FISSEA 34th Annual Conference:

*Refining Cybersecurity Culture: WIIFM**

May 14-15, 2024
Rockville, MD

*What's in it for me?

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Federal Information Security Educators (FISSEA)

34th Annual FISSEA Conference

“Refining Cybersecurity Culture: WIIFM”

May 14, 2024

9:00am – 5:00pm ET

#FISSEA | nist.gov/fissea

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Please Note…

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.

Conference Welcome

Brooke Crisp
FISSEA Co-Chair

Frauke Steinmeier
FISSEA Co-Chair

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 2025
Email fissea@list.nist.gov

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

NCCoE Welcome

Cherilyn Pascoe
Director

Master of Ceremonies Welcome

Marian Merritt
Deputy Director of NICE
National Institute of Standards and Technology

KEYNOTE *Security Training: Going Beyond the Checkbox*

Lance Spitzner
Technical Director
SANS Security Awareness

Security Training: Going Beyond the Checkbox

lspitzner@sans.org

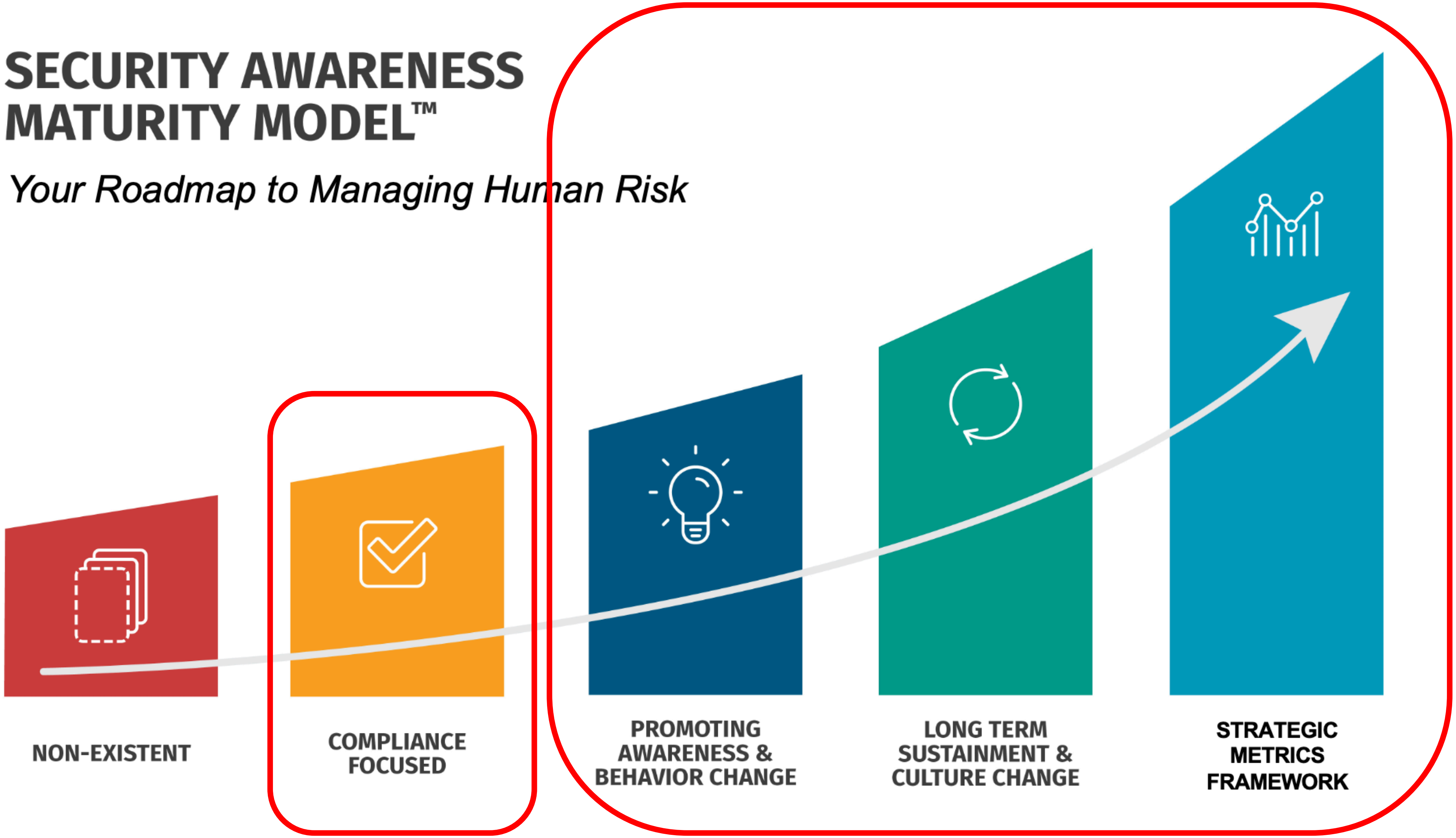
SANS SECURITY AWARENESS

2021 Dat
verizo
DBIR
Data Breach Investigations Report
2008
DBIR
2023 Data Breach Investigations Report
2005
verizon
2024 Data Breach Investigations Report
verizon business

65% of all breaches involve the human element

SECURITY AWARENESS MATURITY MODEL™

Your Roadmap to Managing Human Risk



NON-EXISTENT

COMPLIANCE FOCUSED

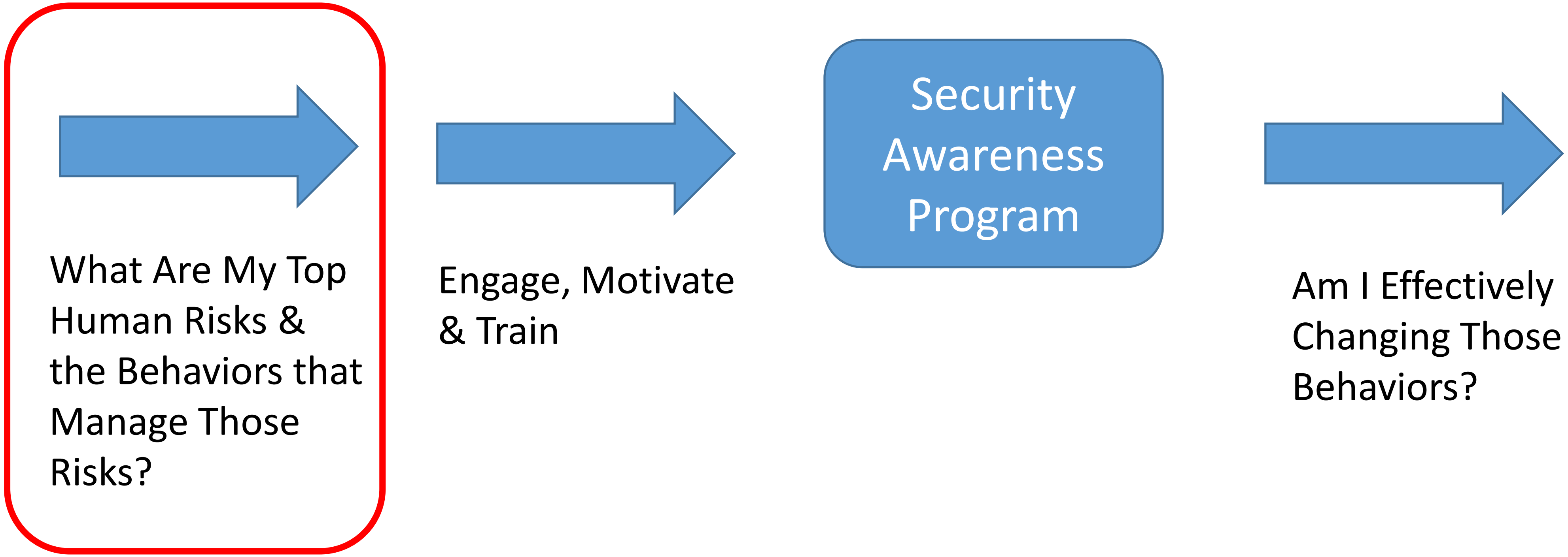
PROMOTING AWARENESS & BEHAVIOR CHANGE

LONG TERM SUSTAINMENT & CULTURE CHANGE

STRATEGIC METRICS FRAMEWORK

SANS SECURITY AWARENESS

Steps to Managing Human Risk



What Are My Top Human Risks & the Behaviors that Manage Those Risks?

Engage, Motivate & Train

Security Awareness Program

Am I Effectively Changing Those Behaviors?

1. What Are My Top Human Risks?

- To effectively manage human risk you need to first identify and prioritize your human risks
- These decisions should be driven by data, not emotion

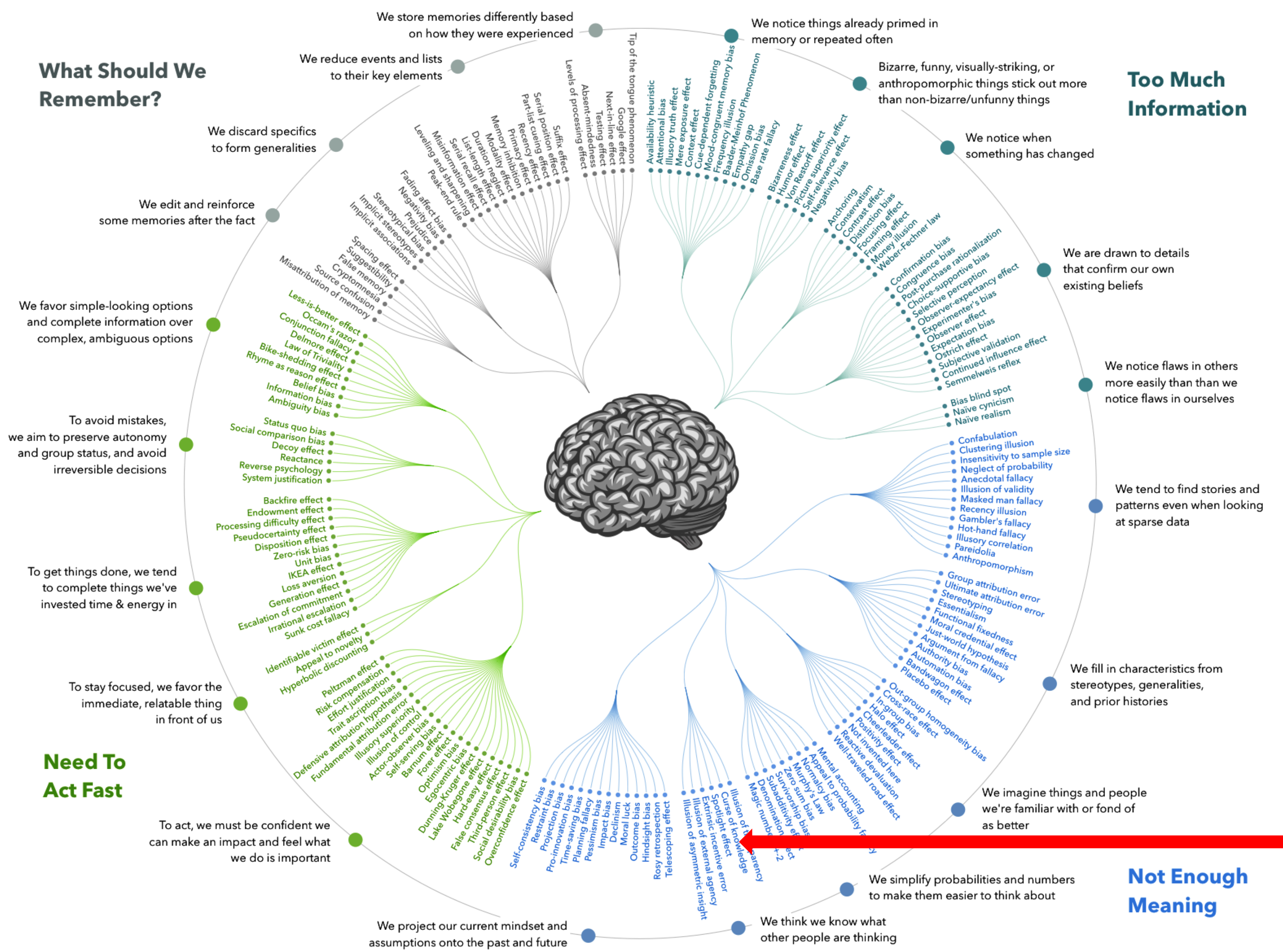
Data Sources to Determine Your Top Risks

- Past incidents / breaches
- Past assessments / audits
- Industry risk reports
- Human risk / behavior assessments
- Cyber Threat Intelligence (CTI)

Focus on as Few Risks as Possible

- People can remember only so much—*cognitive overload*
- Every behavior has a cost to employees and your organization
- You have limited time and resources
- Fewer topics are easier to reinforce

COGNITIVE BIAS CODEX



Too Much Information

We notice things already primed in memory or repeated often

- Availability heuristic
- Attentional bias
- Illusory truth effect
- Mere exposure effect
- Context effect
- Cue-dependent forgetting
- Mood-congruent memory bias
- Frequency illusion
- Baader-Meinhof Phenomenon
- Empathy gap
- Omission bias
- Base rate fallacy

Bizarre, funny, visually-striking, or anthropomorphic things stick out more than non-bizarre/unfunny things

- Bizarreness effect
- Humor effect
- Von Restorff effect
- Picture superiority effect
- Self-relevance effect
- Negativity bias

We notice when something has changed

- Anchoring
- Conservatism
- Contrast effect
- Distinction bias
- Focusing effect
- Framing effect
- Money illusion
- Weber-Fechner law

We are drawn to details that confirm our own existing beliefs

- Confirmation bias
- Congruence bias
- Post-purchase rationalization
- Choice-supportive bias
- Selective perception
- Observer-expectancy effect
- Experimenter's bias
- Observer effect
- Expectation bias
- Ostrich effect
- Subjective validation
- Continued influence effect
- Semmelweis reflex

We notice flaws in others more easily than than we notice flaws in ourselves

- Bias blind spot
- Naïve cynicism
- Naïve realism

Not Enough Meaning

We tend to find stories and patterns even when looking at sparse data

- Confabulation
- Clustering illusion
- Insensitivity to sample size
- Neglect of probability
- Anecdotal fallacy
- Illusion of validity
- Masked man fallacy
- Recency illusion
- Gambler's fallacy
- Hot-hand fallacy
- Illusory correlation
- Pareidolia
- Anthropomorphism

We fill in characteristics from stereotypes, generalities, and prior histories

- Group attribution error
- Ultimate attribution error
- Stereotyping
- Essentialism
- Functional fixedness
- Moral credential effect
- Just-world hypothesis
- Argument from fallacy
- Authority bias
- Automation bias
- Bandwagon effect
- Placebo effect

We imagine things and people we're familiar with or fond of as better

- Out-group homogeneity bias
- Cross-race effect
- In-group bias
- Halo effect
- Cheerleader effect
- Positivity effect
- Not invented here
- Reactive devaluation
- Well-traveled road effect

We simplify probabilities and numbers to make them easier to think about

- Mental accounting
- Appeal to probability fallacy
- Normalcy bias
- Murphy's Law
- Zero sum bias
- Survivorship bias
- Subadditivity effect
- Denomination effect
- Magic number 7+-2

We think we know what other people are thinking

- Illusion of transparency
- Curse of knowledge
- Spotlight effect
- Extrinsic incentive error
- Illusion of external agency
- Illusion of asymmetric insight

We project our current mindset and assumptions onto the past and future

- Self-consistency bias
- Restraint bias
- Projection bias
- Pro-innovation bias
- Time-saving bias
- Planning fallacy
- Pessimism bias
- Impact bias
- Declinism
- Moral luck
- Outcome bias
- Hindsight bias
- Rosy retrospection
- Telescoping effect

Need To Act Fast

To act, we must be confident we can make an impact and feel what we do is important

- Peltzman effect
- Risk compensation
- Effort justification
- Trait ascription bias
- Defensive attribution hypothesis
- Fundamental attribution error
- Illusory superiority
- Illusion of control
- Actor-observer bias
- Self-serving bias
- Barnum effect
- Forer effect
- Optimism bias
- Egocentric bias
- Dunning-Kruger effect
- Lake Wobegone effect
- Hard-easy effect
- False consensus effect
- Third-person effect
- Social desirability bias
- Overconfidence effect

To stay focused, we favor the immediate, relatable thing in front of us

- Identifiable victim effect
- Appeal to novelty
- Hyperbolic discounting

To get things done, we tend to complete things we've invested time & energy in

- Backfire effect
- Endowment effect
- Processing difficulty effect
- Pseudocertainty effect
- Disposition effect
- Zero-risk bias
- Unit bias
- IKEA effect
- Loss aversion
- Generation effect
- Escalation of commitment
- Irrational escalation
- Sunk cost fallacy

To avoid mistakes, we aim to preserve autonomy and group status, and avoid irreversible decisions

- Status quo bias
- Social comparison bias
- Decoy effect
- Reactance
- Reverse psychology
- System justification

We favor simple-looking options and complete information over complex, ambiguous options

- Less-is-better effect
- Occam's razor
- Conjunction fallacy
- Delmore effect
- Law of Triviality
- Bike-shedding effect
- Rhyme as reason effect
- Belief bias
- Information bias
- Ambiguity bias

What Should We Remember?

We edit and reinforce some memories after the fact

- Spacing effect
- Suggestibility
- False memory
- Cryptomnesia
- Source confusion
- Misattribution of memory

We discard specifics to form generalities

- Fading affect bias
- Negativity bias
- Prejudice
- Stereotypical bias
- Implicit stereotypes
- Implicit associations

We reduce events and lists to their key elements

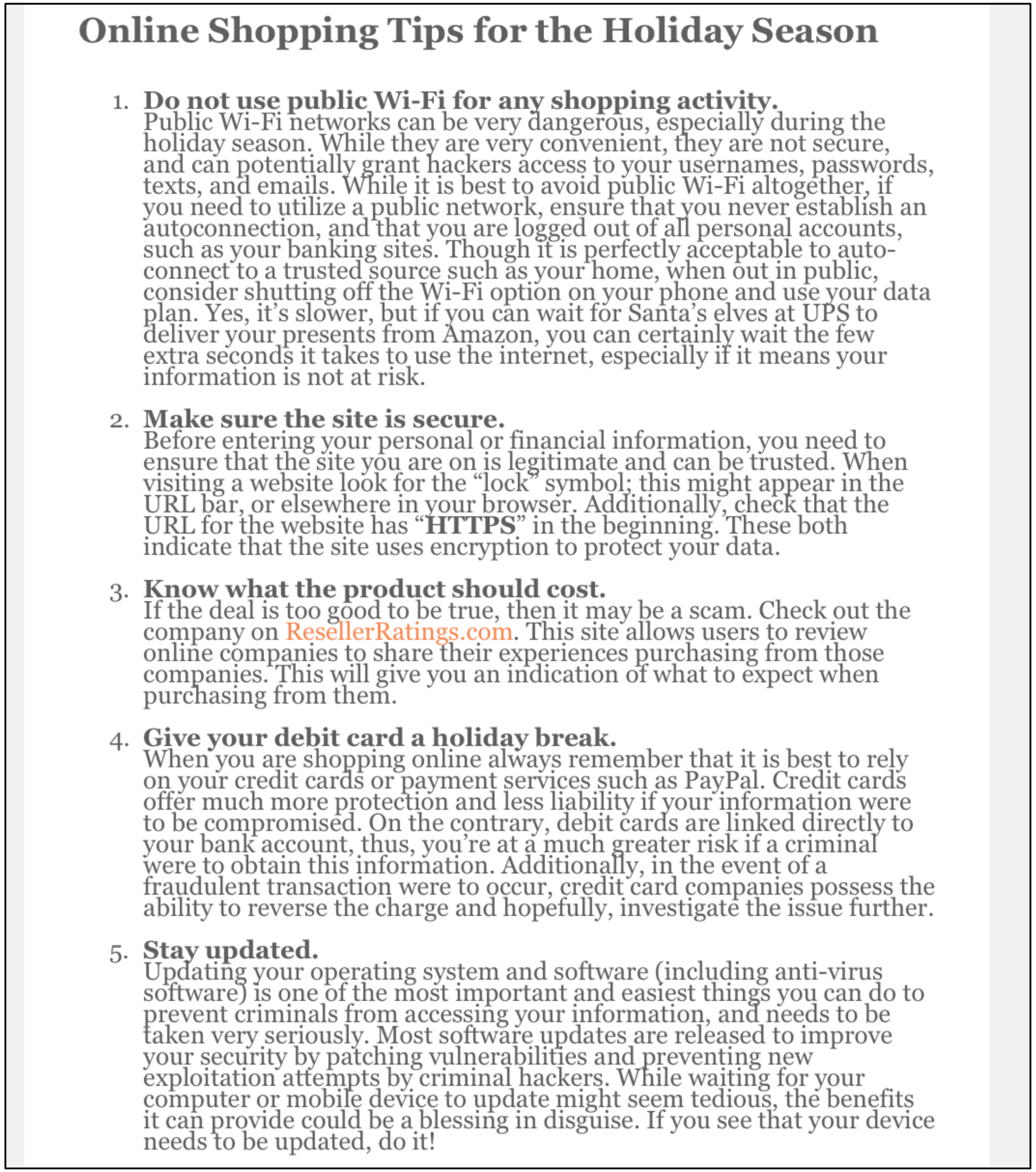
- Suffix effect
- Serial position effect
- Part-list cueing effect
- Recency effect
- Primacy effect
- Memory inhibition
- Modality effect
- Duration neglect
- List-length effect
- Serial recall effect
- Misinformation effect
- Leveling and sharpening
- Peak-end rule

We store memories differently based on how they were experienced

- Levels of processing effect
- Absent-mindedness
- Testing effect
- Next-in-line effect
- Google effect
- Tip of the tongue phenomenon

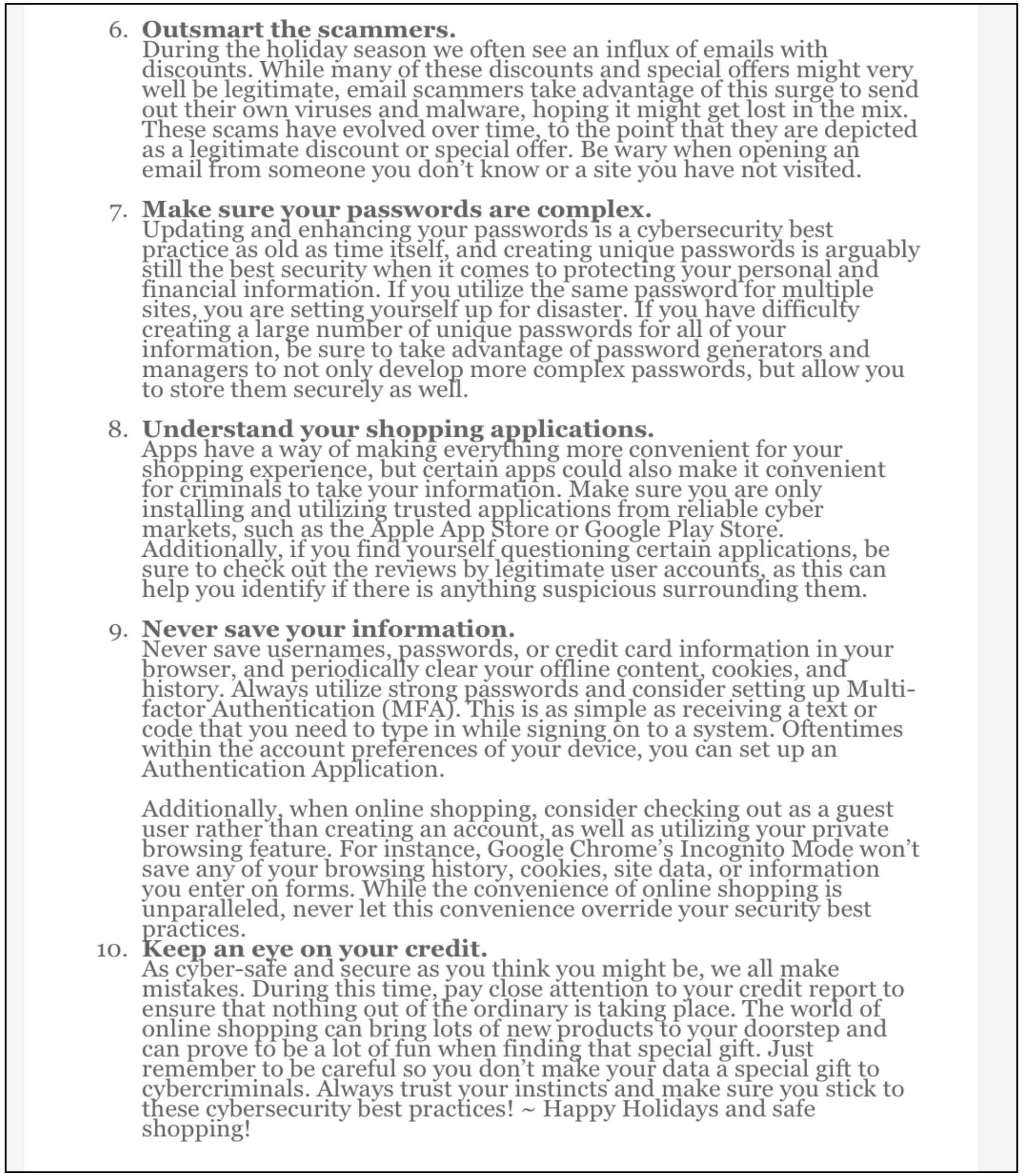
DESIGNHACKS.CO · CATEGORIZATION BY BUSTER BENSON · ALGORITHMIC DESIGN BY JOHN MANOOGIAN III (JM3) · DATA BY WIKIPEDIA

creative commons attribution · share-alike



Online Shopping Tips for the Holiday Season

1. **Do not use public Wi-Fi for any shopping activity.**
   Public Wi-Fi networks can be very dangerous, especially during the holiday season. While they are very convenient, they are not secure, and can potentially grant hackers access to your usernames, passwords, texts, and emails. While it is best to avoid public Wi-Fi altogether, if you need to utilize a public network, ensure that you never establish an autoconnection, and that you are logged out of all personal accounts, such as your banking sites. Though it is perfectly acceptable to auto-connect to a trusted source such as your home, when out in public, consider shutting off the Wi-Fi option on your phone and use your data plan. Yes, it's slower, but if you can wait for Santa's elves at UPS to deliver your presents from Amazon, you can certainly wait the few extra seconds it takes to use the internet, especially if it means your information is not at risk.
2. **Make sure the site is secure.**
   Before entering your personal or financial information, you need to ensure that the site you are on is legitimate and can be trusted. When visiting a website look for the "lock" symbol; this might appear in the URL bar, or elsewhere in your browser. Additionally, check that the URL for the website has "**HTTPS**" in the beginning. These both indicate that the site uses encryption to protect your data.
3. **Know what the product should cost.**
   If the deal is too good to be true, then it may be a scam. Check out the company on ResellerRatings.com. This site allows users to review online companies to share their experiences purchasing from those companies. This will give you an indication of what to expect when purchasing from them.
4. **Give your debit card a holiday break.**
   When you are shopping online always remember that it is best to rely on your credit cards or payment services such as PayPal. Credit cards offer much more protection and less liability if your information were to be compromised. On the contrary, debit cards are linked directly to your bank account, thus, you're at a much greater risk if a criminal were to obtain this information. Additionally, in the event of a fraudulent transaction were to occur, credit card companies possess the ability to reverse the charge and hopefully, investigate the issue further.
5. **Stay updated.**
   Updating your operating system and software (including anti-virus software) is one of the most important and easiest things you can do to prevent criminals from accessing your information, and needs to be taken very seriously. Most software updates are released to improve your security by patching vulnerabilities and preventing new exploitation attempts by criminal hackers. While waiting for your computer or mobile device to update might seem tedious, the benefits it can provide could be a blessing in disguise. If you see that your device needs to be updated, do it!



