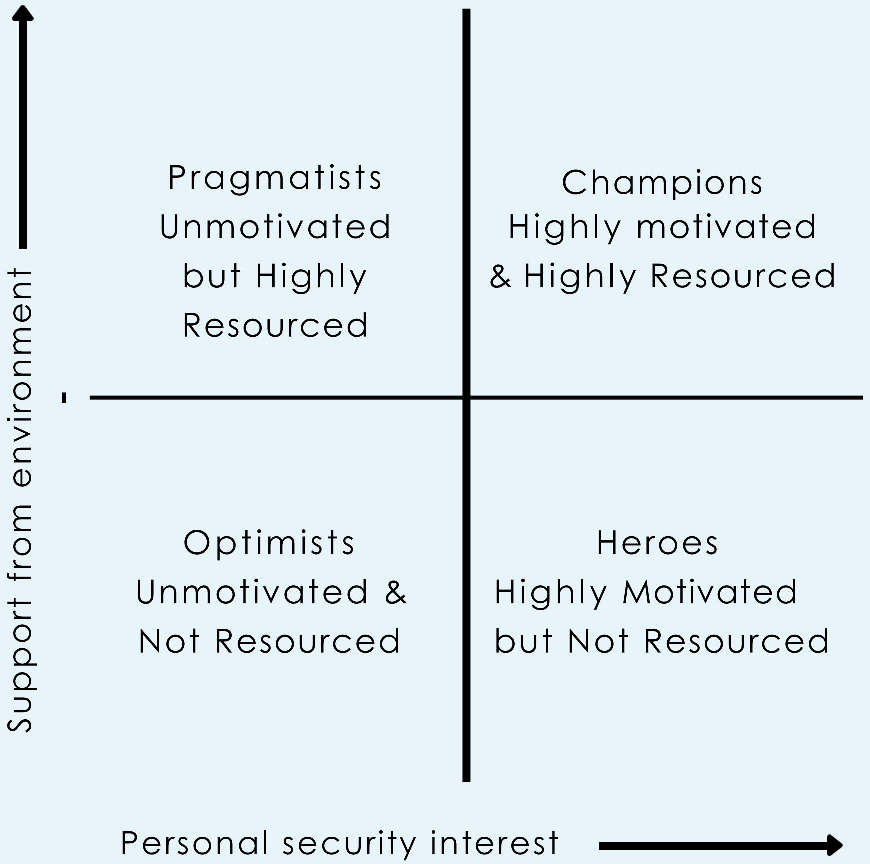
Developer Security Archetypes

Pragmatists are not particularly interested in security but will utilize the tools locally available

Champions have a natural interest in security that is supported by their organizations

Optimists are heavily dependent on the security toolchain

Heroes' interest and drive towards security helps secure development



Pragmatists
Unmotivated
but Highly
Resourced

Champions
Highly motivated
& Highly Resourced

Optimists
Unmotivated &
Not Resourced

Heroes
Highly Motivated
but Not Resourced

Ryan, I., Roedig, U., & Stol, K. J. (2021, June). Understanding developer security archetypes. In 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS) (pp. 37-40). IEEE.