6. **Outsmart the scammers.**
   During the holiday season we often see an influx of emails with discounts. While many of these discounts and special offers might very well be legitimate, email scammers take advantage of this surge to send out their own viruses and malware, hoping it might get lost in the mix. These scams have evolved over time, to the point that they are depicted as a legitimate discount or special offer. Be wary when opening an email from someone you don't know or a site you have not visited.
7. **Make sure your passwords are complex.**
   Updating and enhancing your passwords is a cybersecurity best practice as old as time itself, and creating unique passwords is arguably still the best security when it comes to protecting your personal and financial information. If you utilize the same password for multiple sites, you are setting yourself up for disaster. If you have difficulty creating a large number of unique passwords for all of your information, be sure to take advantage of password generators and managers to not only develop more complex passwords, but allow you to store them securely as well.
8. **Understand your shopping applications.**
   Apps have a way of making everything more convenient for your shopping experience, but certain apps could also make it convenient for criminals to take your information. Make sure you are only installing and utilizing trusted applications from reliable cyber markets, such as the Apple App Store or Google Play Store. Additionally, if you find yourself questioning certain applications, be sure to check out the reviews by legitimate user accounts, as this can help you identify if there is anything suspicious surrounding them.
9. **Never save your information.**
   Never save usernames, passwords, or credit card information in your browser, and periodically clear your offline content, cookies, and history. Always utilize strong passwords and consider setting up Multi-factor Authentication (MFA). This is as simple as receiving a text or code that you need to type in while signing on to a system. Oftentimes within the account preferences of your device, you can set up an Authentication Application.

   Additionally, when online shopping, consider checking out as a guest user rather than creating an account, as well as utilizing your private browsing feature. For instance, Google Chrome's Incognito Mode won't save any of your browsing history, cookies, site data, or information you enter on forms. While the convenience of online shopping is unparalleled, never let this convenience override your security best practices.
10. **Keep an eye on your credit.**
    As cyber-safe and secure as you think you might be, we all make mistakes. During this time, pay close attention to your credit report to ensure that nothing out of the ordinary is taking place. The world of online shopping can bring lots of new products to your doorstep and can prove to be a lot of fun when finding that special gift. Just remember to be careful so you don't make your data a special gift to cybercriminals. Always trust your instincts and make sure you stick to these cybersecurity best practices! ~ Happy Holidays and safe shopping!

Here are key tips to securely making the most when attending a video conference.

Updated Software

Make sure you are always using the latest version of the software. The more recent and updated your software, the more secure you will be. Enable automatic updating whenever possible.

Configure audio/video settings

Set your preferences to mute your microphone and turn off your video when joining a meeting and enable it only when you want.

Your Background

Ensure you do not have any personal or sensitive information behind you during the call. Some video conferencing software lets you set up your own virtual background or blur your background, so people can't see what is behind you.

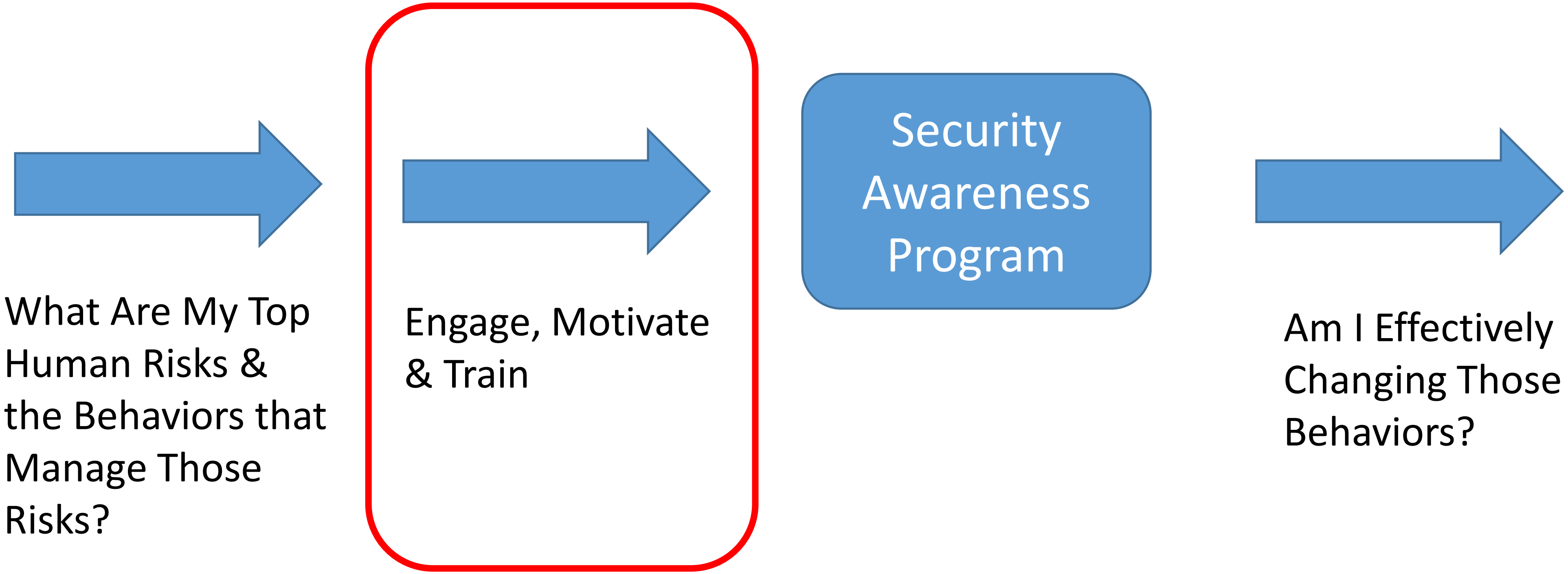
Don't Share Invites

The invite link to a call is the ticket to enter the meeting; others can join if you share.

Don't take screenshots

Protect both our sensitive data and the privacy of others, do not take screenshots unless you ask and have been given permission.

Steps to Managing Human Risk



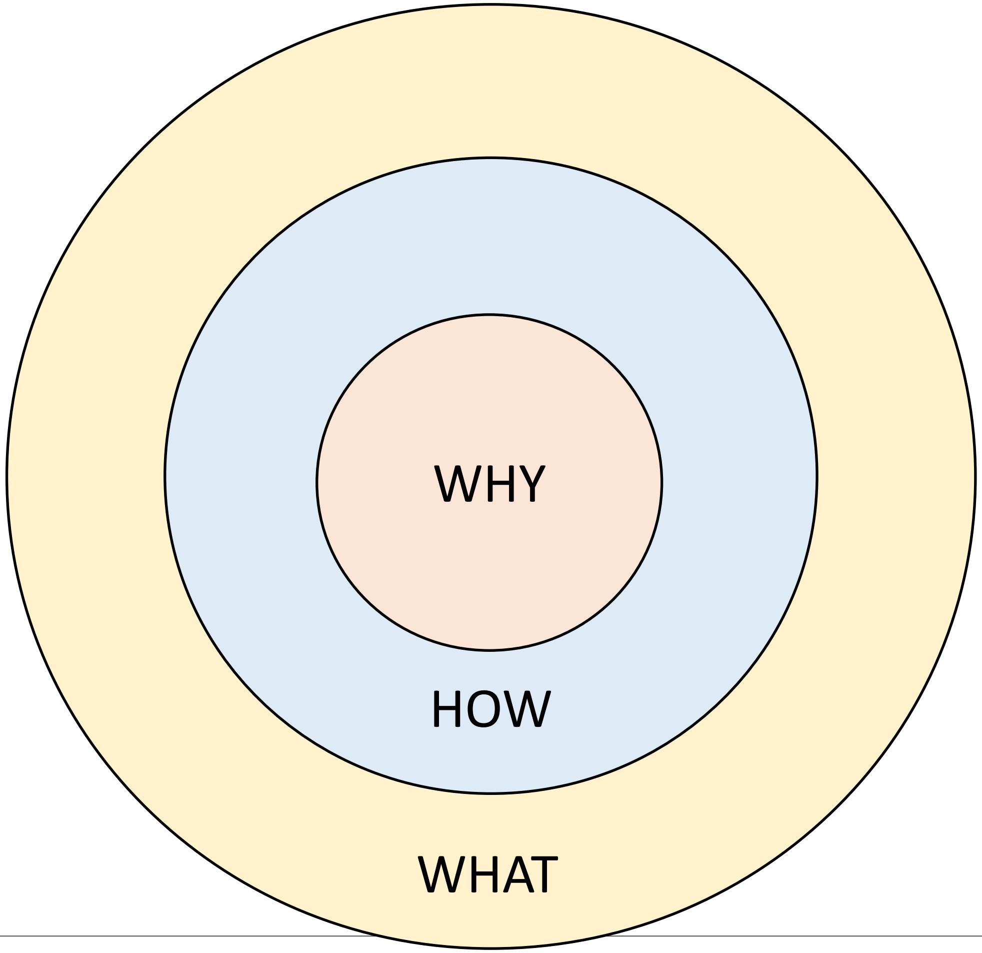
What Are My Top Human Risks & the Behaviors that Manage Those Risks?

Engage, Motivate & Train

Security Awareness Program

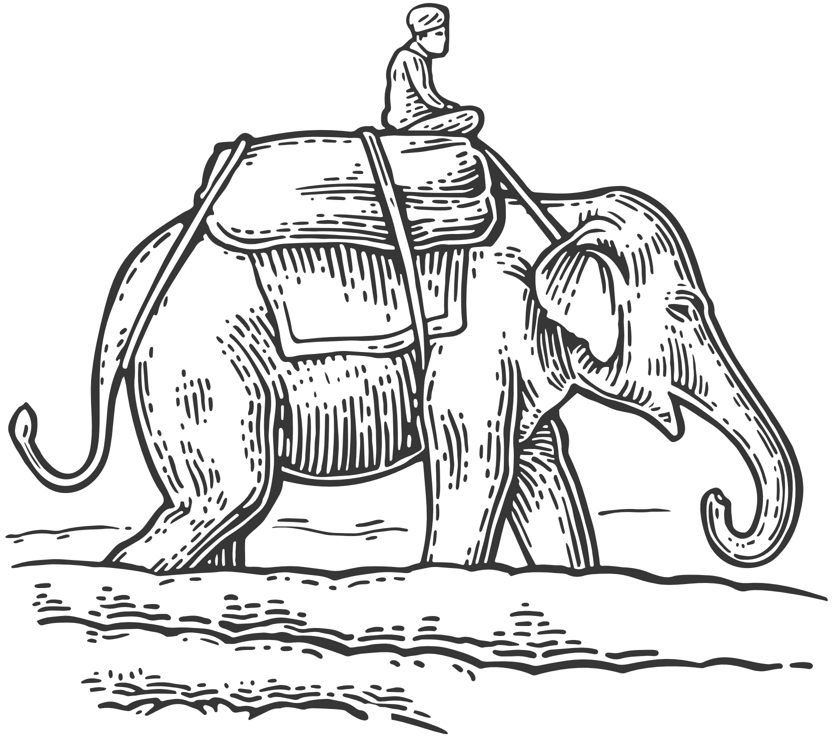
Am I Effectively Changing Those Behaviors?

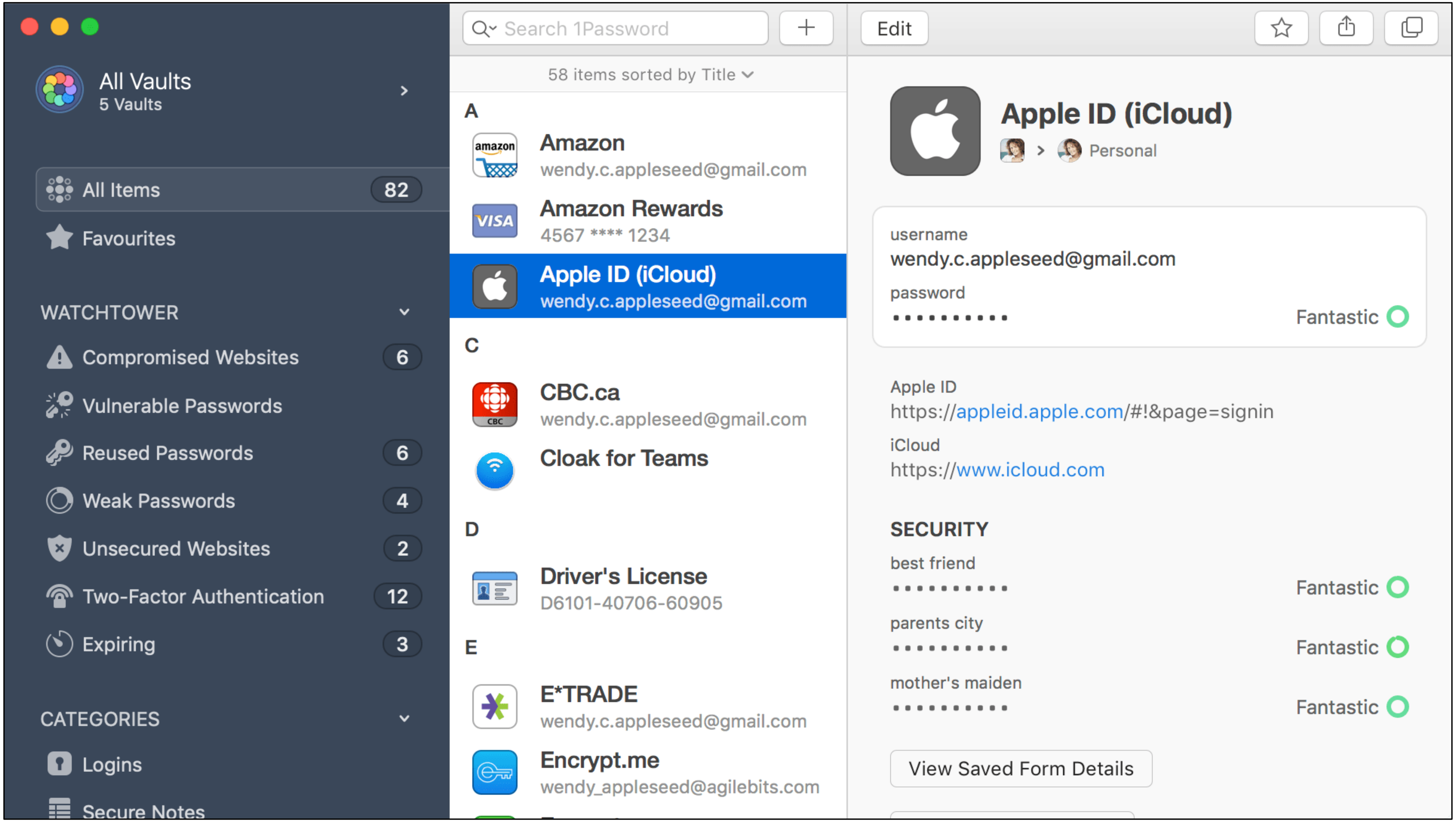
Motivating Change - Start with Why



The Elephant vs. The Rider

The Rider (logic) guides and directs the Elephant (emotion). However, at some point the Elephant simply does what it wants.





A

Amazon
wendy.c.appleseed@gmail.com

Amazon Rewards
4567 **** 1234

Apple ID (iCloud)
wendy.c.appleseed@gmail.com

C

CBC.ca
wendy.c.appleseed@gmail.com

Cloak for Teams

D

Driver's License
D6101-40706-60905

E

E*TRADE
wendy.c.appleseed@gmail.com

Encrypt.me
wendy_appleseed@agilebits.com

Apple ID (iCloud)
Personal

username
wendy.c.appleseed@gmail.com

password
•••••••••• Fantastic

Apple ID
https://appleid.apple.com/#!&page=signin

iCloud
https://www.icloud.com

SECURITY

best friend
•••••••••• Fantastic

parents city
•••••••••• Fantastic

mother's maiden
•••••••••• Fantastic

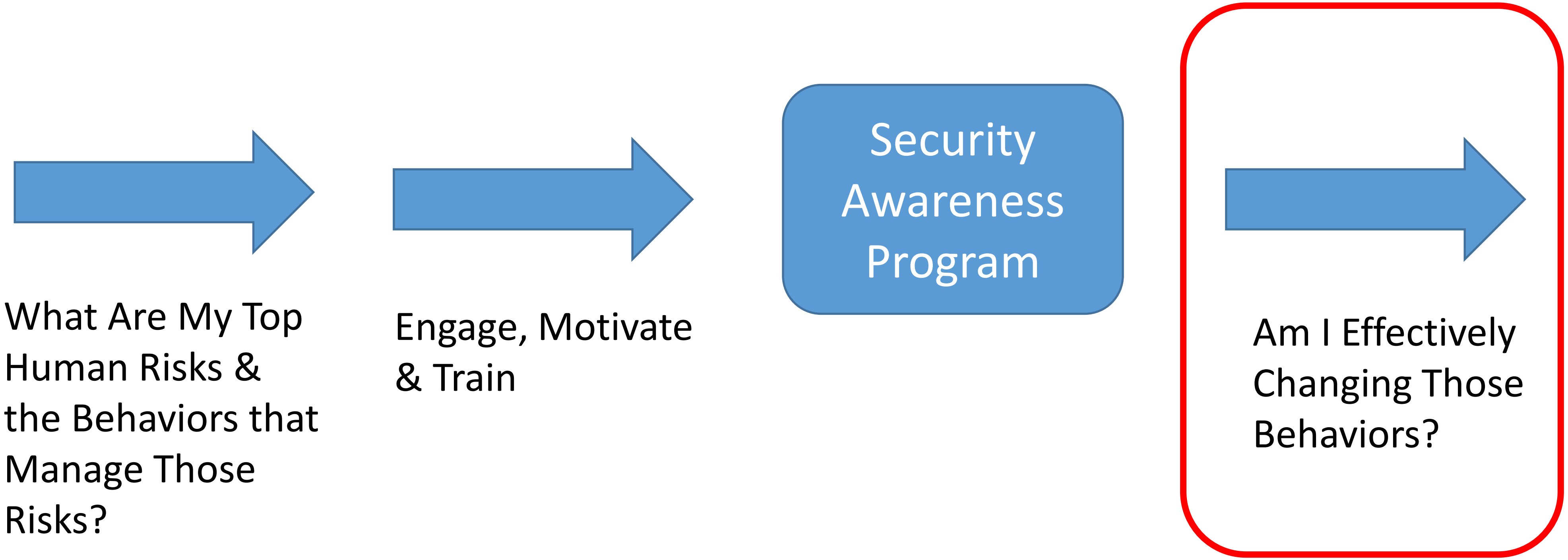
Effective this week, all employees are required to adopt and begin using our new password manager solution. A password manager is a security program that encrypts and stores all your credentials in a single cloud-based vault that you access via the new browser toolbar add-on. We are taking this step due to several APT-based brute force attacks logged over the past two months and to meet new regulation requirements as per SG750-52r5-a1. You are expected to migrate all your passwords to the tool by this Friday, 5 p.m. ET.

To learn how to set up your password manager, refer to the attached eight-page setup guide; all questions concerning setup should be sent to the help desk.

Folks, do you hate passwords? Do you find it a pain trying to remember all your different passwords, constantly generating new ones, or having to repeatedly log in to websites? Well, the security team has a solution for you: password managers. This simple tool takes care of all those problems for you, saving you time, simplifying your life, and making you more secure. Even better, we are providing this solution for home use, so you can both simplify the lives of and secure everyone in your family.

See the attached 90-second video that walks you through how to set up and start using your new password manager. Our security team is standing by on the #PasswordManager Slack channel to help you personally with any questions or issues you might have.

Steps to Managing Human Risk



What Are My Top Human Risks & the Behaviors that Manage Those Risks?

Engage, Motivate & Train

Security Awareness Program

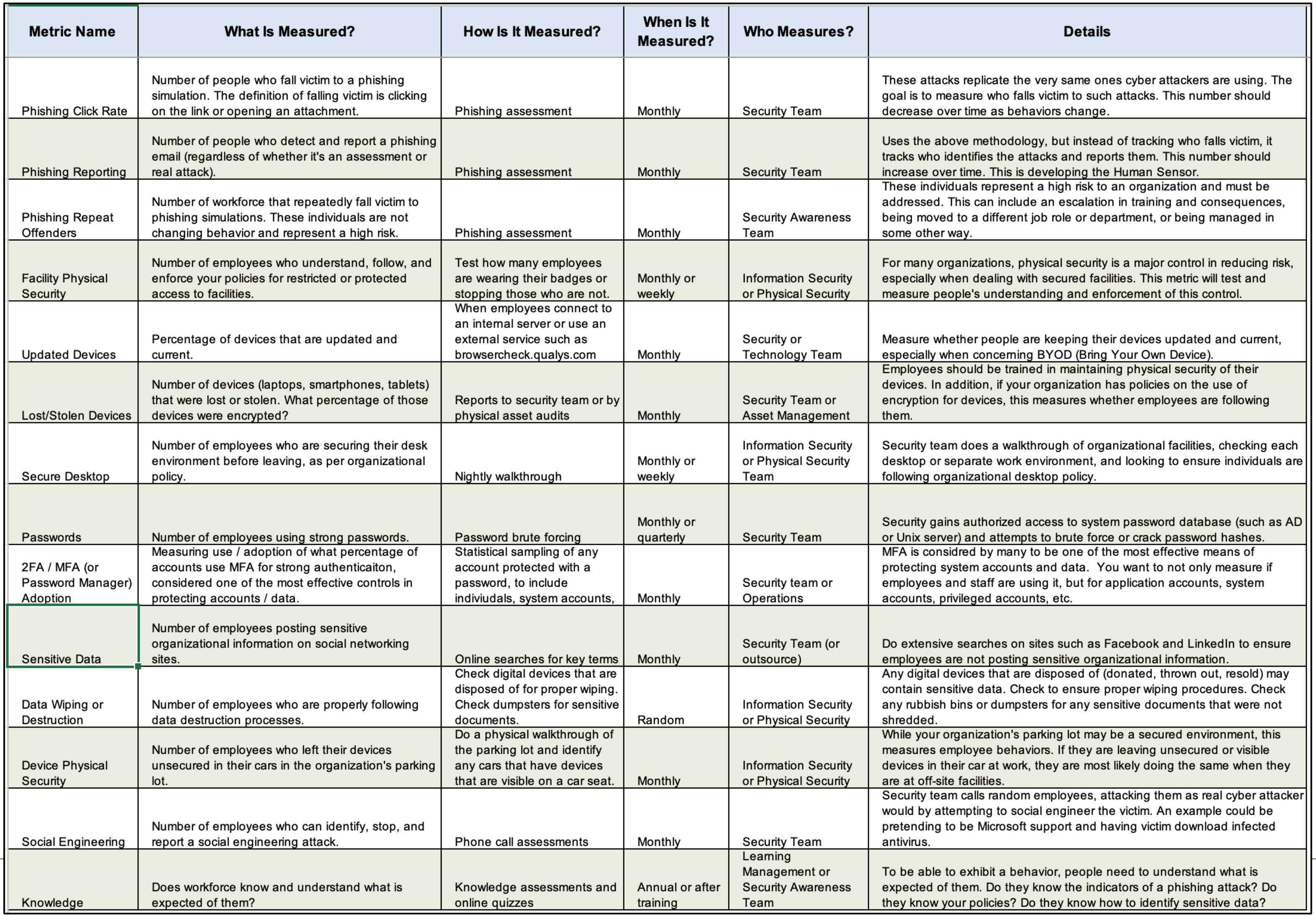
Am I Effectively Changing Those Behaviors?

3. Metrics Framework

- Identify your top human risks
- Identify the key behaviors that manage those risks

Measure those behaviors

Interactive Metrics Matrix



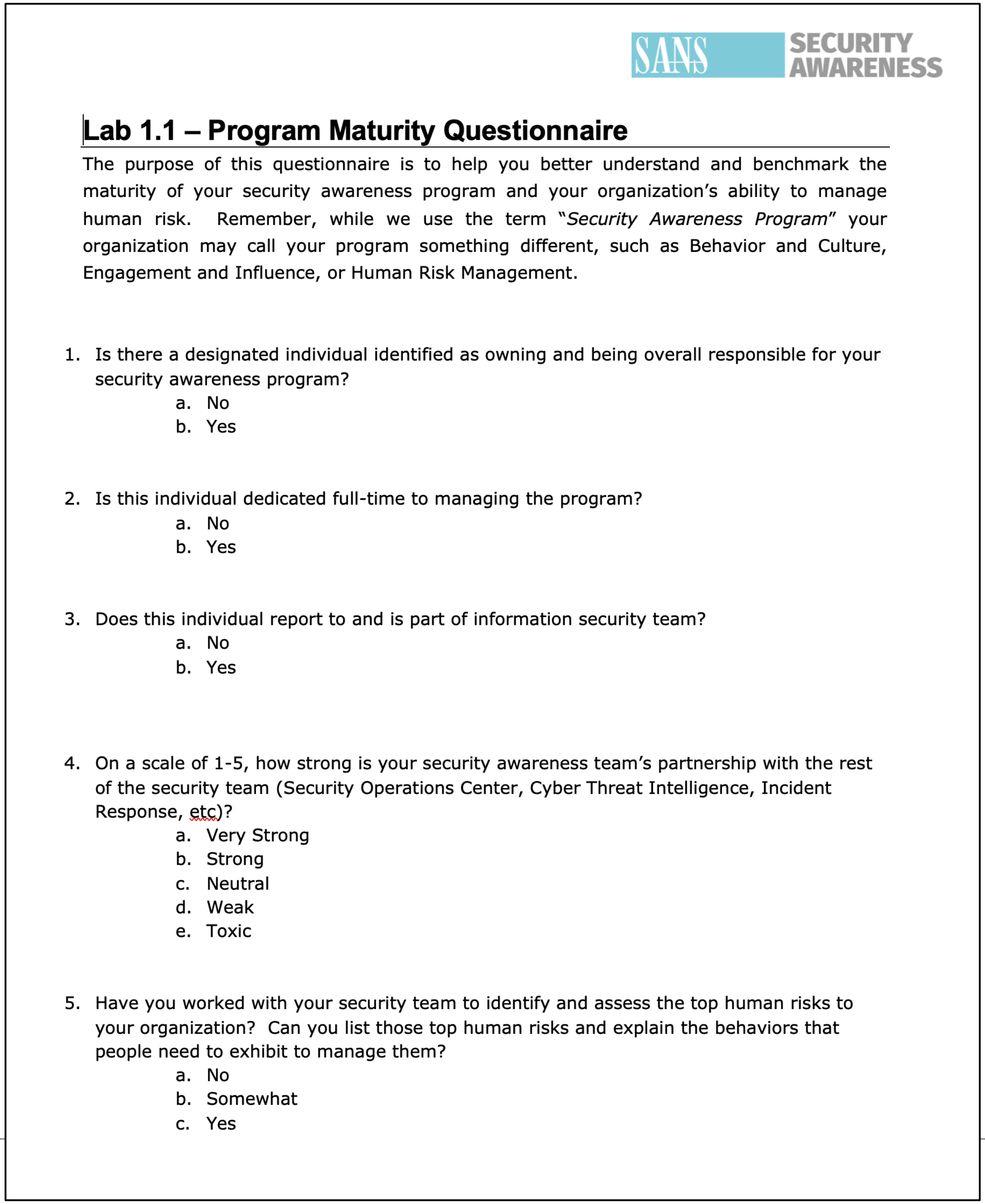
Metric Name	What Is Measured?	How Is It Measured?	When Is It Measured?	Who Measures?	Details
Phishing Click Rate	Number of people who fall victim to a phishing simulation. The definition of falling victim is clicking on the link or opening an attachment.	Phishing assessment	Monthly	Security Team	These attacks replicate the very same ones cyber attackers are using. The goal is to measure who falls victim to such attacks. This number should decrease over time as behaviors change.
Phishing Reporting	Number of people who detect and report a phishing email (regardless of whether it's an assessment or real attack).	Phishing assessment	Monthly	Security Team	Uses the above methodology, but instead of tracking who falls victim, it tracks who identifies the attacks and reports them. This number should increase over time. This is developing the Human Sensor.
Phishing Repeat Offenders	Number of workforce that repeatedly fall victim to phishing simulations. These individuals are not changing behavior and represent a high risk.	Phishing assessment	Monthly	Security Awareness Team	These individuals represent a high risk to an organization and must be addressed. This can include an escalation in training and consequences, being moved to a different job role or department, or being managed in some other way.
Facility Physical Security	Number of employees who understand, follow, and enforce your policies for restricted or protected access to facilities.	Test how many employees are wearing their badges or stopping those who are not.	Monthly or weekly	Information Security or Physical Security	For many organizations, physical security is a major control in reducing risk, especially when dealing with secured facilities. This metric will test and measure people's understanding and enforcement of this control.
Updated Devices	Percentage of devices that are updated and current.	When employees connect to an internal server or use an external service such as browsercheck.qualys.com	Monthly	Security or Technology Team	Measure whether people are keeping their devices updated and current, especially when concerning BYOD (Bring Your Own Device).
Lost/Stolen Devices	Number of devices (laptops, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted?	Reports to security team or by physical asset audits	Monthly	Security Team or Asset Management	Employees should be trained in maintaining physical security of their devices. In addition, if your organization has policies on the use of encryption for devices, this measures whether employees are following them.
Secure Desktop	Number of employees who are securing their desk environment before leaving, as per organizational policy.	Nightly walkthrough	Monthly or weekly	Information Security or Physical Security Team	Security team does a walkthrough of organizational facilities, checking each desktop or separate work environment, and looking to ensure individuals are following organizational desktop policy.
Passwords	Number of employees using strong passwords.	Password brute forcing	Monthly or quarterly	Security Team	Security gains authorized access to system password database (such as AD or Unix server) and attempts to brute force or crack password hashes.
2FA / MFA (or Password Manager) Adoption	Measuring use / adoption of what percentage of accounts use MFA for strong authenticaiton, considered one of the most effective controls in protecting accounts / data.	Statistical sampling of any account protected with a password, to include indiviudals, system accounts,	Monthly	Security team or Operations	MFA is considred by many to be one of the most effective means of protecting system accounts and data. You want to not only measure if employees and staff are using it, but for application accounts, system accounts, privileged accounts, etc.
Sensitive Data	Number of employees posting sensitive organizational information on social networking sites.	Online searches for key terms	Monthly	Security Team (or outsource)	Do extensive searches on sites such as Facebook and LinkedIn to ensure employees are not posting sensitive organizational information.
Data Wiping or Destruction	Number of employees who are properly following data destruction processes.	Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.	Random	Information Security or Physical Security	Any digital devices that are disposed of (donated, thrown out, resold) may contain sensitive data. Check to ensure proper wiping procedures. Check any rubbish bins or dumpsters for any sensitive documents that were not shredded.
Device Physical Security	Number of employees who left their devices unsecured in their cars in the organization's parking lot.	Do a physical walkthrough of the parking lot and identify any cars that have devices that are visible on a car seat.	Monthly	Information Security or Physical Security	While your organization's parking lot may be a secured environment, this measures employee behaviors. If they are leaving unsecured or visible devices in their car at work, they are most likely doing the same when they are at off-site facilities.
Social Engineering	Number of employees who can identify, stop, and report a social engineering attack.	Phone call assessments	Monthly	Security Team	Security team calls random employees, attacking them as real cyber attacker would by attempting to social engineer the victim. An example could be pretending to be Microsoft support and having victim download infected antivirus.
Knowledge	Does workforce know and understand what is expected of them?	Knowledge assessments and online quizzes	Annual or after training	Learning Management or Security Awareness Team	To be able to exhibit a behavior, people need to understand what is expected of them. Do they know the indicators of a phishing attack? Do they know your policies? Do they know how to identify sensitive data?

Strategic Metrics

- Number of incidents
- Attacker dwell time
- Costs related to incidents
- Audit and policy violations

Summary

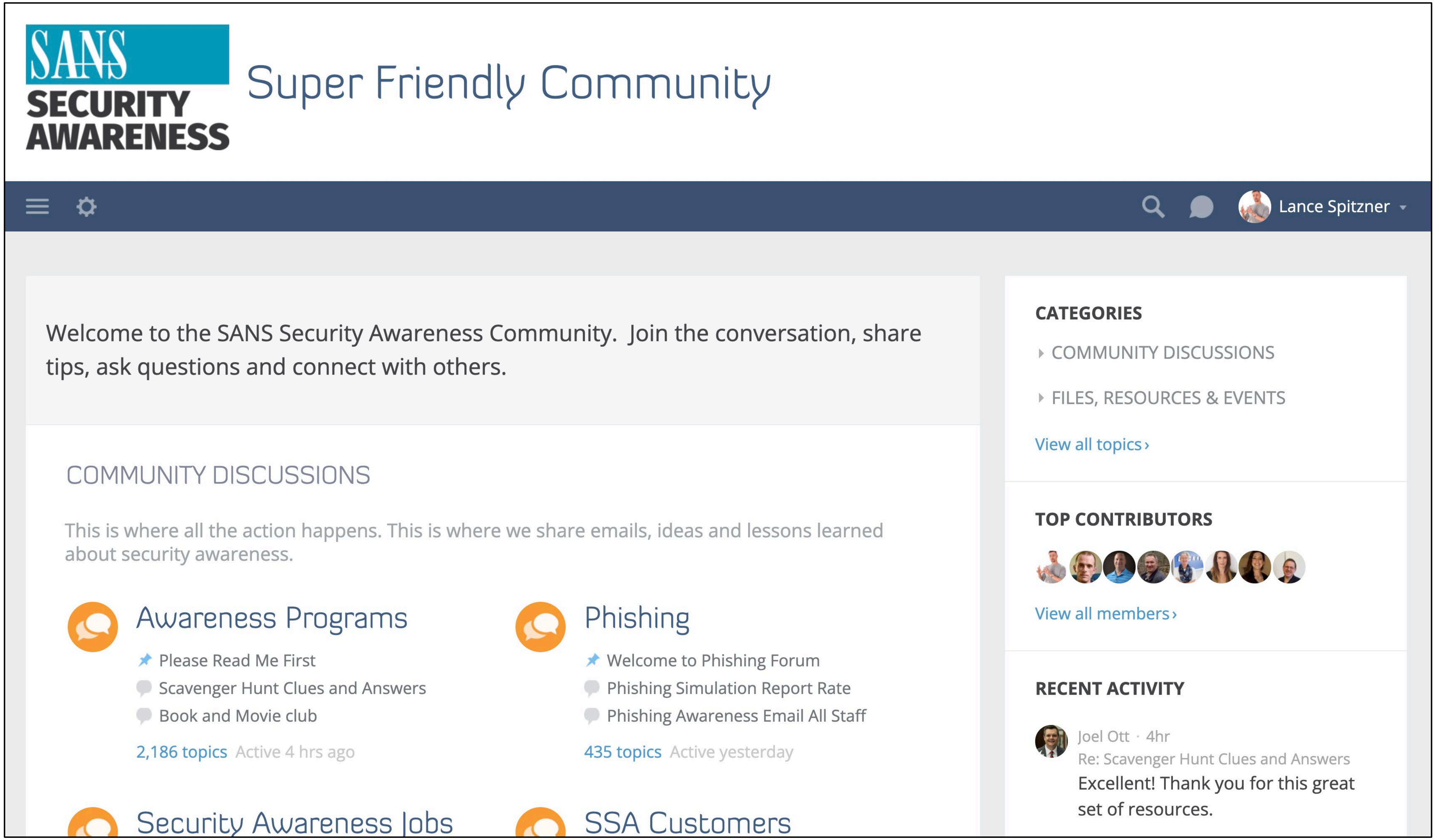
1. Take a risk focus, the compliance will follow
2. Have person in charge of security training partner with (or part of) the security team
3. Focus-on and reinforce top human risk
4. Motivate with why, enable by making security simple



Lab 1.1 – Program Maturity Questionnaire

The purpose of this questionnaire is to help you better understand and benchmark the maturity of your security awareness program and your organization's ability to manage human risk. Remember, while we use the term "*Security Awareness Program*" your organization may call your program something different, such as Behavior and Culture, Engagement and Influence, or Human Risk Management.

1. Is there a designated individual identified as owning and being overall responsible for your security awareness program?
    a. No
    b. Yes
2. Is this individual dedicated full-time to managing the program?
    a. No
    b. Yes
3. Does this individual report to and is part of information security team?
    a. No
    b. Yes
4. On a scale of 1-5, how strong is your security awareness team's partnership with the rest of the security team (Security Operations Center, Cyber Threat Intelligence, Incident Response, etc)?
    a. Very Strong
    b. Strong
    c. Neutral
    d. Weak
    e. Toxic
5. Have you worked with your security team to identify and assess the top human risks to your organization? Can you list those top human risks and explain the behaviors that people need to exhibit to manage them?
    a. No
    b. Somewhat
    c. Yes



Super Friendly Community

Welcome to the SANS Security Awareness Community. Join the conversation, share tips, ask questions and connect with others.

COMMUNITY DISCUSSIONS

This is where all the action happens. This is where we share emails, ideas and lessons learned about security awareness.

Awareness Programs
- Please Read Me First
- Scavenger Hunt Clues and Answers
- Book and Movie club

2,186 topics Active 4 hrs ago

Phishing
- Welcome to Phishing Forum
- Phishing Simulation Report Rate
- Phishing Awareness Email All Staff

435 topics Active yesterday

Security Awareness Jobs

SSA Customers

CATEGORIES
- COMMUNITY DISCUSSIONS
- FILES, RESOURCES & EVENTS

View all topics ›

TOP CONTRIBUTORS

View all members ›

RECENT ACTIVITY

Joel Ott · 4hr
Re: Scavenger Hunt Clues and Answers
Excellent! Thank you for this great set of resources.

lspitzner@sans.org

The NICE Framework and an Evolving Cybersecurity Workforce

Karen Wetzel
Manager of the NICE Framework, NICE
National Institute of Standards and Technology

The NICE Framework and an Evolving Cybersecurity Workforce

Karen A. Wetzel, Lead, NICE Framework
National Institute of Standards and Technology
U.S. Department of Commerce
karen.wetzel@nist.gov

FISSEA Conference | May 2024

Cybersecurity Workforce Challenges

- Aging workforce
- Growing demand
- Low retention
- Low availability of entry points for new workers
- Low diversity
- Highly experienced and skilled workforce requirements

NICE | workforce framework for cybersecurity

Image source: shutterstock.com

Image Source: https://pxhere.com/en/photo/1562171

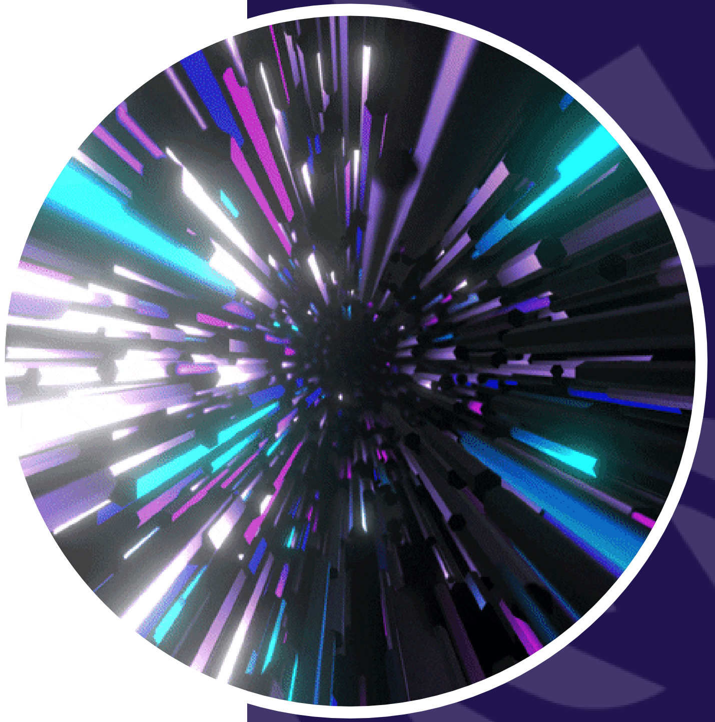
Cybersecurity Workforce Opportunities

- Demand for workers is high
- Work is well paying
- Mission is attractive
- Positions can often accommodate remote work
- Multiple career pathways

NICE | workforce framework for cybersecurity

Preparing for the Future

- Digital economy
- AI/ML/IoT
- OT/IT convergence
- Distributed workforce
- Increased attacks, phishing, ransomware
- Etc.



http://bit.ly/2L8Cbnl

NICE | workforce framework for cybersecurity

NICE FRAMEWORK COMPONENTS V1.0.0

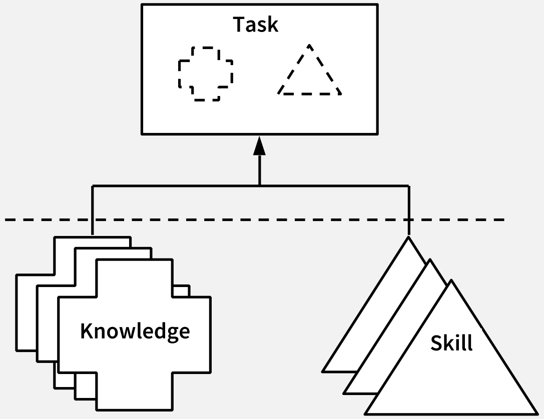
UPDATED WORK ROLES & CATEGORIES, INCLUDING ONE NEW WORK ROLE!

- OVERSIGHT & GOVERNANCE
- DESIGN & DEVELOPMENT
- IMPLEMENTATION & OPERATION
- PROTECTION & DEFENSE
- INVESTIGATION
- CYBERSPACE INTELLIGENCE
- CYBERSPACE EFFECTS

11 NEW COMPETENCY AREAS

- Access Controls
- Artificial Intelligence (AI) Security
- Asset Management
- Cloud Security
- Communications Security
- Cryptography
- Cyber Resiliency
- DevSecOps
- Operating Systems (OS) Security
- Operational Technology (OT) Security
- Supply Chain Security

OVER 2,000 UPDATED TASK, KNOWLEDGE, & SKILL (TKS) STATEMENTS



www.nist.gov/nice/framework

Resource: NICE Framework Resource Center

Value for...

EMPLOYERS

- Broaden workforce pipeline and increase diversity
- Create job descriptions and assess candidate skills
- Track and plan workforce capabilities
- Develop employees through role-based training

LEARNERS (students, job-seekers, and employees)

- Discover and plan for cybersecurity careers
- Knowledge and skills development
- Demonstrate capability and evidence competency

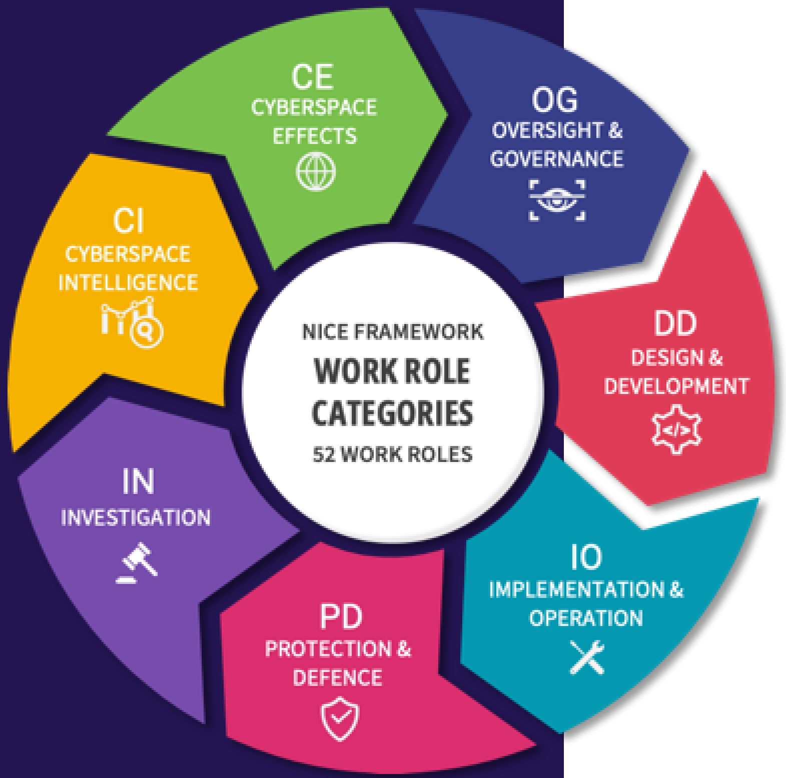
EDUCATORS

- Develop learning courses and programs that address employer needs
- Align learning experiences with the NICE Framework
- Conduct performance-based assessments

GOVERNMENT • INDUSTRY • ACADEMIA

NICE | workforce framework for cybersecurity

Evolving to Meet Current & Future Needs

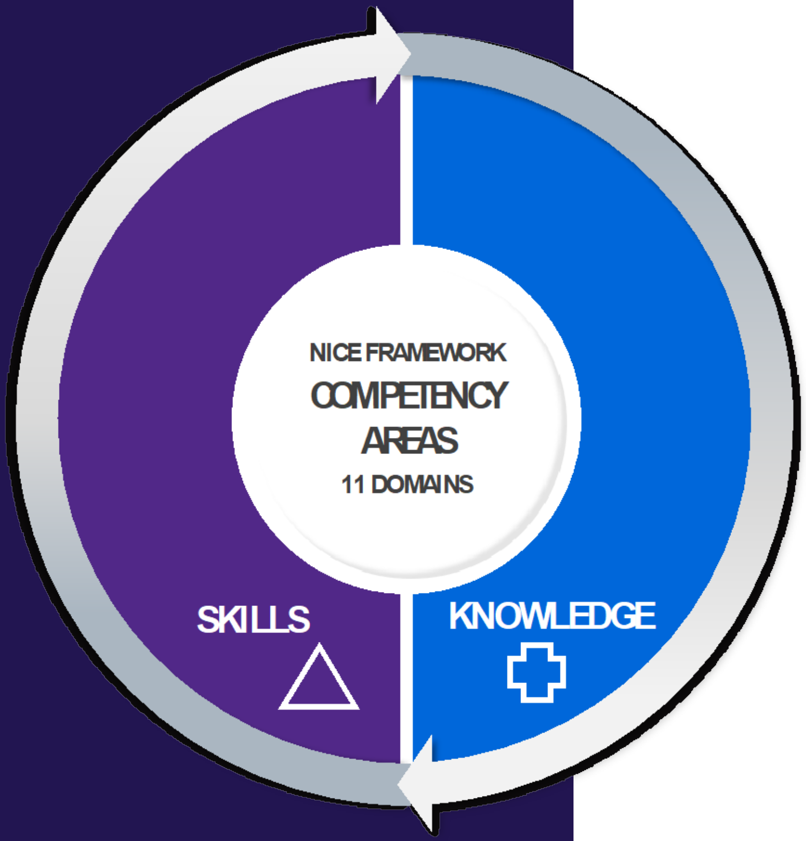


Work Roles

Potential New Roles:
- Cybersecurity Risk Analysis
- Cybercrime Prosecution
- Learning Program Management
- OT Cybersecurity Engineering
- Product Security
- SCRM Analysis
- Secure Procurement
- Security Engineering
- Systems Security Engineering