Psychological Heuristics

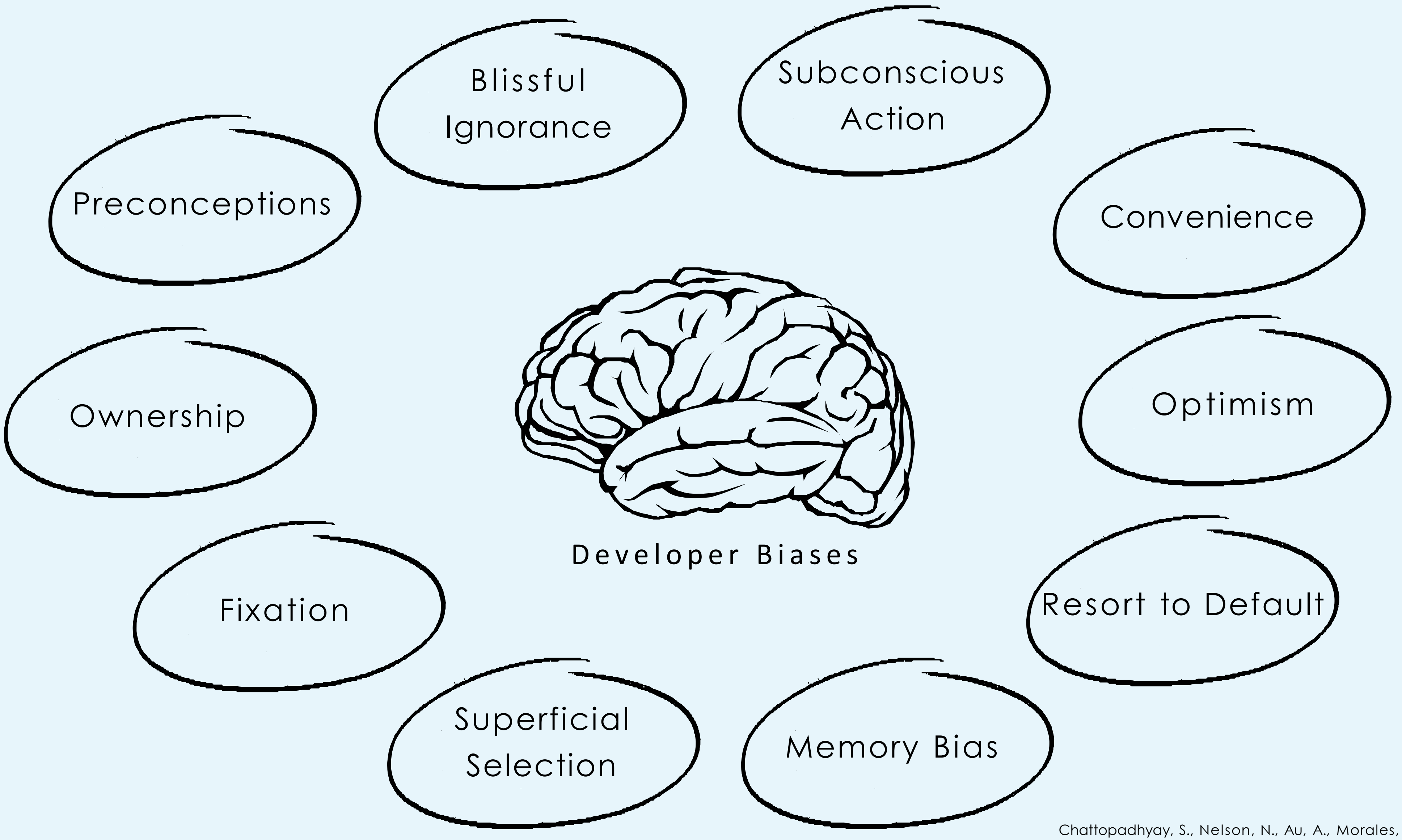
Heuristics require less cognitive effort

Humans have a short working memory

Humans will use the least amount of effort necessary and arrive at a sub-optimal solution

Security solutions should reach the developer as and when they are needed, not the other way around

Oliveira, D., Rosenthal, M., Morin, N., Yeh, K. C., Cappos, J., & Zhuang, Y. (2014, December). It's the psychology stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer's blind spots. In Proceedings of the 30th Annual Computer Security Applications Conference (pp.



Developer Biases

Blissful Ignorance

Subconscious Action

Preconceptions

Convenience

Ownership

Optimism

Fixation

Resort to Default

Superficial Selection

Memory Bias

Chattopadhyay, S., Nelson, N., Au, A., Morales, N., Sanchez, C., Pandita, R., & Sarma, A. (2020, June). A tale from the trenches: cognitive biases and software development. In Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering (pp. 654-665).

Solutions Search Patterns

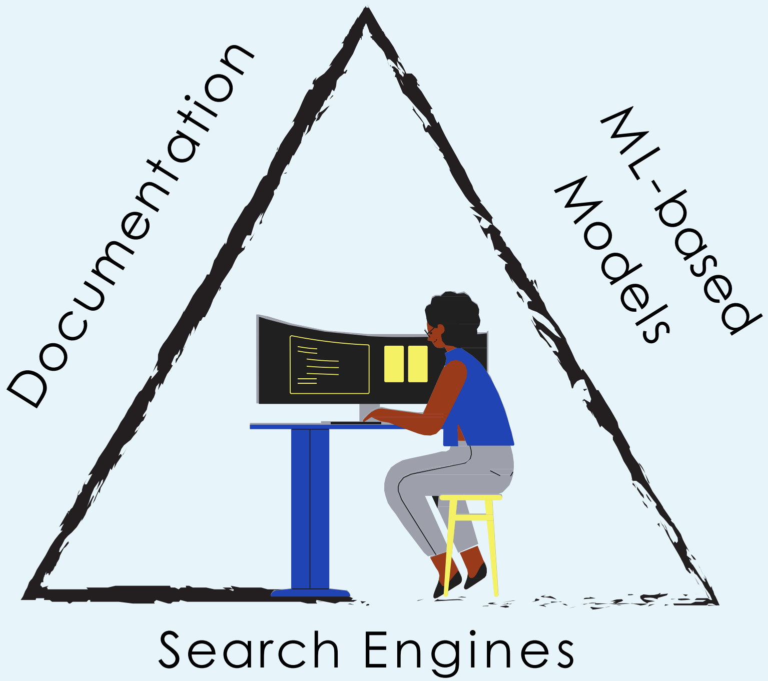
Ease of access

Ephemeral elements

Conceptual versus actionable

Veracity of claims

Completeness



Documentation

ML-based Models

Search Engines

Partnership (Security 🤝 DevOps)

Listen. Don't preach.