Work Role Updates
- Review of existing work roles (e.g., Digital Evidence Forensics)
- Impact of automation/AI on existing roles
- New or updated TKS statements for existing roles

Evolving to Meet Current & Future Needs



Competency Area Development

- Access Controls
- Artificial Intelligence (AI) Security
- Asset Management
- Cloud Security
- Communications Security
- Cryptography
- Cyber Resiliency
- DevSecOps
- Operating Systems (OS) Security
- Operational Technology (OT) Security
- Supply Chain Security

New Work Role: How We Got Here

We started with Cybersecurity Awareness

- **Sept. 2021 NICE Workshop: "Developing a Workforce for Security Awareness and Behavior Change"**
- **Related NICE Framework Work Roles:**
    - Cybersecurity Workforce Management (OG-WRL-003 | OPM 751)
    - Cybersecurity Curriculum Development (OG-WRL-004 | OPM 711)
    - Cybersecurity Instruction (OG-WRL-005 | OPM 712)
- **800-53, "Awareness and Training" (AT) Category:**
    - Policy and Procedures
    - Literacy Training and Awareness
    - Role-Based Training
    - Training Records
    - Contacts with Security Groups and Associations
    - Training Feedback
- **CSF 2.0, "Awareness and Training" (PR.AT) Category:**
  The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks

Initial Drafting

- Cybersecurity Awareness: Responsible for creating, maintaining, and determining the efficacy of the organizational cybersecurity awareness program.
- Initial Task identification and development

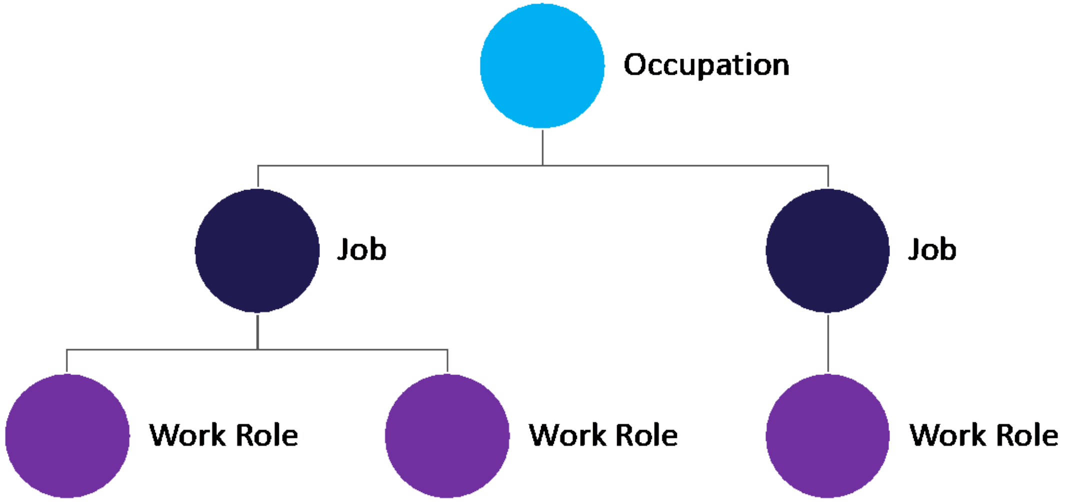
Reimagining: Learning Program Management

- NIST SP 800-50 Revision: Building a Cybersecurity and Privacy Learning Program
    - "provides guidance to create and manage a program that includes cybersecurity and privacy awareness campaigns, role-based training, and other workforce education programs"
    - Introduces "Learning Program Manager"

What are Learning Program Management responsibilities?

Learning Program Managers… [are] responsible for the **analysis, design, development, and delivery** of the [Cybersecurity and Privacy Learning Programs] CPLPs….”

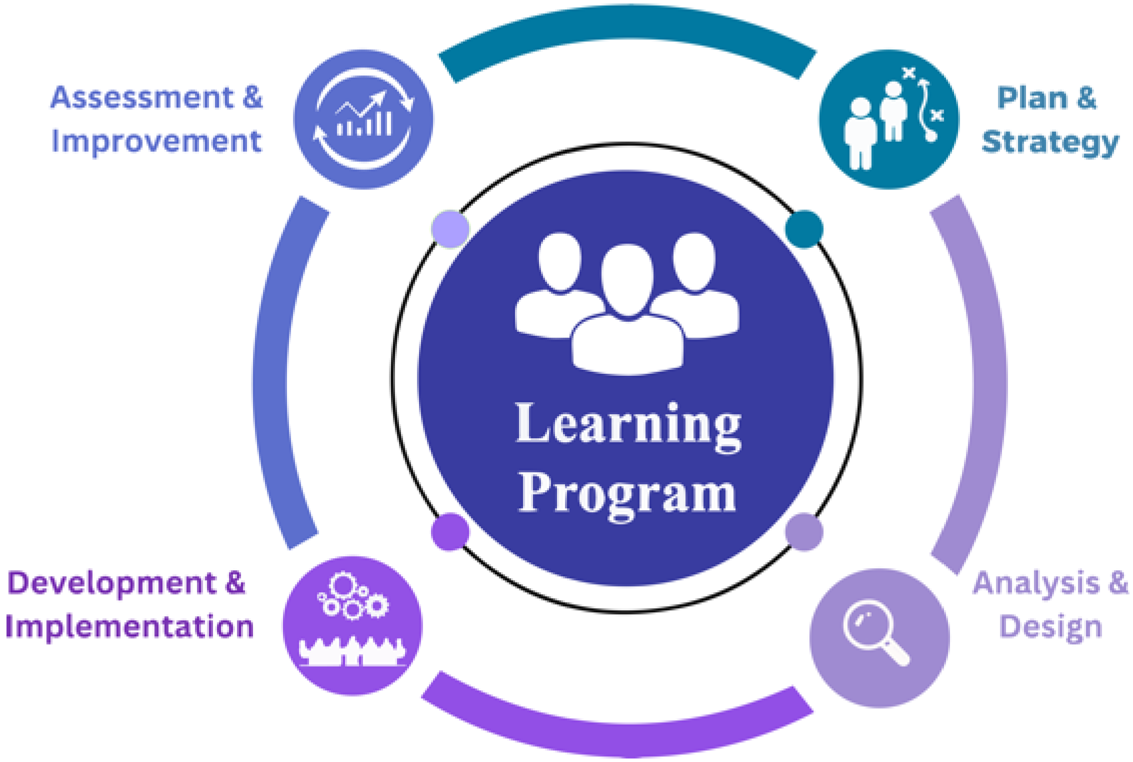
NIST 800-50 Revision Draft



Learning Program Management

Responsible for creating, maintaining, and determining the efficacy of the organizational workforce learning program. Includes managing and directing program resources and engaging with leadership and management in support of program goals.

1. **Build the Program**
    a. Create a strategic plan
    b. Develop CPLP policies and procedures
    c. Determine CPLP measurements and metrics
    d. Secure program resources
2. **Implement and Manage the Program**
    a. Inventory the workforce
    b. Inventory learning resources
    c. Determine learning needs
    d. Fulfill learning needs
3. **Conduct Program Assessment and Reporting**
    a. Determine program efficacy
    b. Reporting

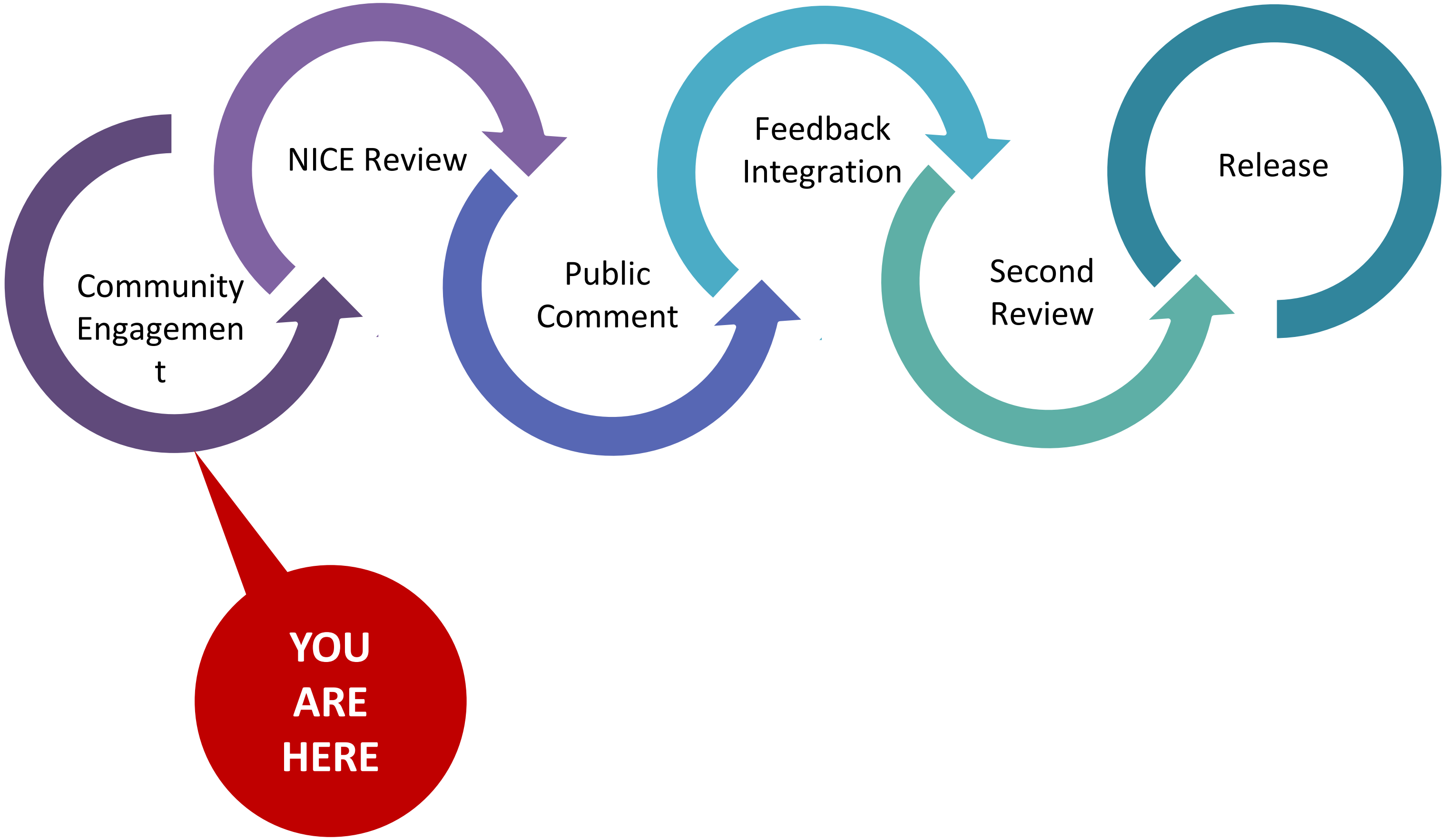


SP 800-50 Draft Revision: Building a Cybersecurity and Privacy Learning Program

Share Your Feedback!

NICEFramework@nist.gov

1. **Is this role needed?**
    a. Is it a role that currently exists in organizations?
    b. Is the scope unique and distinct from other roles?
    c. Does it support organizational cybersecurity?
2. **Do these broad duties and their parts ring true with your experience?**
3. **Would you be willing to help develop TKS for this role?**



NICE workforce framework for cybersecurity www.nist.gov/nice • NICE@nist.gov

34th Annual FISSEA Conference

Morning Networking Break and Exhibitor Showcase

10:30am-11:00am ET

#FISSEA | nist.gov/fissea

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

Welcome Back!

Brooke Crisp
FISSEA Co-Chair

The Human Firewall: Innovative Approaches for HR in Cybersecurity Training

Ani Banerjee
Chief Human Resource Officer
KnowBe4

KnowBe4
Human error. Conquered.

The Human Firewall

Innovative Approaches for HR in Cybersecurity Training

About me

- ★ 30 years of HR experience
- ★ Global companies
- ★ VMware, Dell, Yahoo!, and AOL
- ★ Currently the Chief Human Resources Officer for KnowBe4, provider of the world's largest security awareness training and simulated phishing platform used by more than 65,000 organizations!

KnowBe4
Human error. Conquered.

Overview

Cybersecurity culture vs traditional training

Additional challenges for remote/hybrid employees

Ideas for taking Cybersecurity from training to creating a

culture Cross departmental collaboration

Cybersecurity Culture vs Training

Learning Culture

- Focuses on creating habitual practices ✓
- Is embedded in company norms ✓
- Continuous and ongoing ✓
- Becomes second nature to employees ✓

Training

- ✗ Focuses on getting the information
- ✗ Is rarely discussed after completion
- ✗ Traditionally done once a year
- ✗ Mandatory for employees

Remote / Hybrid Challenges

Lack of "physical" security

Insecure Wi-Fi networks

Difficulty enforcing protocols

Engagement levels in culture

From Training to Culture!

- ✓ Using AI, training and risk scores geared towards each department/role and individual habits
- ✓ Regular simulated phishing tests
- ✓ Regular training to include other “bad actor” tactics used

- ✓ Empower employees to be constantly learning
- ✓ Allow mistakes to be learning opportunities
- ✓ MAKE IT FUN and celebrate the wins!

Cross Department Collaboration

HR

Legal

IT / InfoSec

- Create policies
- Personalize training
- Up to date best practices
- Make it engaging

Any Questions?

Thank you all for coming and we hope you enjoy the rest of the FISSEA conference!

KnowBe4
Human error. Conquered.

Digital Literacy and Disinformation

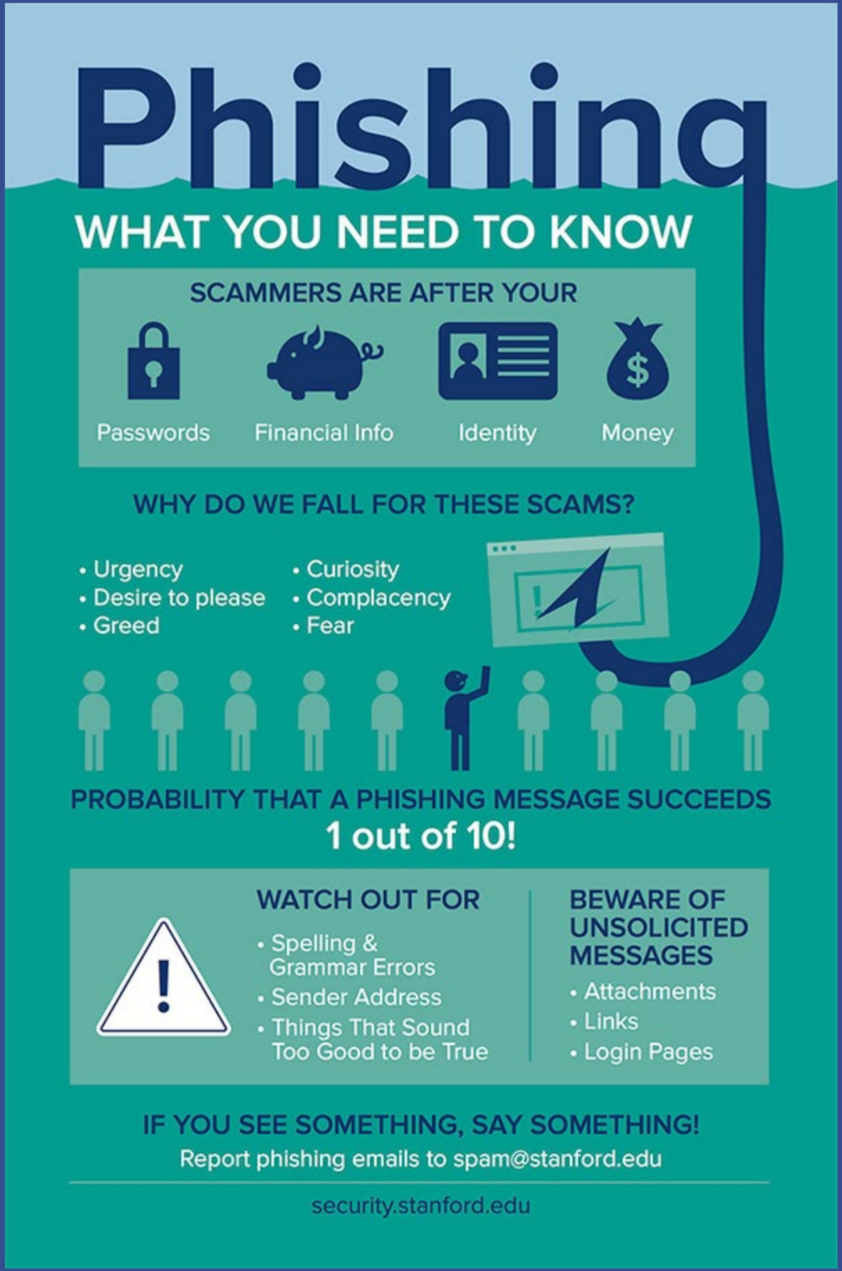
Anita Nikolich
University of Illinois

Media Literacy and Gamification

FISSEA May 14, 2024

Anita Nikolich

D·A·R·T·



Phishing

WHAT YOU NEED TO KNOW

SCAMMERS ARE AFTER YOUR

Passwords

Financial Info

Identity

Money

WHY DO WE FALL FOR THESE SCAMS?

- Urgency
- Desire to please
- Greed
- Curiosity
- Complacency
- Fear

PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS

1 out of 10!

WATCH OUT FOR

- Spelling & Grammar Errors
- Sender Address
- Things That Sound Too Good to be True

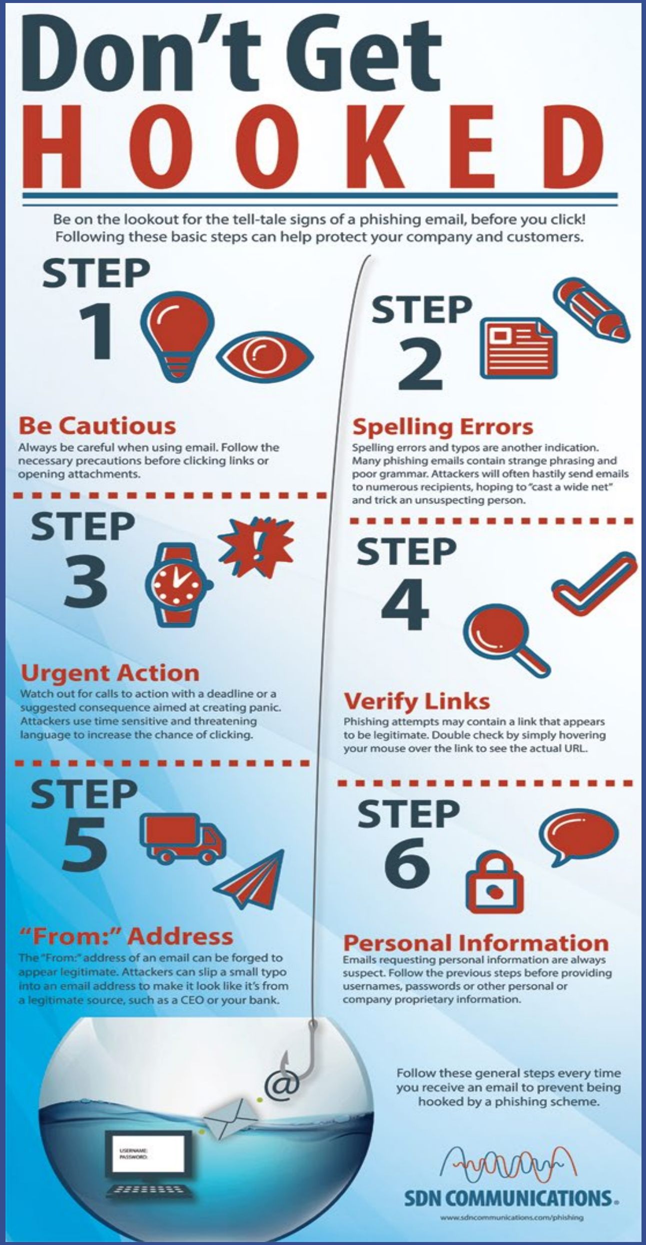
BEWARE OF UNSOLICITED MESSAGES

- Attachments
- Links
- Login Pages

IF YOU SEE SOMETHING, SAY SOMETHING!

Report phishing emails to spam@stanford.edu

security.stanford.edu



Don't Get HOOKED

Be on the lookout for the tell-tale signs of a phishing email, before you click! Following these basic steps can help protect your company and customers.

STEP 1

Be Cautious

Always be careful when using email. Follow the necessary precautions before clicking links or opening attachments.

STEP 2

Spelling Errors

Spelling errors and typos are another indication. Many phishing emails contain strange phrasing and poor grammar. Attackers will often hastily send emails to numerous recipients, hoping to "cast a wide net" and trick an unsuspecting person.

STEP 3

Urgent Action

Watch out for calls to action with a deadline or a suggested consequence aimed at creating panic. Attackers use time sensitive and threatening language to increase the chance of clicking.

STEP 4

Verify Links

Phishing attempts may contain a link that appears to be legitimate. Double check by simply hovering your mouse over the link to see the actual URL.

STEP 5

"From:" Address

The "From:" address of an email can be forged to appear legitimate. Attackers can slip a small typo into an email address to make it look like it's from a legitimate source, such as a CEO or your bank.

STEP 6

Personal Information

Emails requesting personal information are always suspect. Follow the previous steps before providing usernames, passwords or other personal or company proprietary information.

Follow these general steps every time you receive an email to prevent being hooked by a phishing scheme.

SDN COMMUNICATIONS®

www.sdncommunications.com/phishing

Project Origins

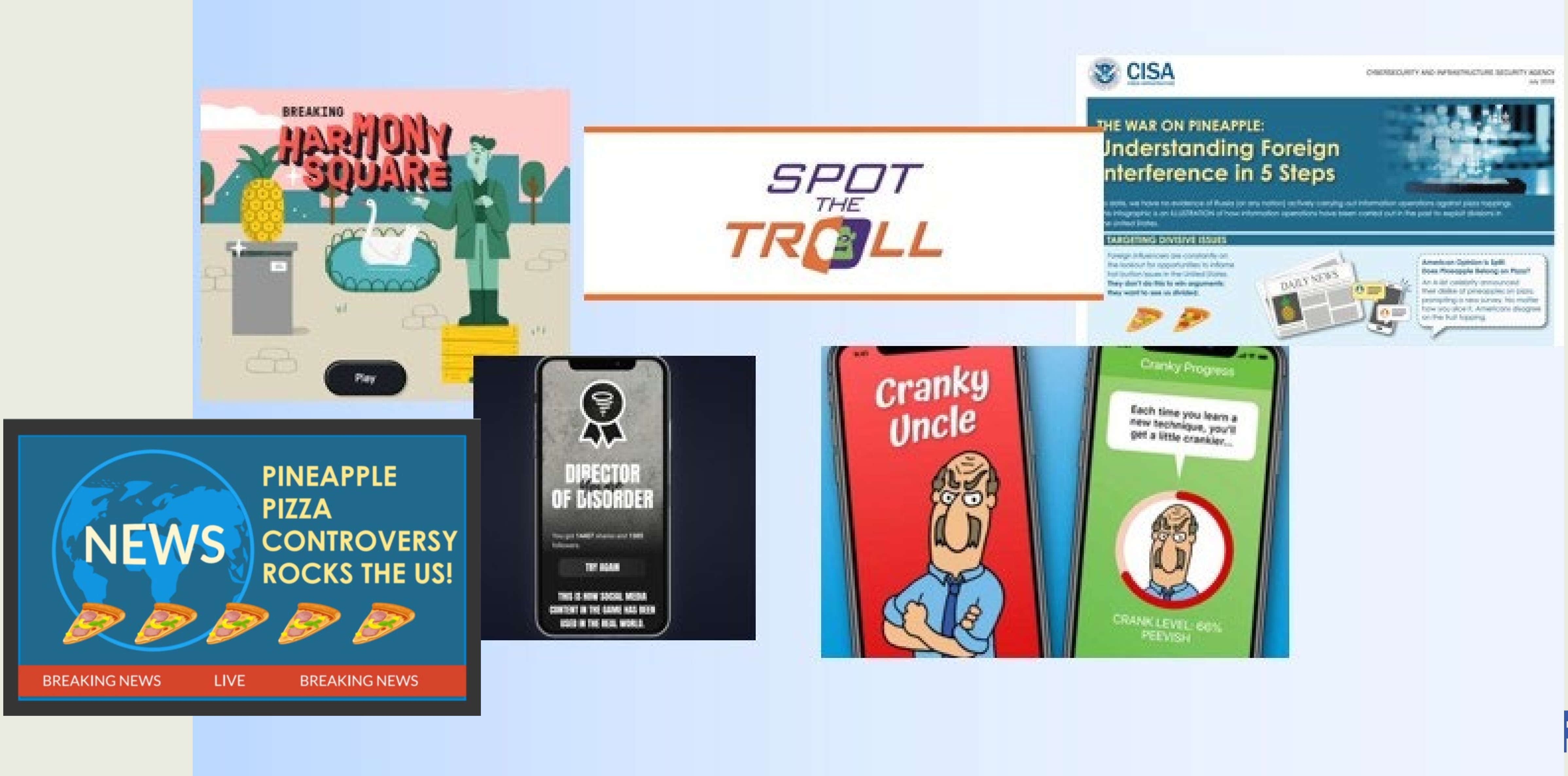
Trust and Authenticity in Communications Systems
(2021)

Team Expertise

- Cybersecurity
- Deep Fakes
- Game Design
- Social Media Campaigns
- Gerontology
- Communications
- Storytelling
- Cryptocurrency Scams

D·A·R·T

Gamifying Media Literacy



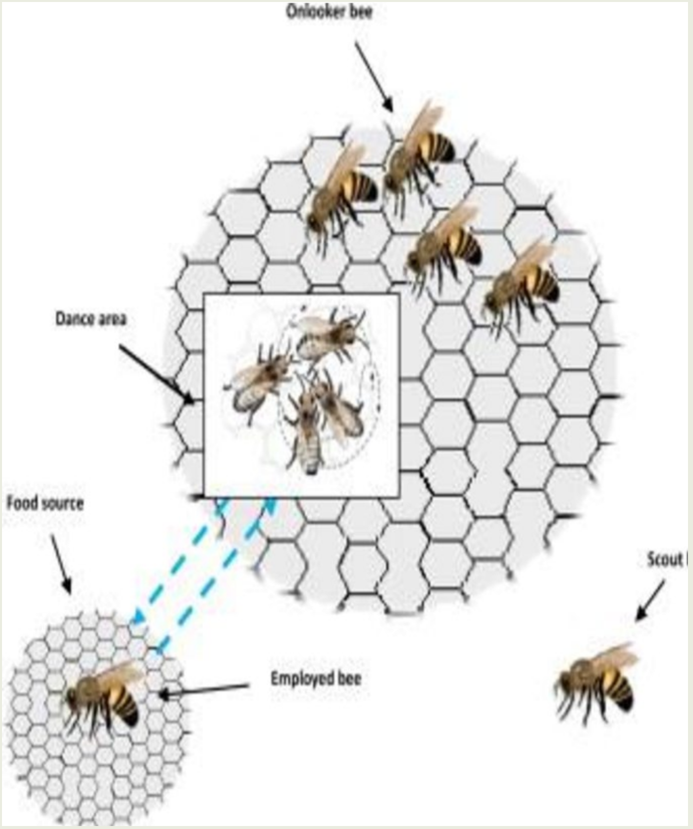
Why is Media Literacy Such a Challenge?

Truth is Often Difficult to Judge

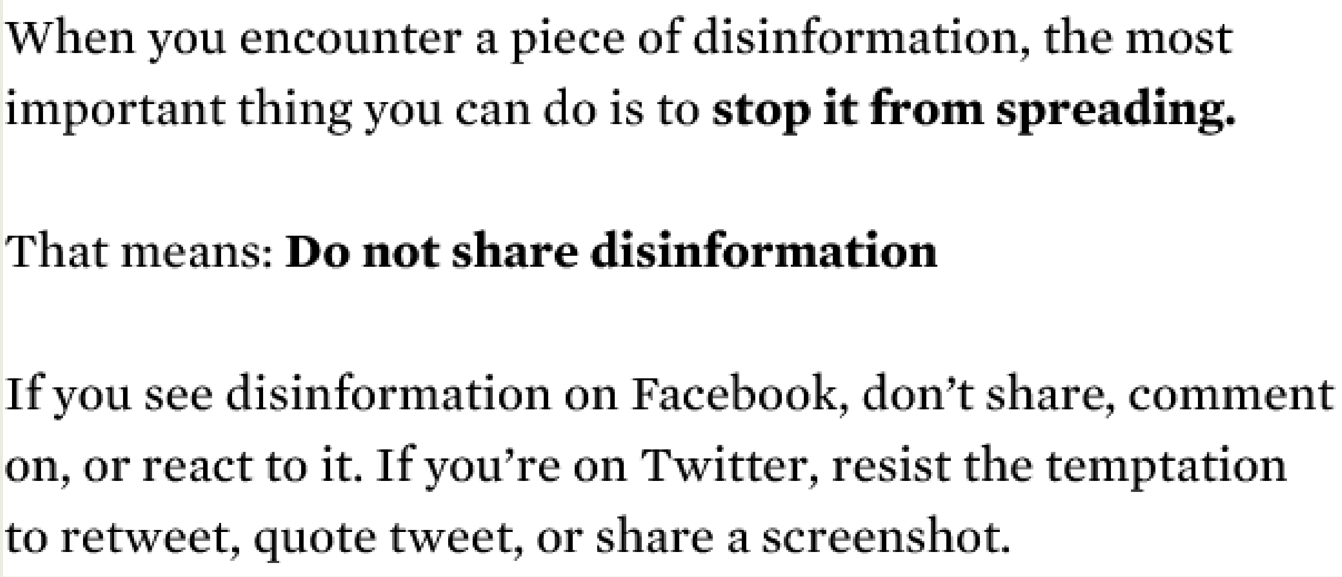
People Are Not Rational

Snake Oil:

-Peddling a **solution** to solving media literacy



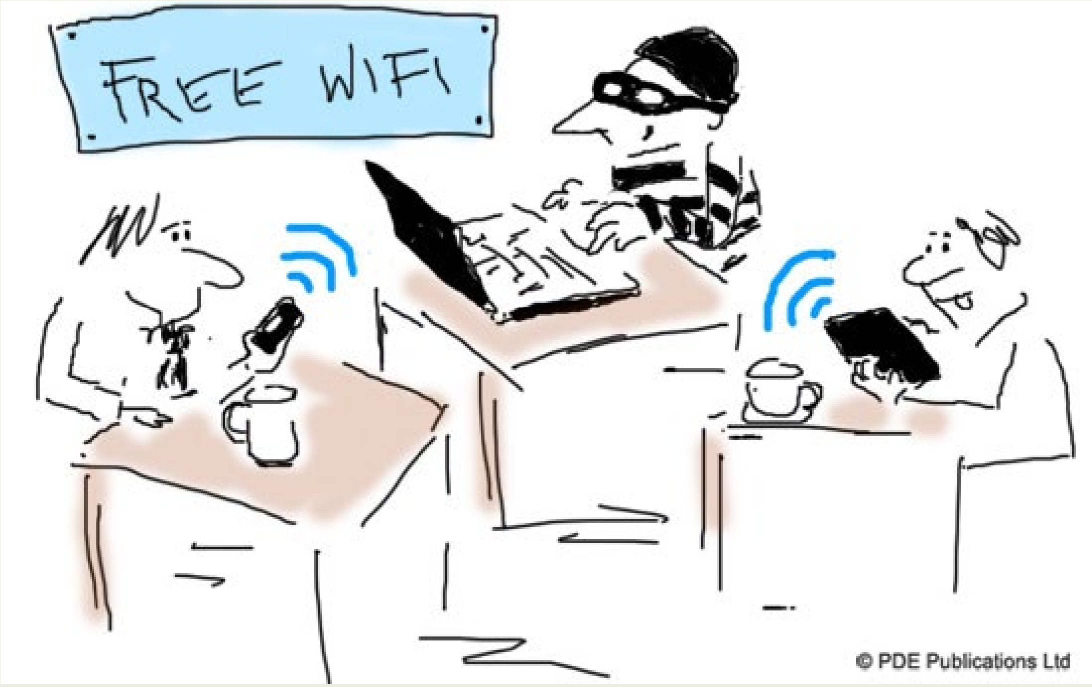
Tips on Information Hygiene Often Unhelpful



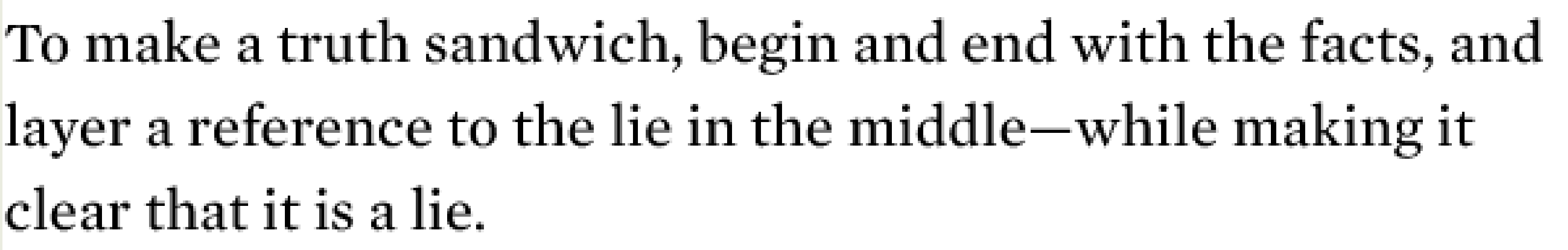
When you encounter a piece of disinformation, the most important thing you can do is to **stop it from spreading.**

That means: **Do not share disinformation**

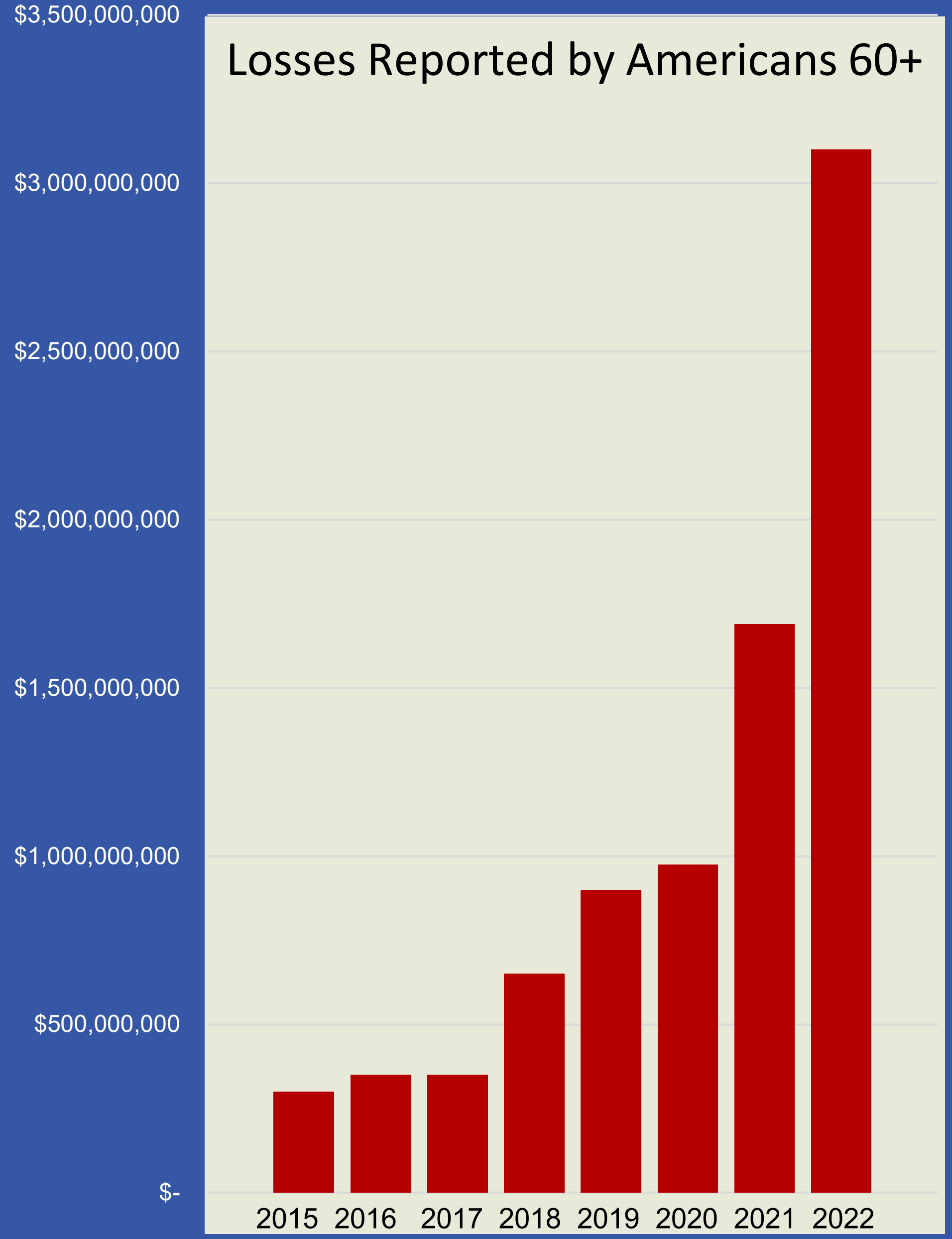
If you see disinformation on Facebook, don’t share, comment on, or react to it. If you’re on Twitter, resist the temptation to retweet, quote tweet, or share a screenshot.



© PDE Publications Ltd



To make a truth sandwich, begin and end with the facts, and layer a reference to the lie in the middle—while making it clear that it is a lie.



$35,101

Average loss per incident

5,456

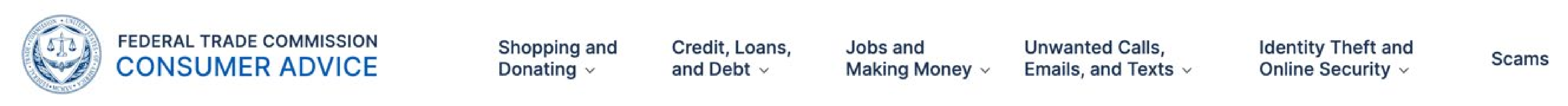
Victims losing more than $100K

Source: FBI Elder Fraud Report (2022).

Existing Resources Aren't Enough

AARP®
Fraud Watch Network

MW
MediaWise
for SENIORS


FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and Donating ⌄
Credit, Loans, and Debt ⌄
Jobs and Making Money ⌄
Unwanted Calls, Emails, and Texts ⌄
Identity Theft and Online Security ⌄
Scams

Hacker Highschool
SECURITY AWARENESS FOR TEENS

Anti-Phishing Phil™

Target Audience

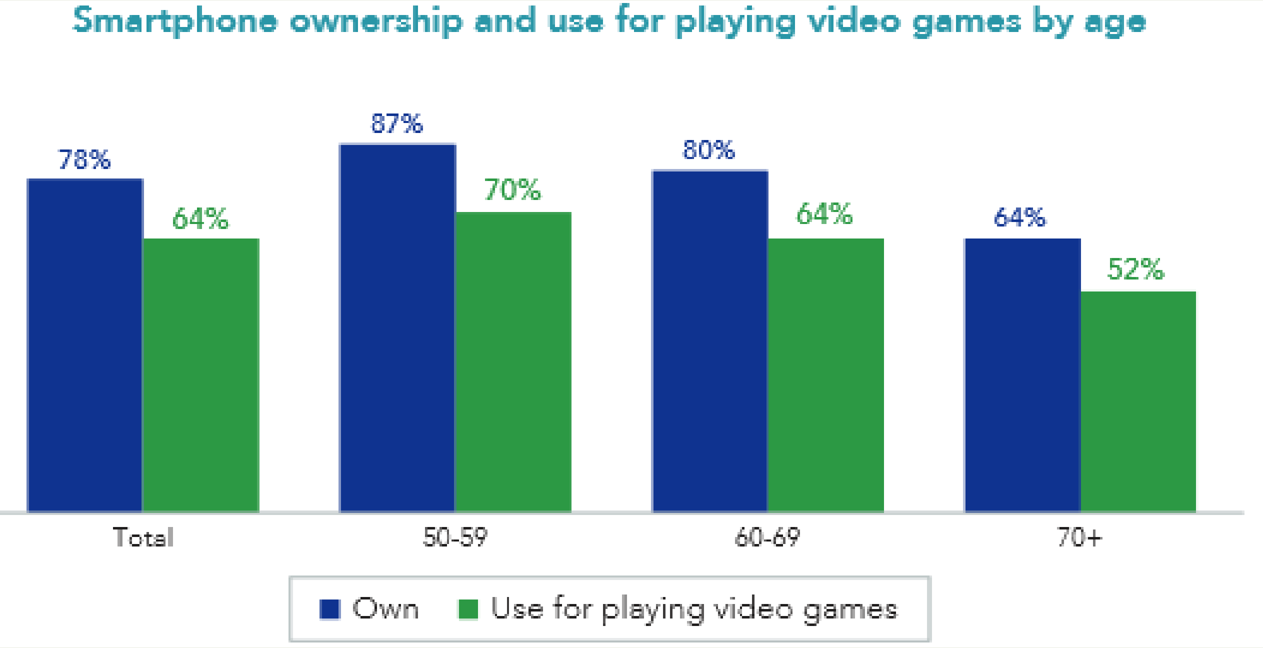
Age: 60+

Has a phone or tablet

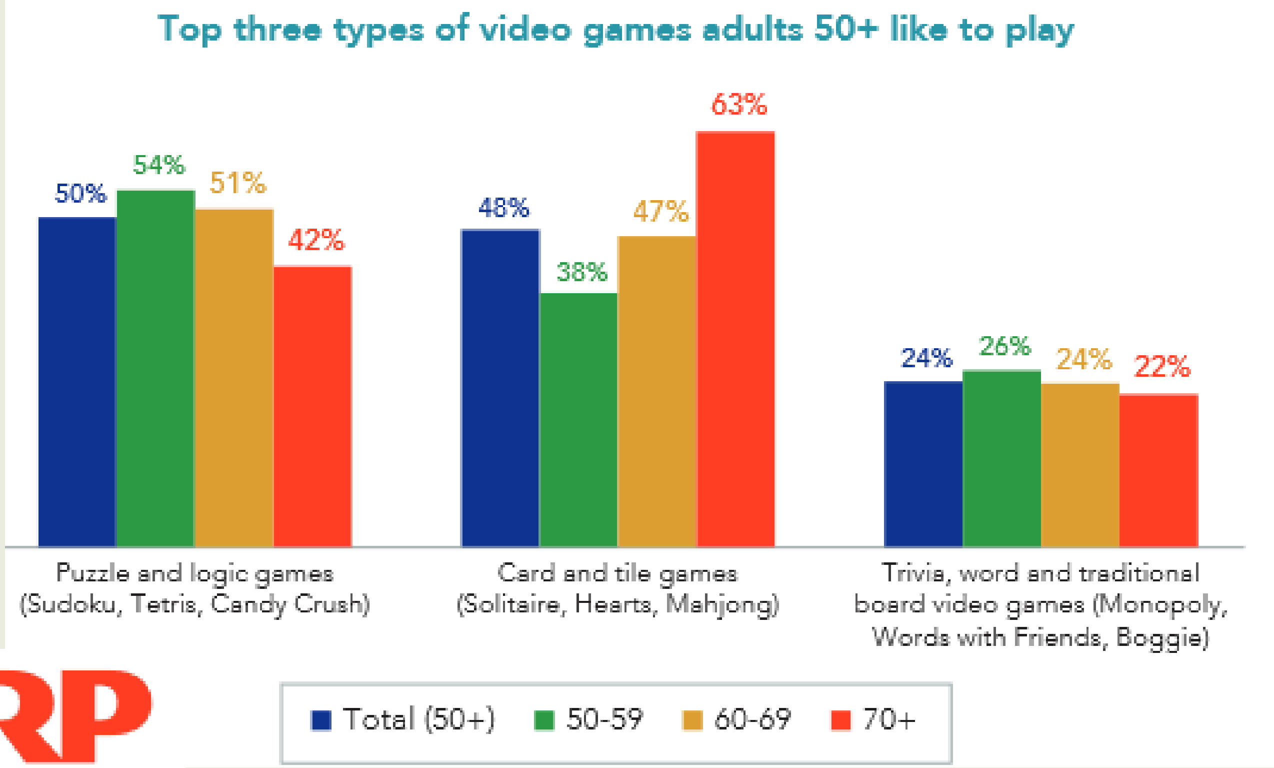
Plays single player games to:

- Relax
- Keep the mind sharp
- Socialize

Why a Game?

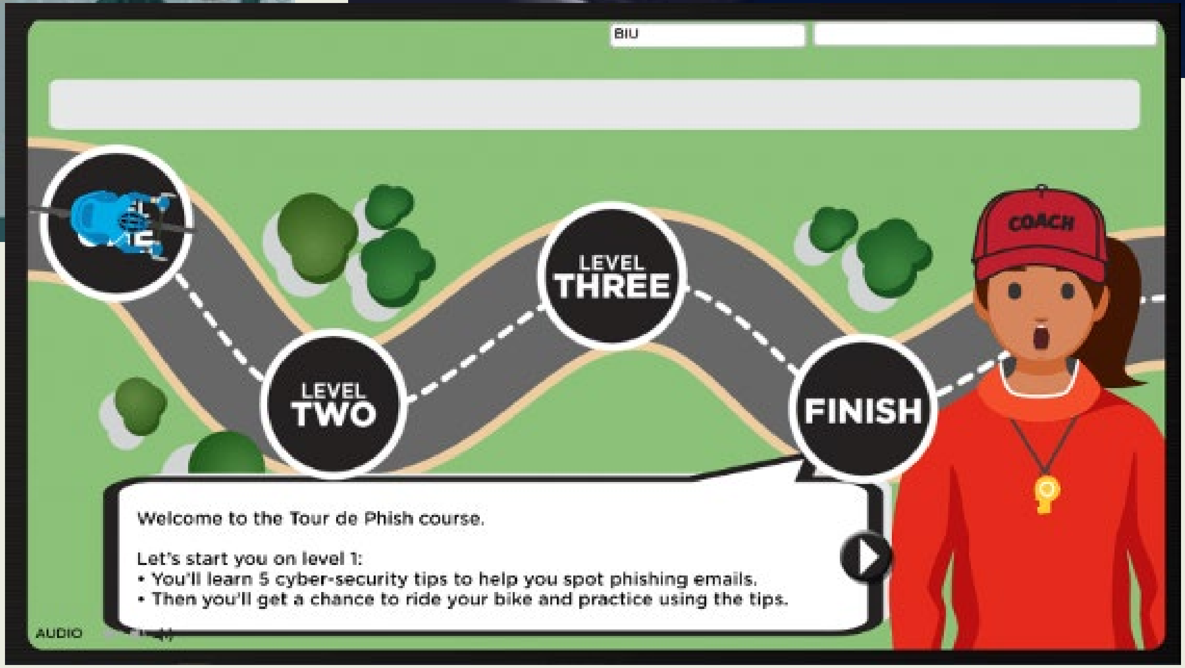


Many believe games help their mental sharpness/brain health



AARP

Traditional Security Gamification



Welcome to the Tour de Phish course.

Let's start you on level 1:
- You'll learn 5 cyber-security tips to help you spot phishing emails.
- Then you'll get a chance to ride your bike and practice using the tips.