Understand developer perspectives and constraints

Suggest viable solutions within those constraints

Provide implementation details to enable devsecops

Create and support a security champions program

Thou shalt
sign thy code

Developer Incentives

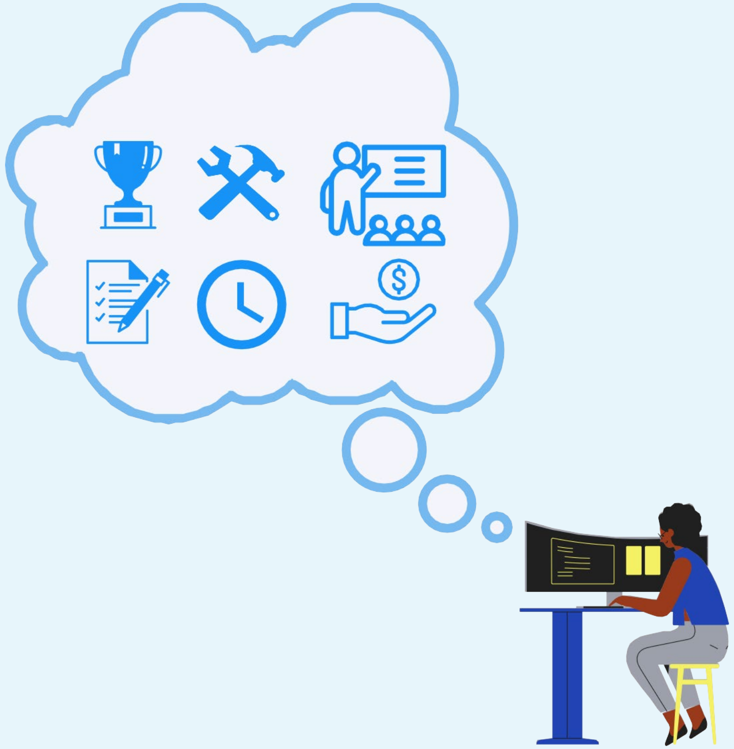
Financial resources

Time allocations during sprint cycles

Internal documentations detailing security solutions

Easy access to effective security toolchain

Periodic targeted security training and support



Documentation

Encourage and incentivize teams to document

Little documentation is better than

no documentation Do not seek

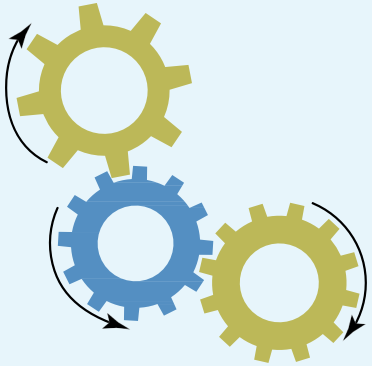
perfection while documenting

The Golden Order of Impact

People

Buy-in from stakeholders

>



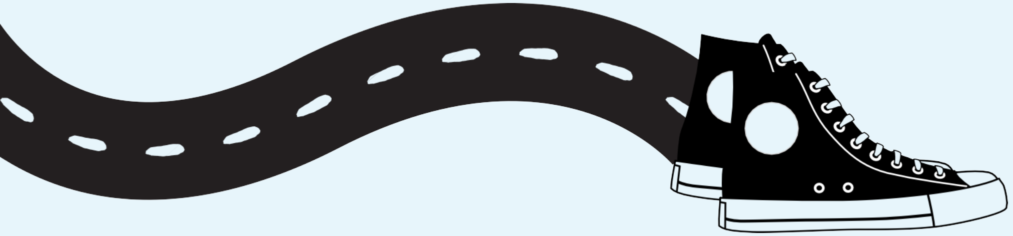
Process

Well-defined and easily adopted

>

Tools

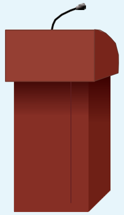
Effective, efficient, and fast execution



Thank You

NIST FISSEA Winter Forum: February 14, 2023

Questions?



Dr. Pranshu Bajpai

Closing Remarks

Brooke Crisp

IT Cybersecurity Specialist
Social Security Administration

THANK YOU

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

https://www.surveymonkey.com/r/2023FISSEAWinterForum

#FISSEA2023 | nist.gov/fissea

Get Involved

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

Volunteer for the Planning Committee
https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee

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

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

SAVE THE DATE

Federal Information Security Educators (FISSEA) Conference

May 16, 2023

#FISSEA2023 | nist.gov/fissea

fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

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