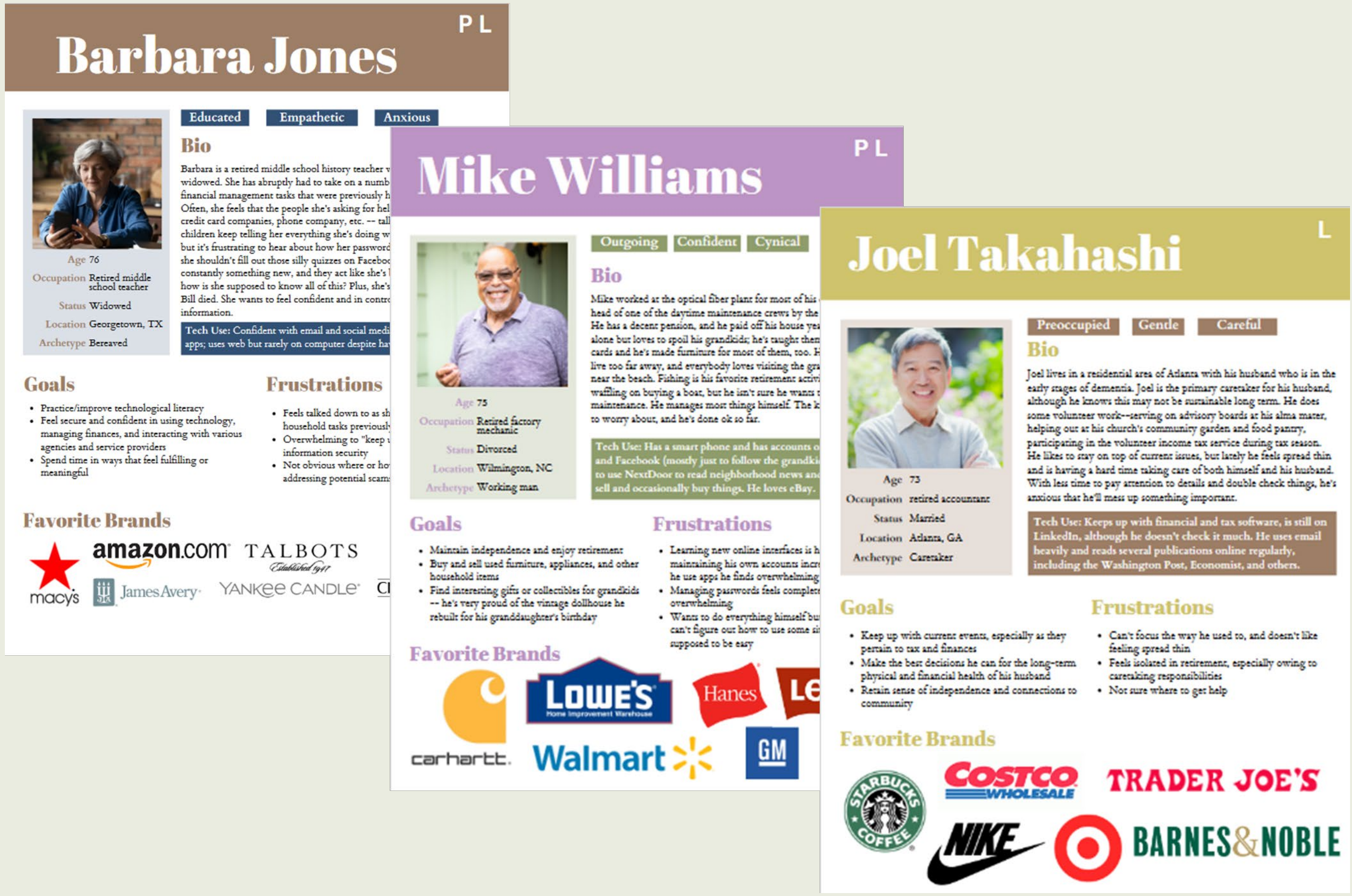
What Are We Really Trying to Accomplish?

Designing the Game: User Research & User Personas

What do older adults understand about scams - have they been scammed?

Do they know how to report?

Would they use a game??



Barbara Jones P L

Educated | Empathetic | Anxious

Bio

Barbara is a retired middle school history teacher w
widowed. She has abruptly had to take on a numb
financial management tasks that were previously h
Often, she feels that the people she's asking for hel
credit card companies, phone company, etc. -- tall
children keep telling her everything she's doing w
but it's frustrating to hear about how her password
she shouldn't fill out those silly quizzes on Faceboo
constantly something new, and they act like she's
how is she supposed to know all of this? Plus, she's
Bill died. She wants to feel confident and in contr
information.

Tech Use: Confident with email and social medi
apps; uses web but rarely on computer despite ha

Age 76
Occupation Retired middle school teacher
Status Widowed
Location Georgetown, TX
Archetype Bereaved

Goals

- Practice/improve technological literacy
- Feel secure and confident in using technology, managing finances, and interacting with various agencies and service providers
- Spend time in ways that feel fulfilling or meaningful

Frustrations

- Feels talked down to as sh
  household tasks previousl
- Overwhelming to "keep u
  information security
- Not obvious where or ho
  addressing potential scam

Favorite Brands

Mike Williams P L

Outgoing | Confident | Cynical

Bio

Mike worked at the optical fiber plant for most of his
head of one of the daytime maintenance crews by the
He has a decent pension, and he paid off his house yea
alone but loves to spoil his grandkids; he's taught them
cards and he's made furniture for most of them, too. H
live too far away, and everybody loves visiting the gra
near the beach. Fishing is his favorite retirement activi
waffling on buying a boat, but he isn't sure he wants t
maintenance. He manages most things himself. The k
to worry about, and he's done ok so far.

Tech Use: Has a smart phone and has accounts o
and Facebook (mostly just to follow the grandki
to use NextDoor to read neighborhood news and
sell and occasionally buy things. He loves eBay.

Age 75
Occupation Retired factory mechanic
Status Divorced
Location Wilmington, NC
Archetype Working man

Goals

- Maintain independence and enjoy retirement
- Buy and sell used furniture, appliances, and other household items
- Find interesting gifts or collectibles for grandkids -- he's very proud of the vintage dollhouse he rebuilt for his granddaughter's birthday

Frustrations

- Learning new online interfaces is h
  maintaining his own accounts incre
  he use apps he finds overwhelming
- Managing passwords feels complete
  overwhelming
- Wants to do everything himself bu
  can't figure out how to use some si
  supposed to be easy

Favorite Brands

Joel Takahashi L

Preoccupied | Gentle | Careful

Bio

Joel lives in a residential area of Atlanta with his husband who is in the early stages of dementia. Joel is the primary caretaker for his husband, although he knows this may not be sustainable long term. He does some volunteer work--serving on advisory boards at his alma mater, helping out at his church's community garden and food pantry, participating in the volunteer income tax service during tax season. He likes to stay on top of current issues, but lately he feels spread thin and is having a hard time taking care of both himself and his husband. With less time to pay attention to details and double check things, he's anxious that he'll mess up something important.

Tech Use: Keeps up with financial and tax software, is still on LinkedIn, although he doesn't check it much. He uses email heavily and reads several publications online regularly, including the Washington Post, Economist, and others.

Age 73
Occupation retired accountant
Status Married
Location Atlanta, GA
Archetype Caretaker

Goals

- Keep up with current events, especially as they pertain to tax and finances
- Make the best decisions he can for the long-term physical and financial health of his husband
- Retain sense of independence and connections to community

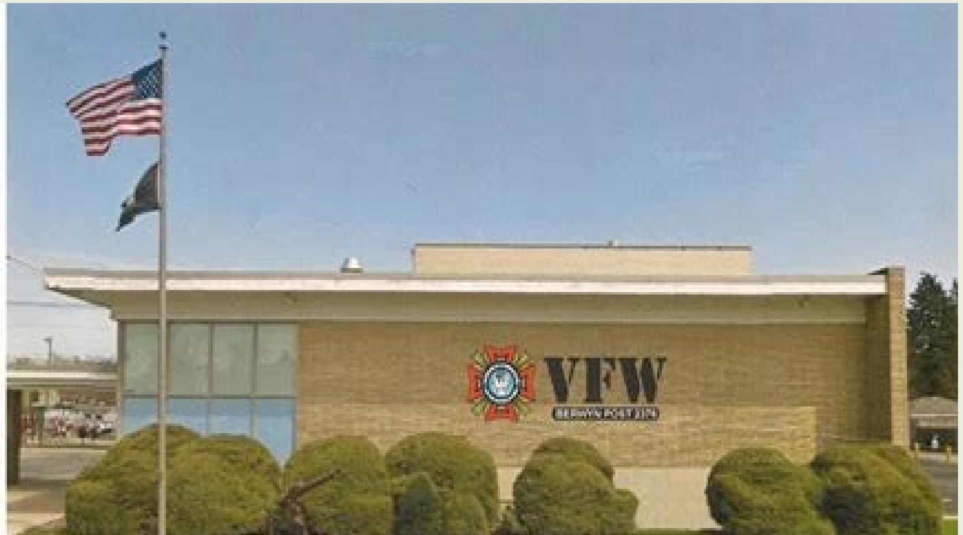
Frustrations

- Can't focus the way he used to, and doesn't like feeling spread thin
- Feels isolated in retirement, especially owing to caretaking responsibilities
- Not sure where to get help

Favorite Brands

Talking and Listening to Users

Pickens County, SC Flea Market



Assisted Living Supervisor

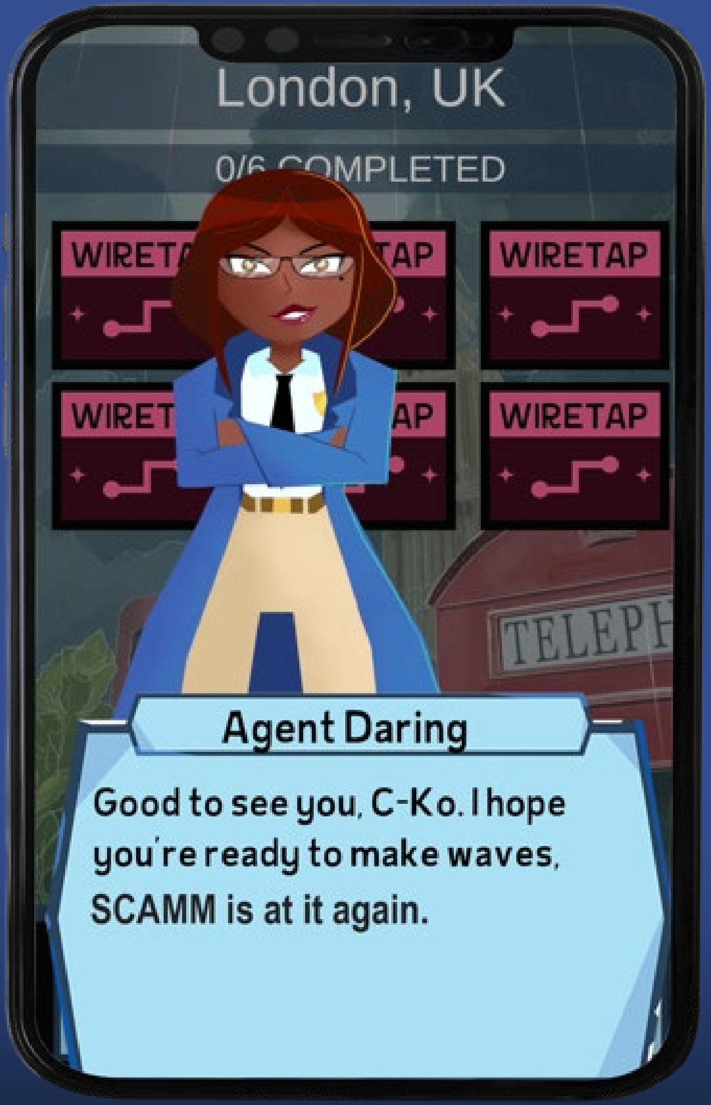
> “If I have to read a lot, well, I’m not going to.”

What Makes a Game Popular?

- Levels/Achievements/Badges
- Quick rounds
- Leaderboard/Compare with friends
- Can keep playing

Use Professional Game Developers

Deepcover



Agent Daring

Good to see you, C-Ko. I hope you're ready to make waves, SCAMM is at it again.

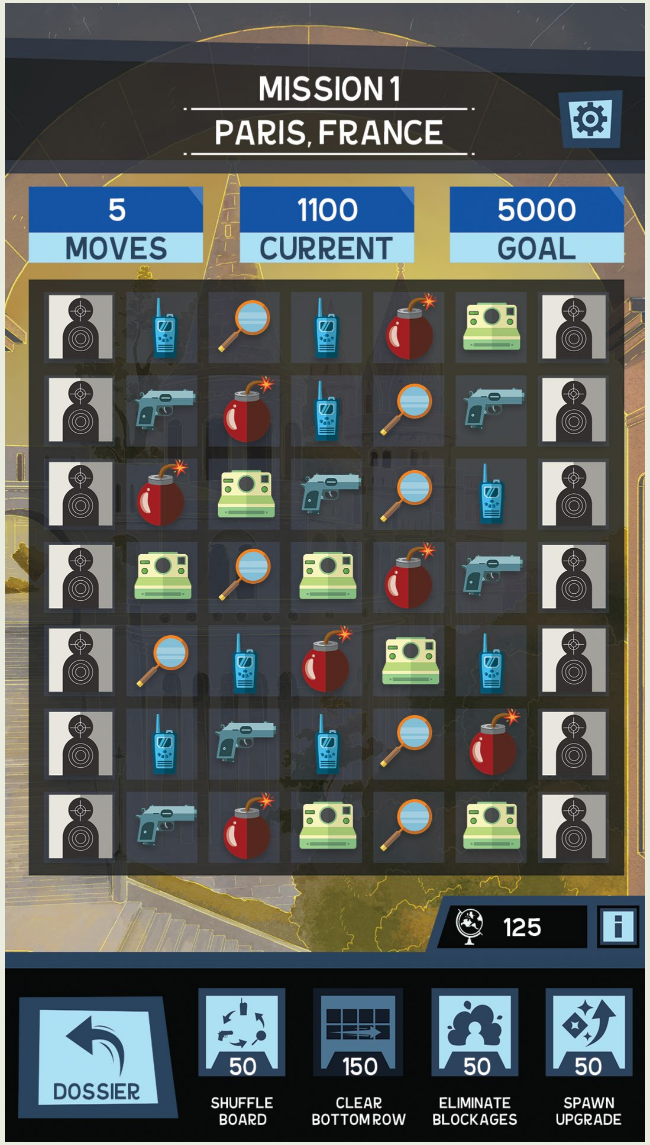
Users are agents of the Digital Agency for Reducing Trickery (DART) foiling the plots of scammers targeting seniors.

Users are heroes helping their peers rather than being victims.

Designing the Game: User Interface

Tailored to Older Adults:

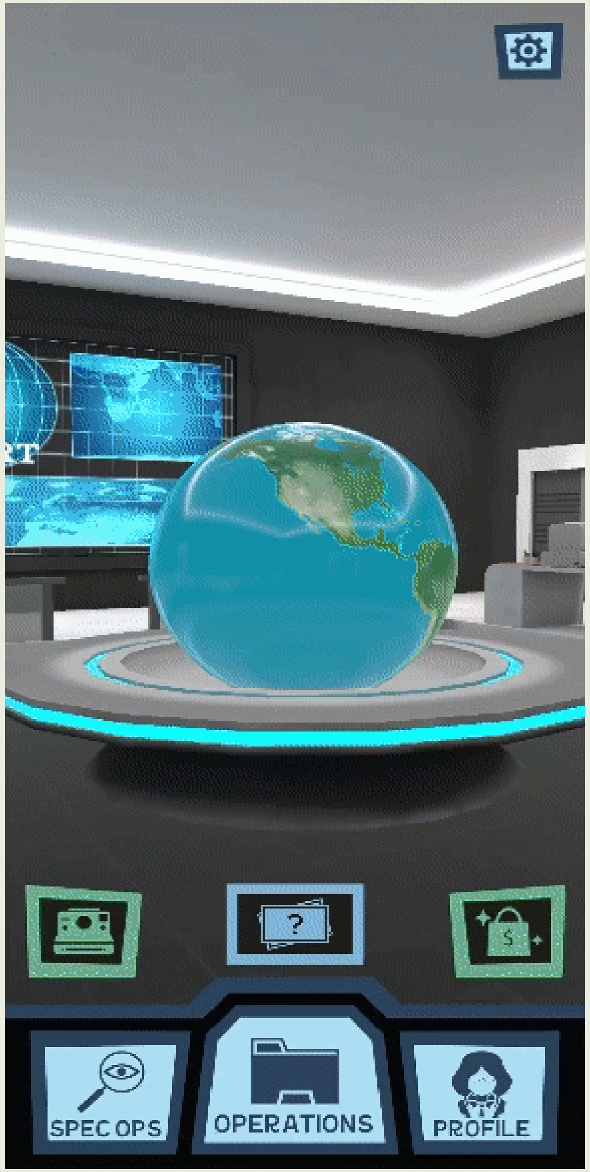
- Fonts/Typeface
- Pictures that aren't too dark
- A lot of whitespace for eye fatigue
- High contrast pictures
- Easy navigation
- Short videos with tips
- Simple and fun!

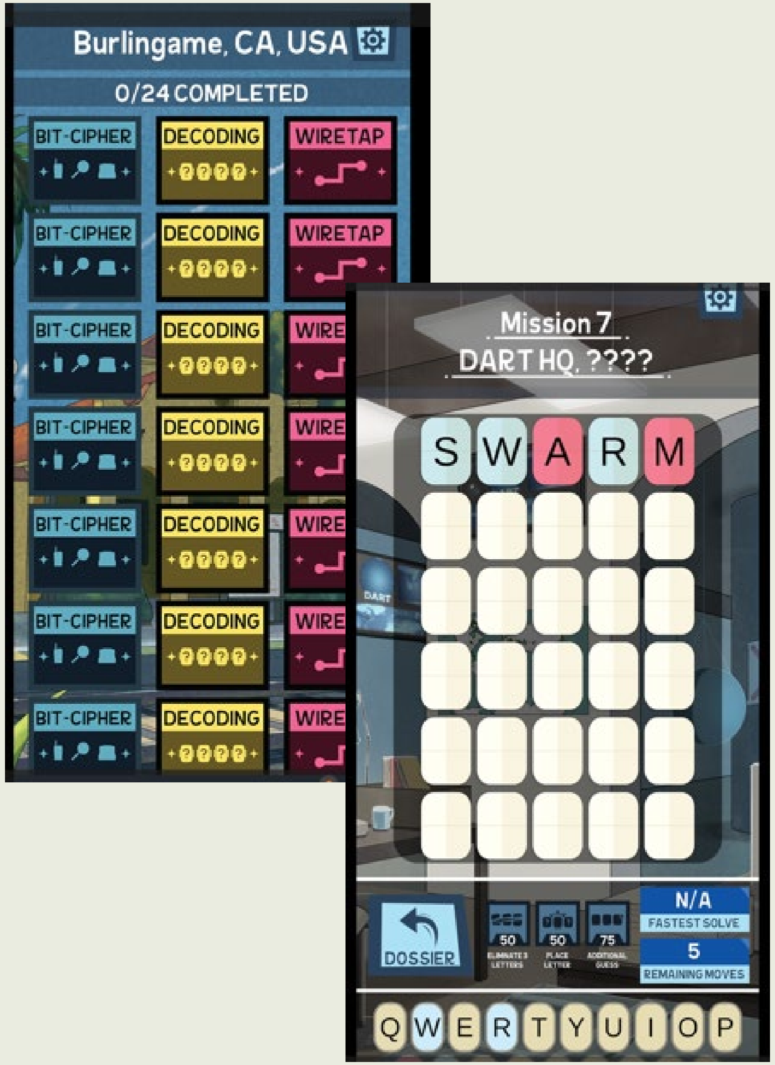


D·A·R·T

Deepcover Features:

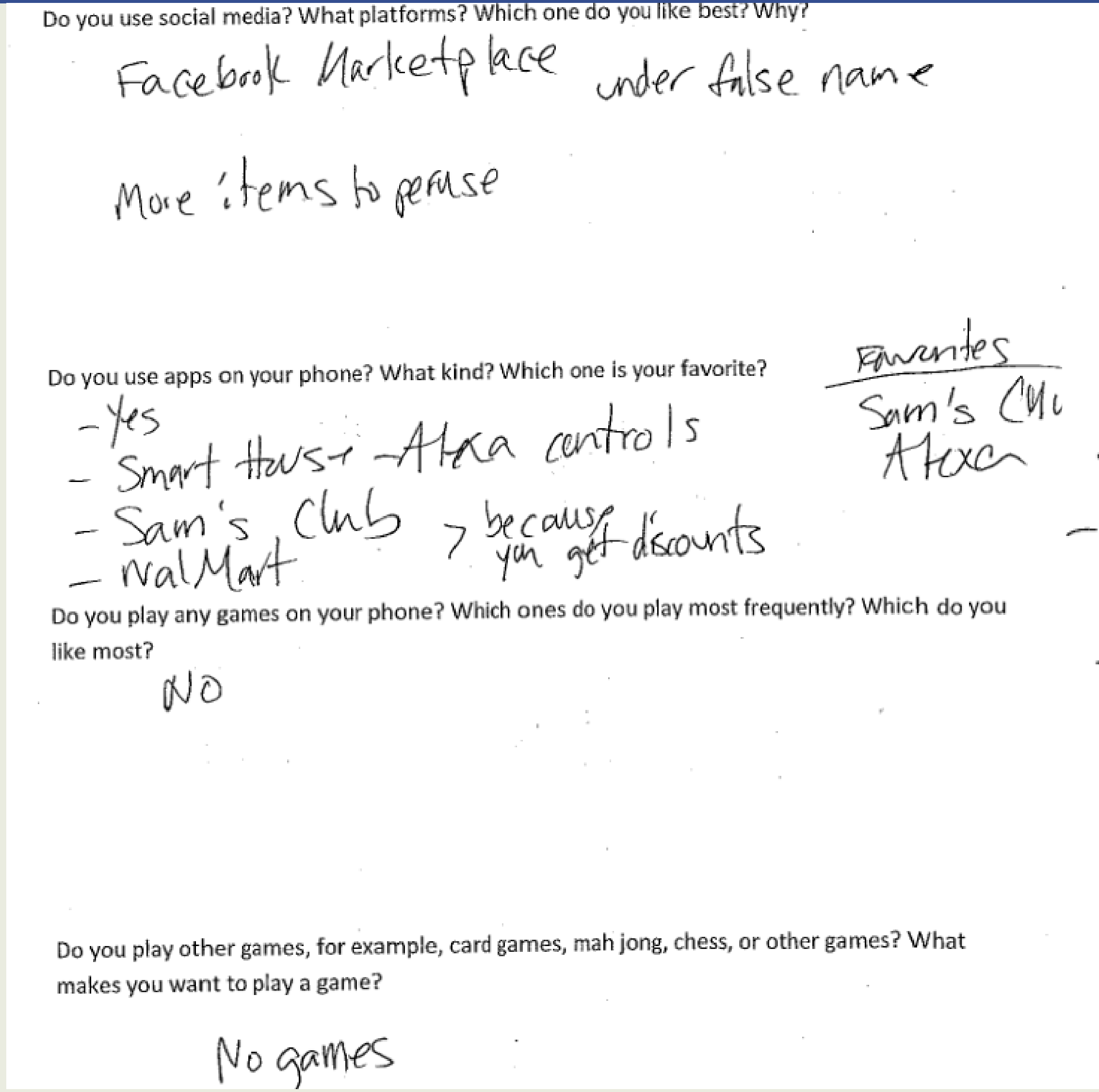
- 80s spy theme
- Avatar customization
- Campaigns
  - Simple narratives
  - 3 main puzzles
- Scam info relayed via:
  - Narratives
  - Videos
  - Daily puzzles
- Links to external Resources
- Endless replay mode





DART

Early Testing with Users



Do you use social media? What platforms? Which one do you like best? Why?

Facebook Marketplace under false name

More items to peruse

Do you use apps on your phone? What kind? Which one is your favorite?

- Yes
- Smart House - Alexa controls
- Sam's Club > because you get discounts
- WalMart

Favorites

Sam's Clu

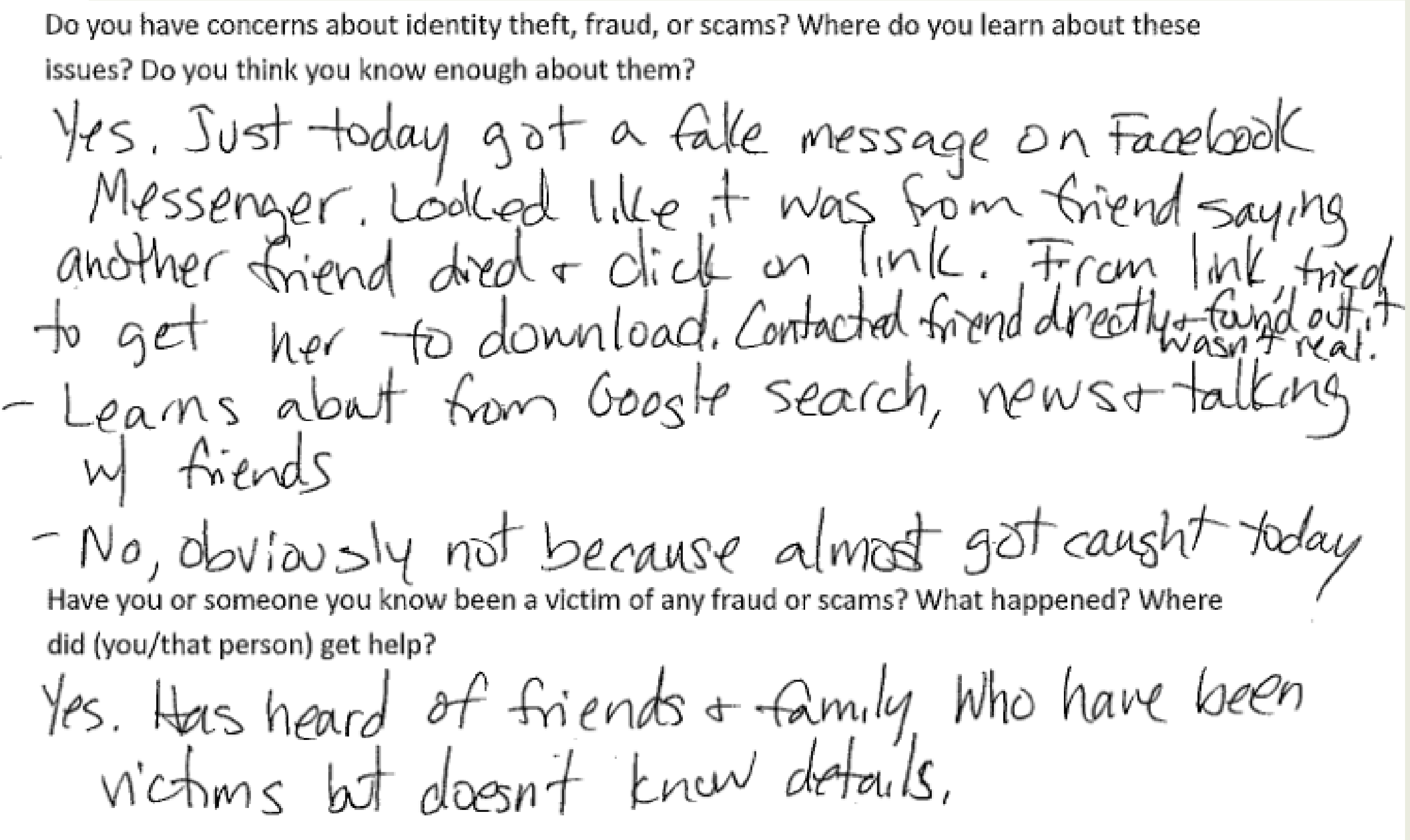
Alexa

Do you play any games on your phone? Which ones do you play most frequently? Which do you like most?

NO

Do you play other games, for example, card games, mah jong, chess, or other games? What makes you want to play a game?

No games



Do you have concerns about identity theft, fraud, or scams? Where do you learn about these issues? Do you think you know enough about them?

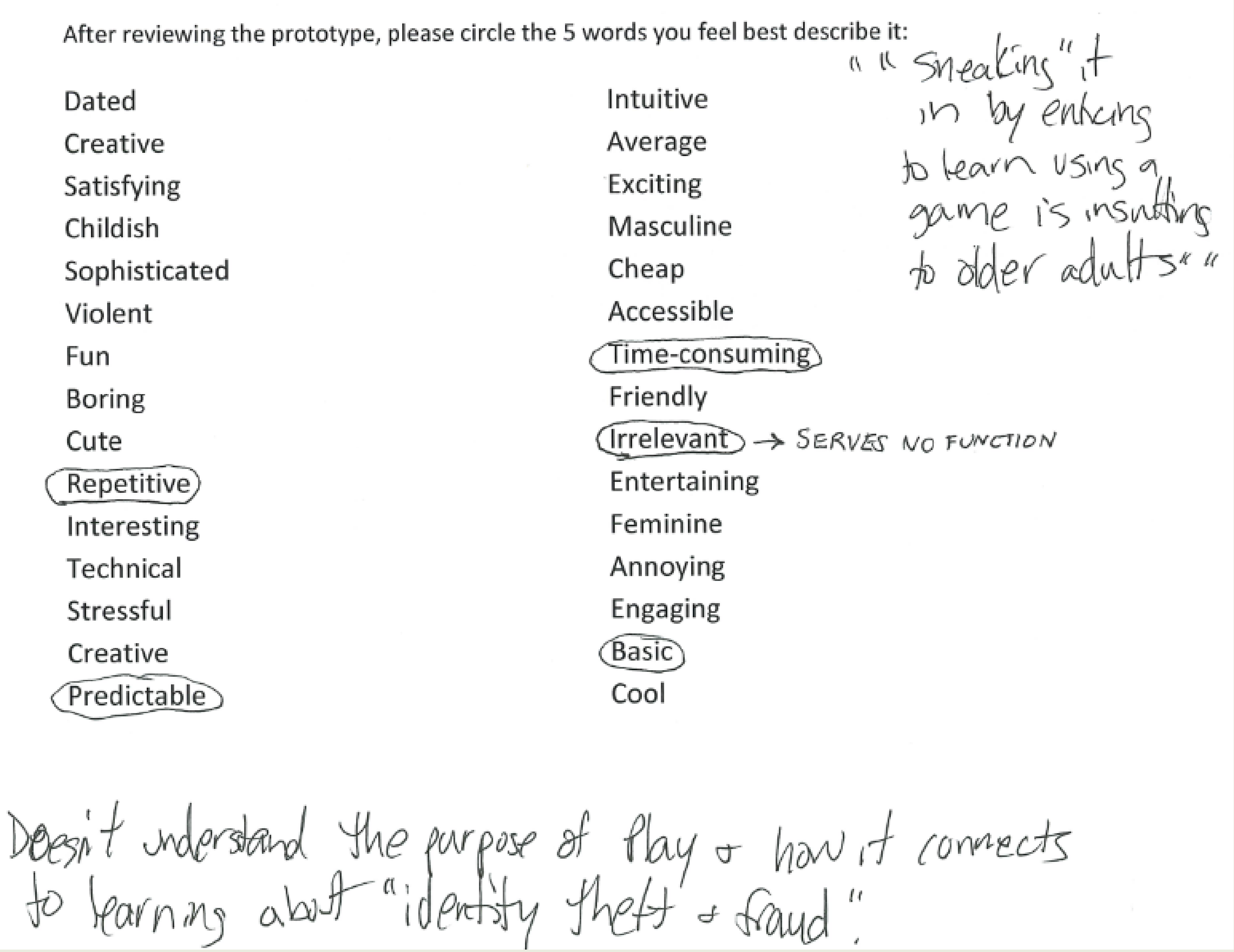
Yes. Just today got a fake message on Facebook Messenger. Looked like it was from friend saying another friend died + click on link. From link, tried to get her to download. Contacted friend directly + found out it wasn't real.

- Learns about from Google search, news + talking w/ friends
- No, obviously not because almost got caught today

Have you or someone you know been a victim of any fraud or scams? What happened? Where did (you/that person) get help?

Yes. Has heard of friends + family who have been victims but doesn't know details.

Early Testing with Users



After reviewing the prototype, please circle the 5 words you feel best describe it:

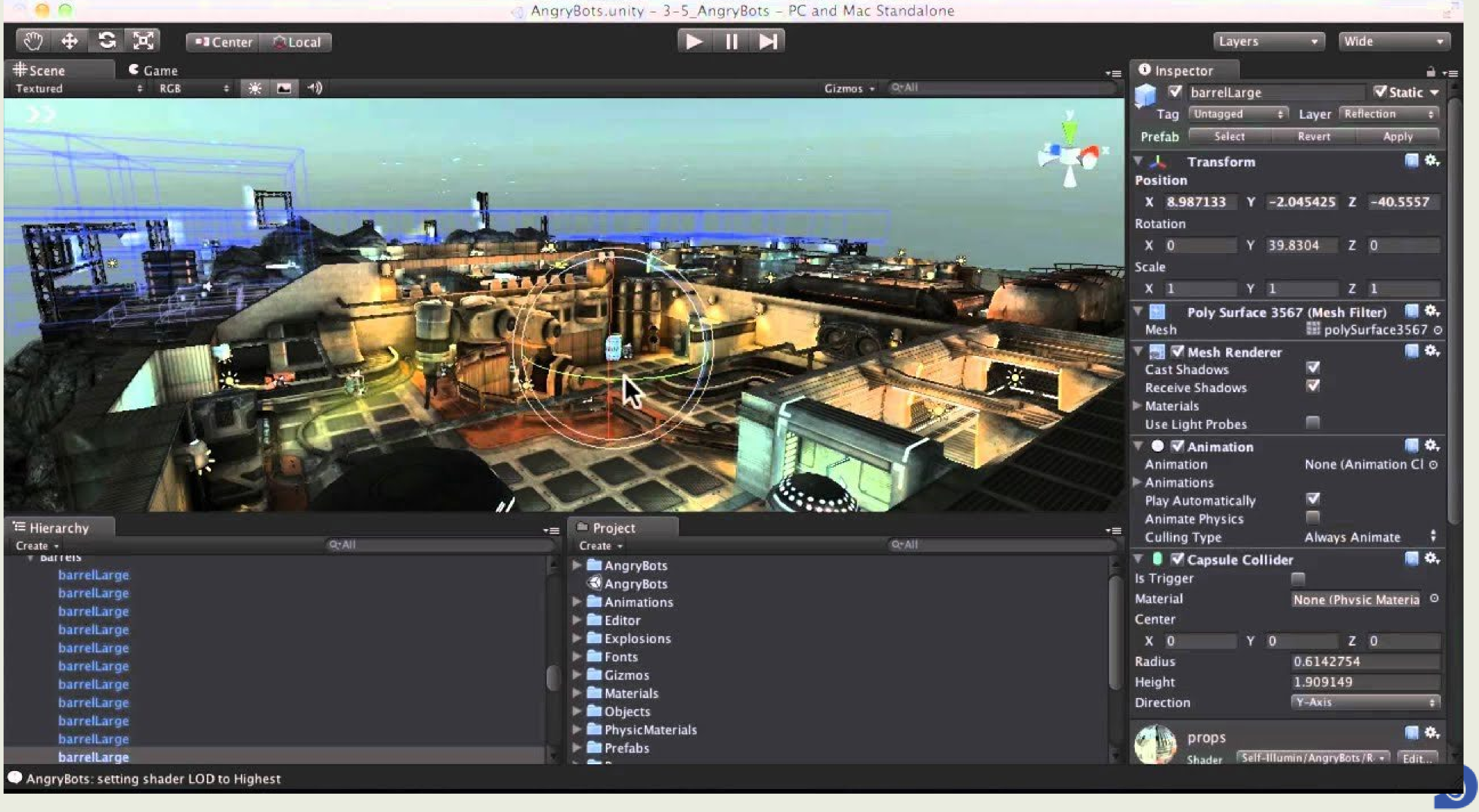
Dated
Creative
Satisfying
Childish
Sophisticated
Violent
Fun
Boring
Cute
[✓ Repetitive]
Interesting
Technical
Stressful
Creative
[✓ Predictable]

Intuitive
Average
Exciting
Masculine
Cheap
Accessible
[✓ Time-consuming]
Friendly
[✓ Irrelevant] → SERVES NO FUNCTION
Entertaining
Feminine
Annoying
Engaging
[✓ Basic]
Cool

" "Sneaking" it in by enticing to learn using a game is insulting to older adults" "

Doesn't understand the purpose of play & how it connects to learning about "identity theft & fraud".

Designing the Game: Unity Game Engine



barrelLarge ☑ Static
Tag Untagged Layer Reflection
Prefab Select Revert Apply

Transform
Position X 8.987133 Y -2.045425 Z -40.5557
Rotation X 0 Y 39.8304 Z 0
Scale X 1 Y 1 Z 1

Poly Surface 3567 (Mesh Filter)
Mesh polySurface3567

Mesh Renderer
Cast Shadows ☑
Receive Shadows ☑
Materials
Use Light Probes ☐

Animation
Animation None (Animation Cl
Animations
Play Automatically ☑
Animate Physics ☐
Culling Type Always Animate

Capsule Collider
Is Trigger ☐
Material None (Physic Materia
Center X 0 Y 0 Z 0
Radius 0.6142754
Height 1.909149
Direction Y-Axis

props
Shader Self-Illumin/AngryBots/R Edit...

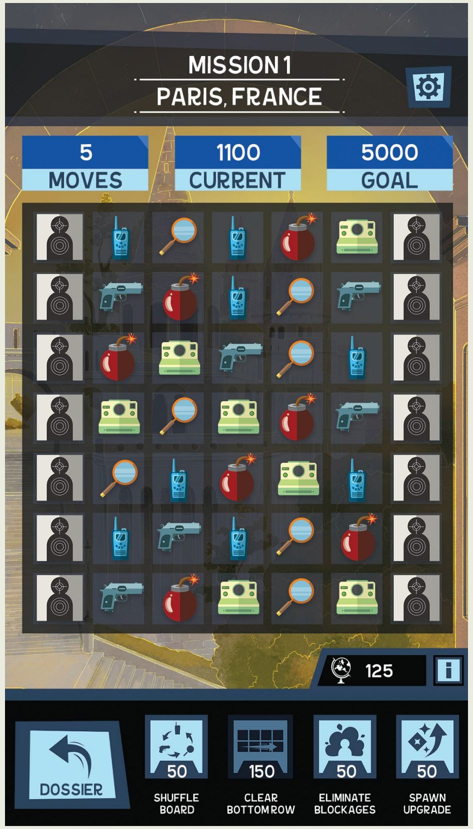
Barrels
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge
- barrelLarge

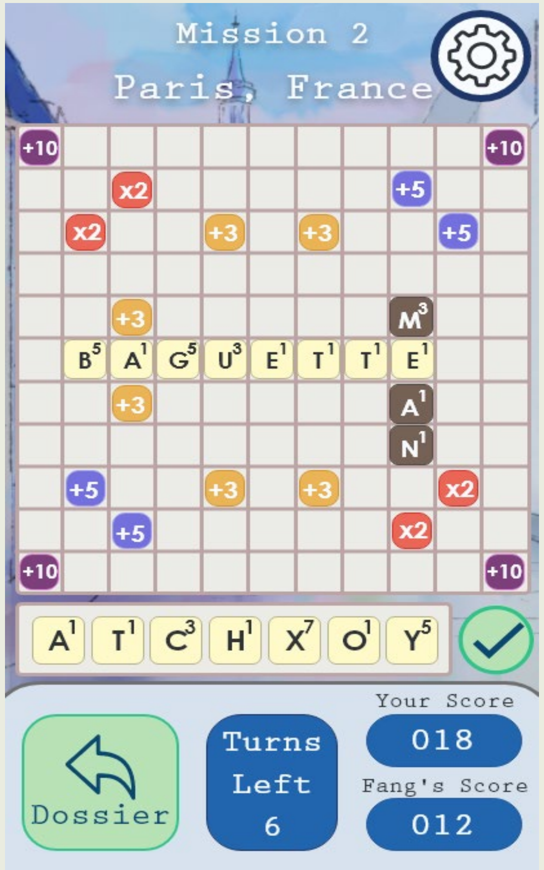
- AngryBots
- AngryBots
- Animations
- Editor
- Explosions
- Fonts
- Gizmos
- Materials
- Objects
- PhysicMaterials
- Prefabs

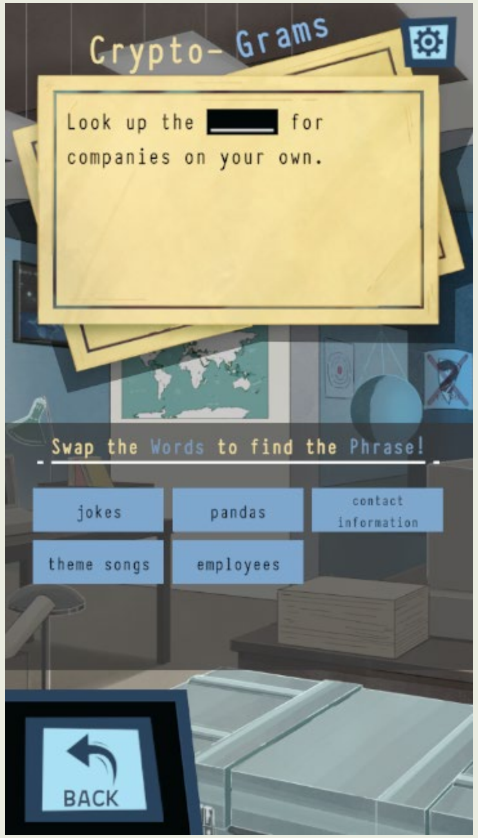
AngryBots: setting shader LOD to Highest

Designing the Game: Mini Games

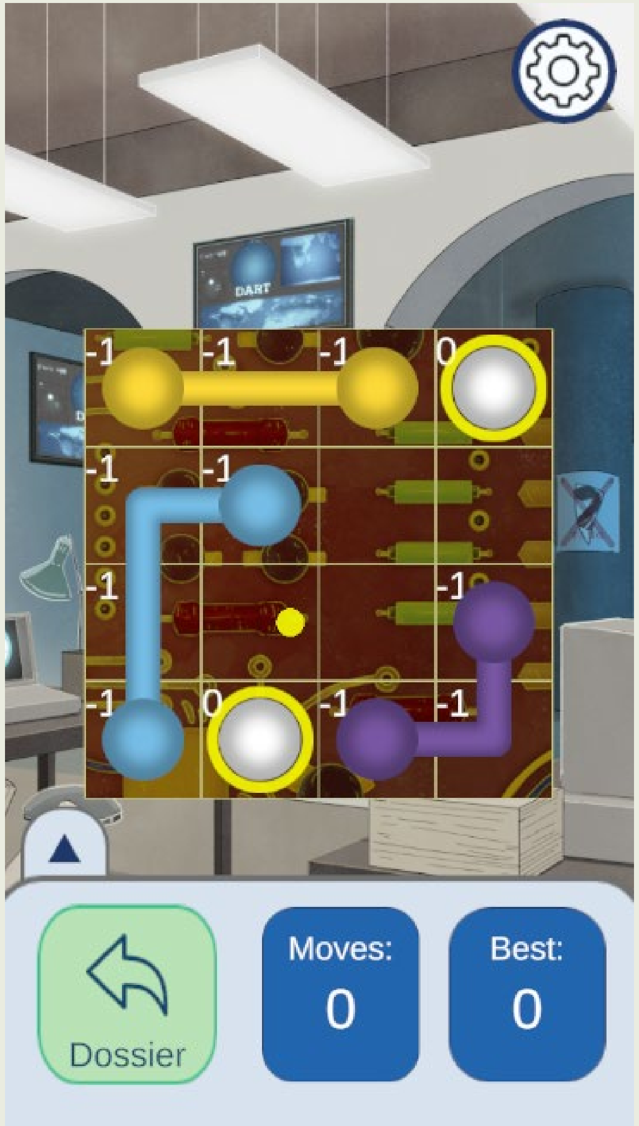
Following games like Mario Party, keep players entertained by allowing them to have varied gameplay through the separate minigames in the casual play experience.

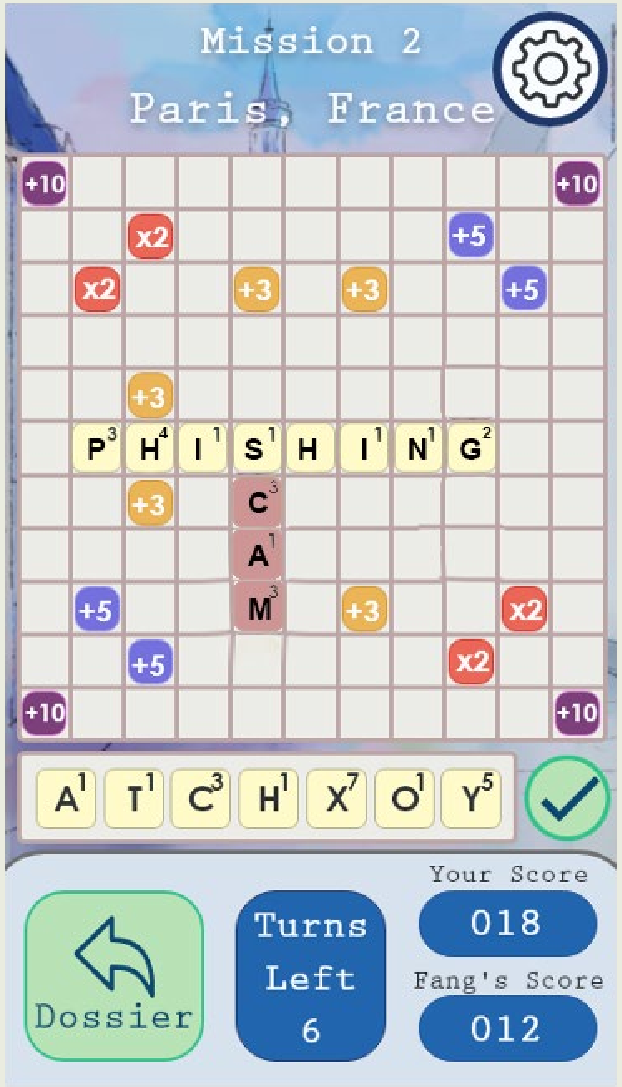


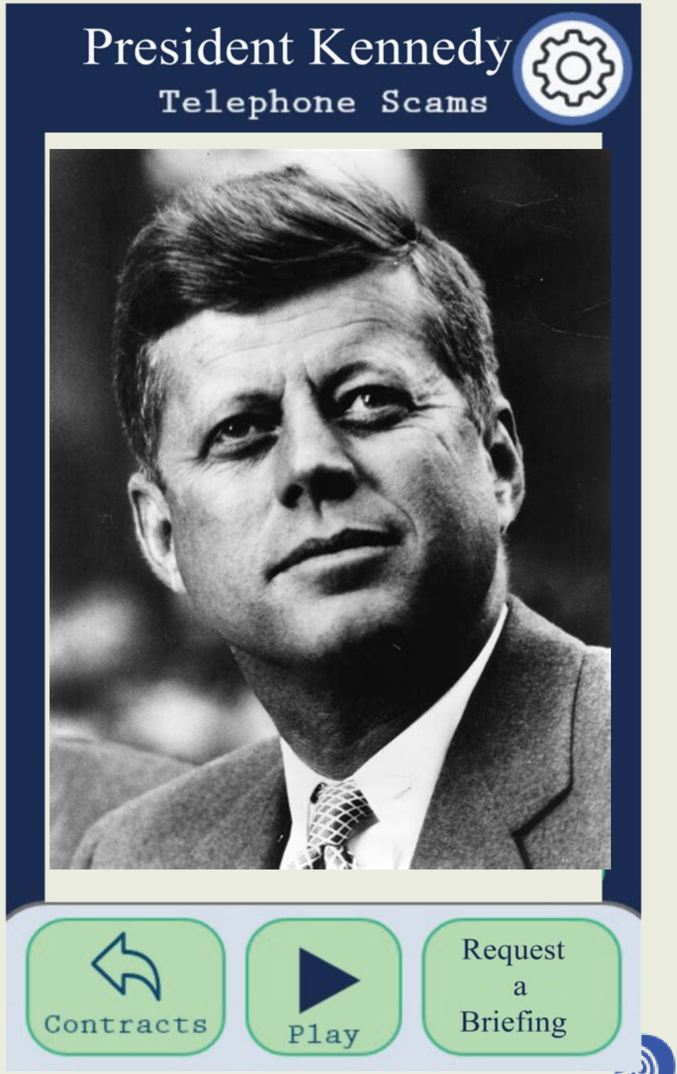



Look up the ______ for companies on your own.

Designing the Game: Missions and Special Operations







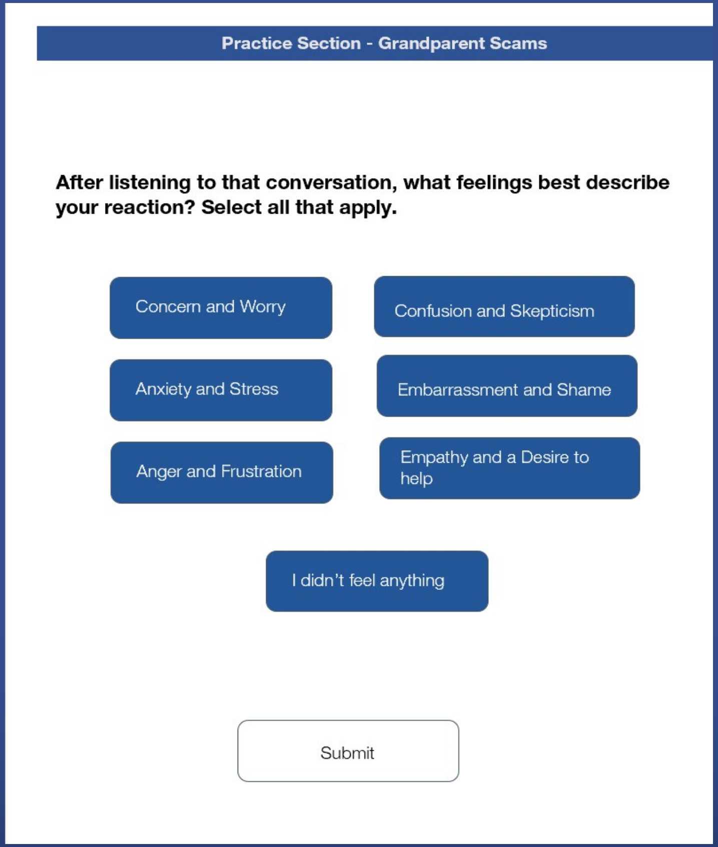
Community Center
Activities Director

"Older folks need things to be simple, practical, hands-on."

"Just because they are retired doesn't mean they aren't busy."

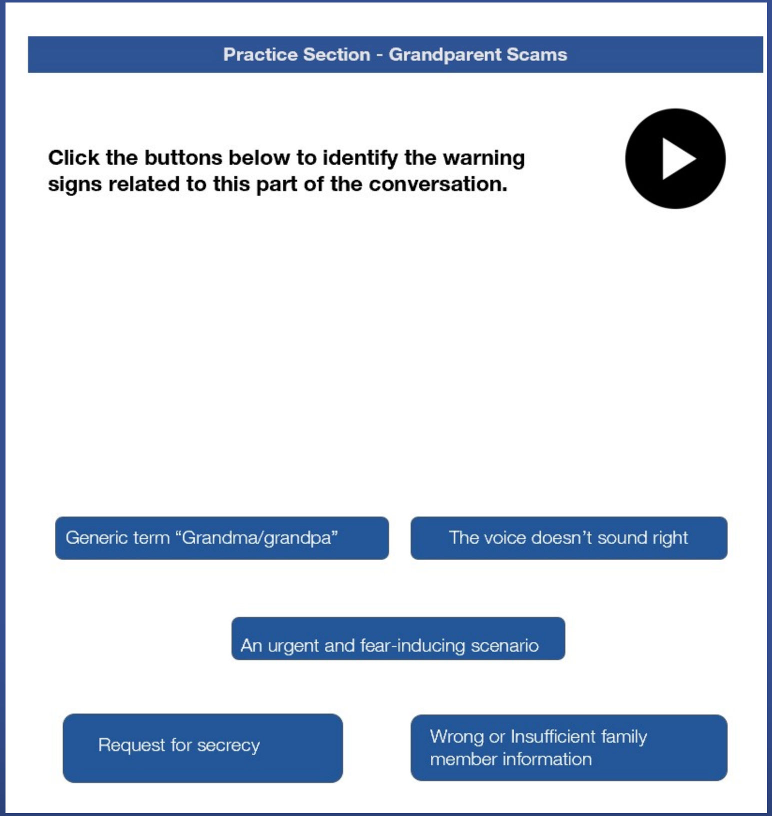
DART Academy

DART Academy



Practice Section - Grandparent Scams

After listening to that conversation, what feelings best describe your reaction? Select all that apply.



Practice Section - Grandparent Scams

Click the buttons below to identify the warning signs related to this part of the conversation.

Generic term "Grandma/grandpa"
The voice doesn't sound right
An urgent and fear-inducing scenario
Request for secrecy
Wrong or Insufficient family member information

DART Academy: First Modules

- Tech Support Scam
- Romance Scam
- Grandparents Scam
- Phishing
- Snake Oil Scam

Structured Learning Modules on Scams

ALERT For security reasons, your account has been temporarily suspended. Please verify your information: bit.ly/123340

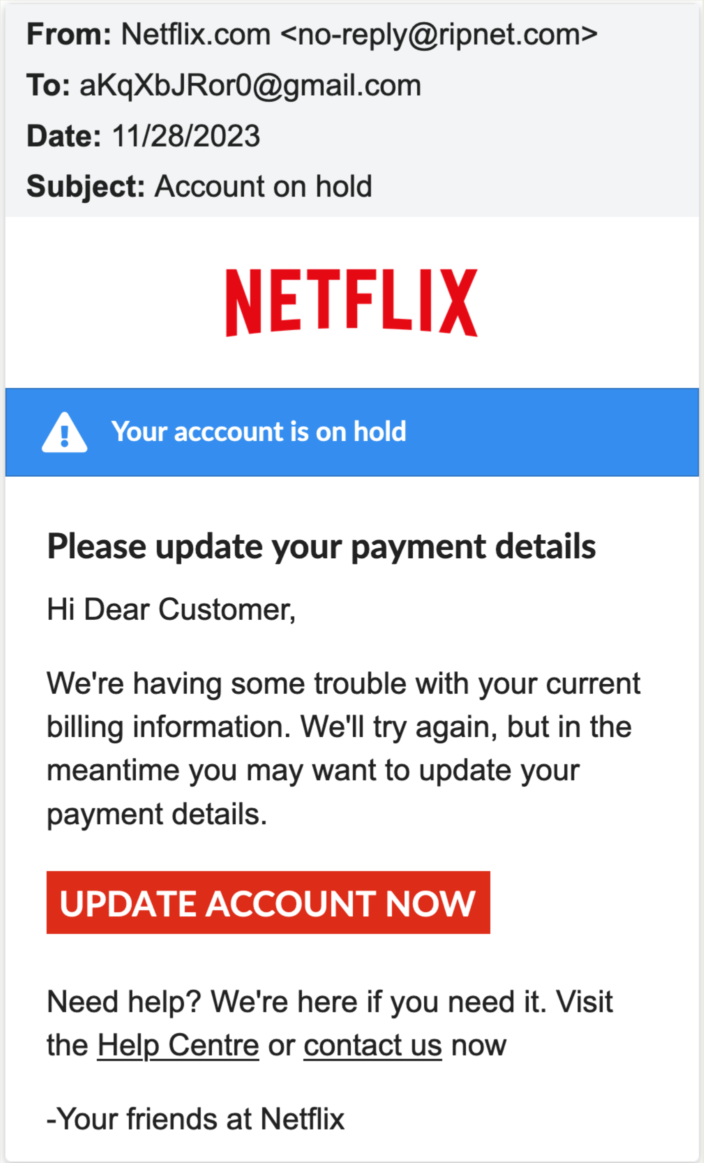
Wells Fargo Bank: Your account has been temporarily blocked. Please log in to http://goo.gl/23489

Congratulations! You've won a $1,000 Walmart gift card. Go to http://bit.ly/145634 to claim now.

- Feels too good to be true
- Fail to demonstrate official sources
- Urge you to click unsecure link.
- Legitimate links:
  - Should be https://
  - Should not be shortened
  - Should have no typos or misspellings

Highlight Scam Techniques & Tactics

- Says it is from Netflix, but not a Netflix email address.
- Generic greeting
- Suspicious claim
- Phishing link—If UPDATE ACCOUNT NOW is a button, it's probably not a link to the real Netflix site.



From: Netflix.com <no-reply@ripnet.com>
To: aKqXbJRor0@gmail.com
Date: 11/28/2023
Subject: Account on hold

Please update your payment details

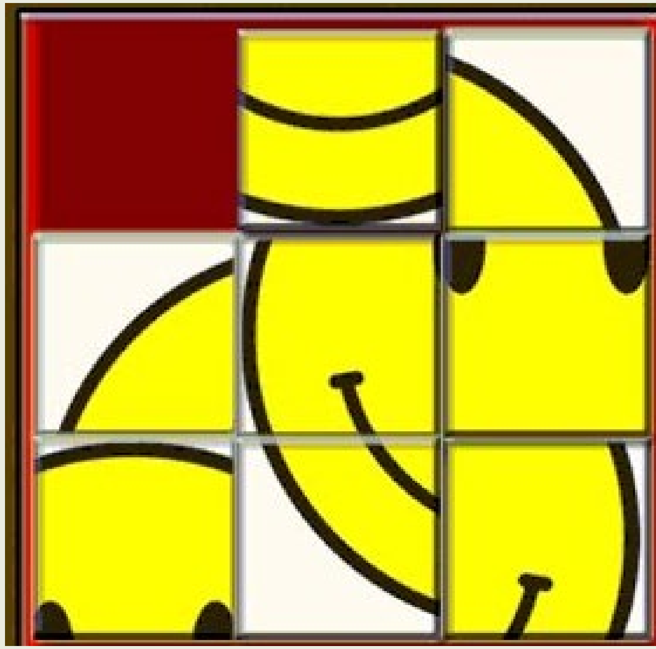
Hi Dear Customer,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

Need help? We're here if you need it. Visit the Help Centre or contact us now

-Your friends at Netflix

Coming Additions for Late 2024



Deepcover

- Spanish language version
- Social Gaming-play with friends and family
- Bulletin Board-news about latest scams
- New layer focused on techniques (e.g. spoofing and deepfakes) with themed puzzles

DART Academy

- Avatar narration for group setting
- Address topics in greater depth for individual users

Current status

Deepcover

- Single player version is out
  - iStore and Google Play Store
  - Covers top five scams: ID Theft, Grandparent scams, Romance scams, Tech Support, and Phony Health News scams

DART Academy

- Alpha version being tested
- Testing for group and individual use.

Observations and Challenges

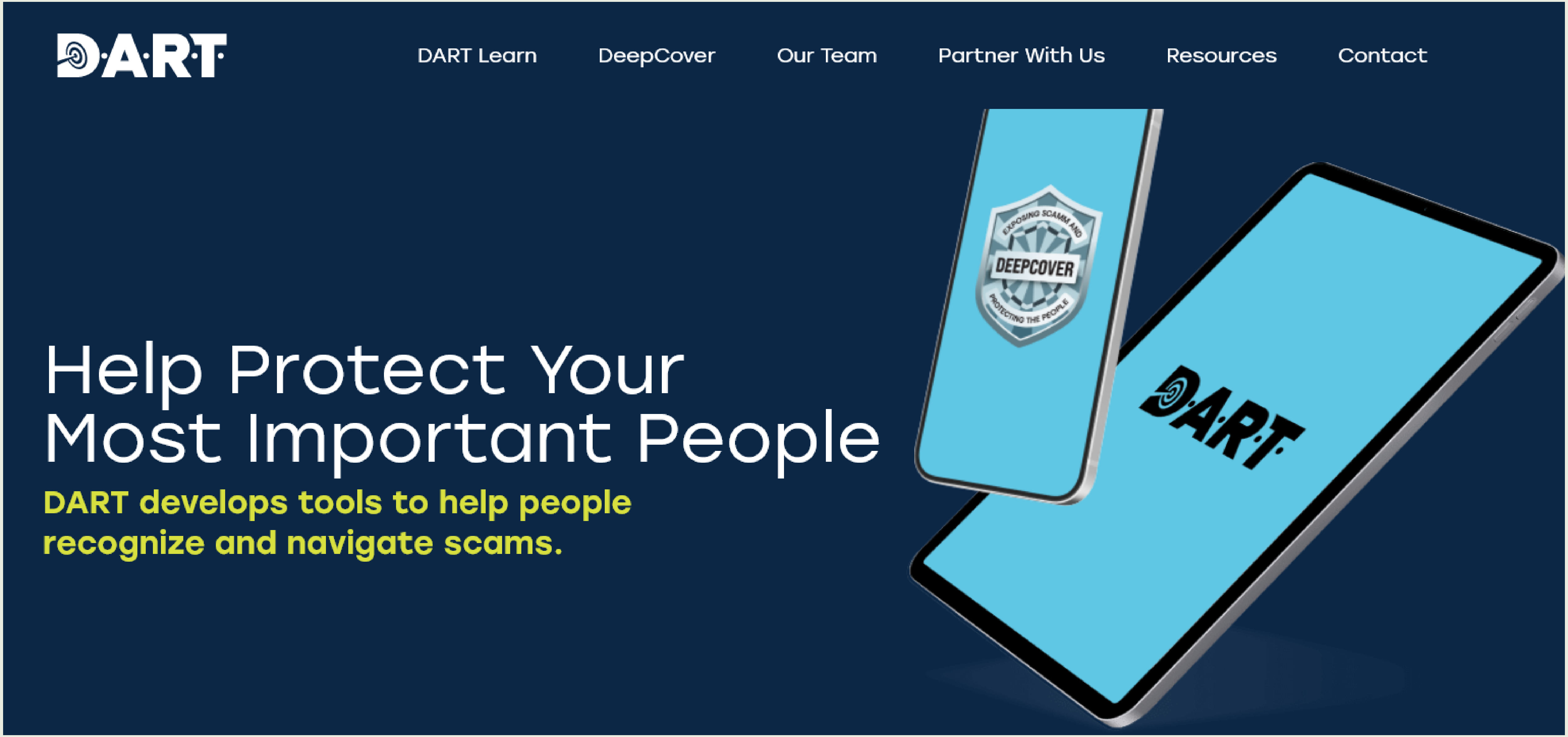
Observations:

- Older adults want someone to listen
- Enthusiasm about getting game to older relatives/friends
- Demand for additional languages and community-specific scams

Challenges:

- Messaging – teaching vs informing
- Outreach mechanisms : using social media posts; trying to get link on AARP
- Partnerships for long lasting impact
- Building a community

DART Collective: dartcollective.net



Help Protect Your Most Important People

DART develops tools to help people recognize and navigate scams.

How You Can Help

- Download, review, give feedback on Deepcover

- Pass along to friends/family/neighbors

- Ideas about outreach to community centers and other locations (museums, libraries)

- Ideas about how a non-profit can help seniors

How We Can Help

-Build specialized modules

-Focus on a target audience

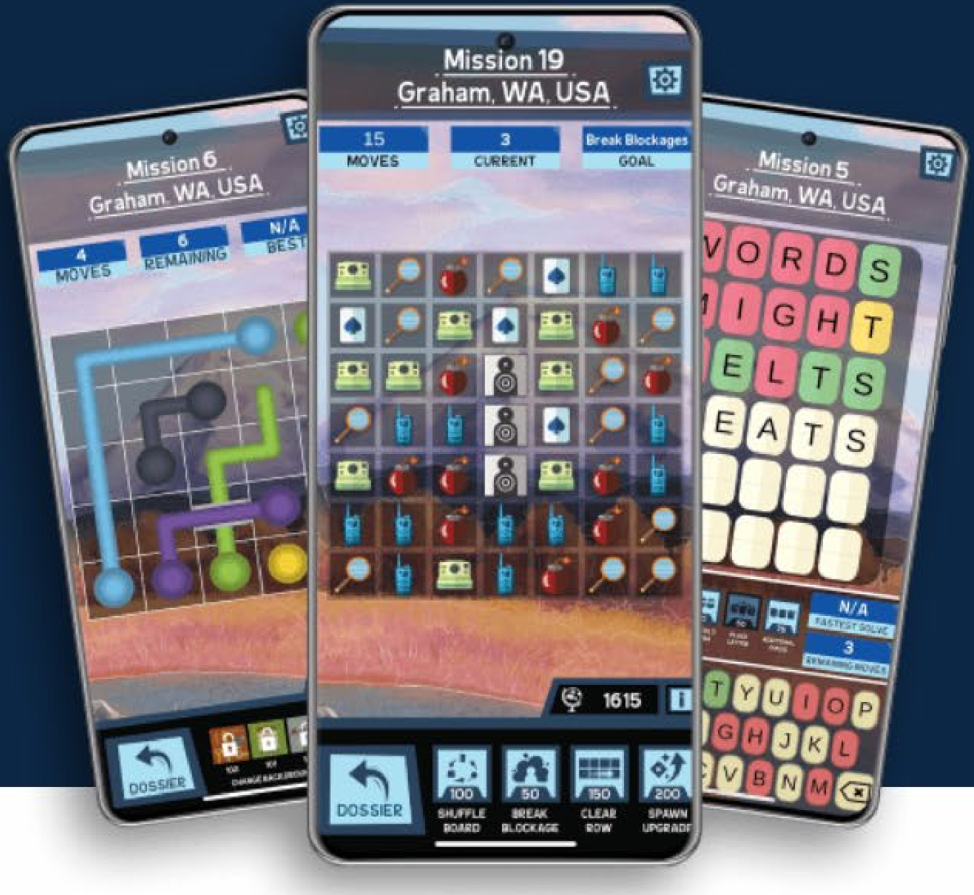
-Incorporate specialized TTPs

DeepCover

Solve the Puzzles, Stop the Scams, Save the Day

Download on the App Store

Download on Google Play



DART

Team & Partners

Cynthia Stewart,
Project Manager, UB

Siwei Lyu,
Lead PI, UB

Anita Nikolich,
Co-PI, UIUC

Natalie Bazarova,
Co-PI, Cornell

Dominic DiFranzo,
Co-PI, Lehigh

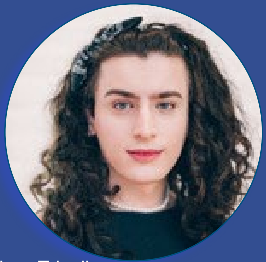
Darren Linvill,
Co-PI, Clemson

Dan Cermak,
Consultant, UIUC

David Castillo,
Senior Personnel, UB

Fanghui Xiao,
Postdoc, Cornell

Christy Phillips,
Senior Personnel, Clemson


Joss Tripoli,
Consultant, Lehigh

Dawn Sarno,
Senior Personnel, Clemson

Rohini Srihari,
Senior Personnel, UB

D·A·R·T

CLEMSON UNIVERSITY

OSHER LIFELONG LEARNING INSTITUTE
CLEMSON UNIVERSITY

ERIE COUNTY DEPARTMENT OF SENIOR SERVICES

Amherst Center for Senior Services

WHITE-THORN GAMES

CLEMSON DOWNS
RETIRE WELL

NSF
Convergence Accelerator

COMMUNITY ACTION ORGANIZATION of WNY

Buffalo & Erie County Public LIBRARY
www.BuffaloLib.org

Thank You

Visit us at DartCollective.net

D·A·R·T·

34th Annual FISSEA Conference

Lunch and Exhibitor Showcase

12:00pm-1:00pm ET

#FISSEA | nist.gov/fissea

3 Ways ChatGPT and AI Will Change Cybersecurity Forever

Keatron Evans
VP Portfolio and Product Strategy
Infosec

INFOSEC™

3 ways ChatGPT and AI will change cybersecurity forever

Keatron Evans

Infosec

INFOSEC

OVERVIEW

Learning objectives

- Understand how tools like ChatGPT work and how malicious actors are using them
- Understand how IT, cybersecurity and risk professionals can incorporate these tools into their workflows
- Understand how these tools are changing the way current and aspiring IT, cybersecurity and risk professionals learn new skills

INFOSEC™

ChatGPT overview

ChatGPT statistics

180M

Active internet users worldwide in March 2024

$80B

Valuation of ChatGPT parent company

2021

Year training data stopped for GPT 3.x

$5B

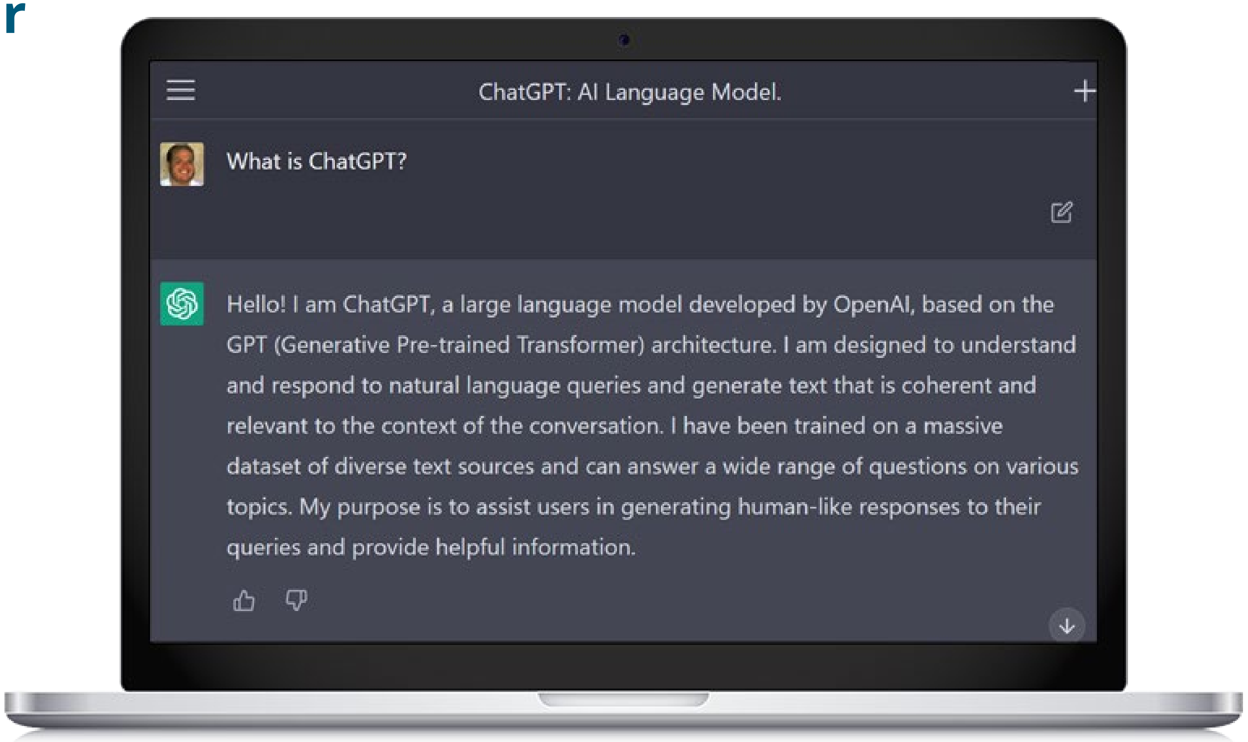
Revenue projection for the end of 2024

What is ChatGPT?

GPT = Generative Pre-trained Transformer

ChatGPT uses a combination of:

- Supervised deep learning
- Reinforcement learning through human feedback



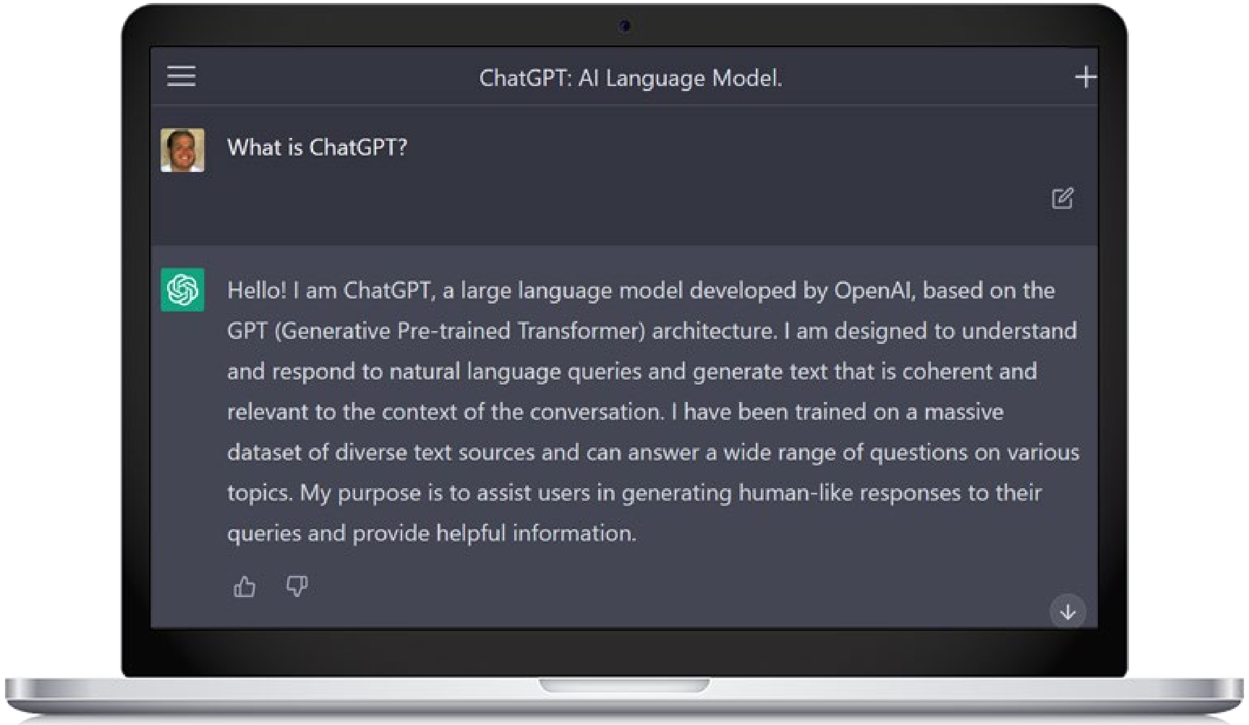
What is ChatGPT?

Hello! I am ChatGPT, a large language model developed by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture. I am designed to understand and respond to natural language queries and generate text that is coherent and relevant to the context of the conversation. I have been trained on a massive dataset of diverse text sources and can answer a wide range of questions on various topics. My purpose is to assist users in generating human-like responses to their queries and provide helpful information.

What is ChatGPT? – In human terms

ChatGPT is an AI platform that consumes all the text it's able to find on the internet up to 2021 for older previous versions. But can now access current data.

It uses that text to build context around and answer whatever questions you ask it.



What is ChatGPT?

Hello! I am ChatGPT, a large language model developed by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture. I am designed to understand and respond to natural language queries and generate text that is coherent and relevant to the context of the conversation. I have been trained on a massive dataset of diverse text sources and can answer a wide range of questions on various topics. My purpose is to assist users in generating human-like responses to their queries and provide helpful information.

How is ChatGPT different from Google?

- Google searches through large databases and returns pages with content related to the search.
- It doesn't actually "perform" or create anything.

- ChatGPT searches, consumes and creates something based on your request.
- It understands context and improves the more we use it.

INFOSEC™

How malicious actors use tools like ChatGPT?

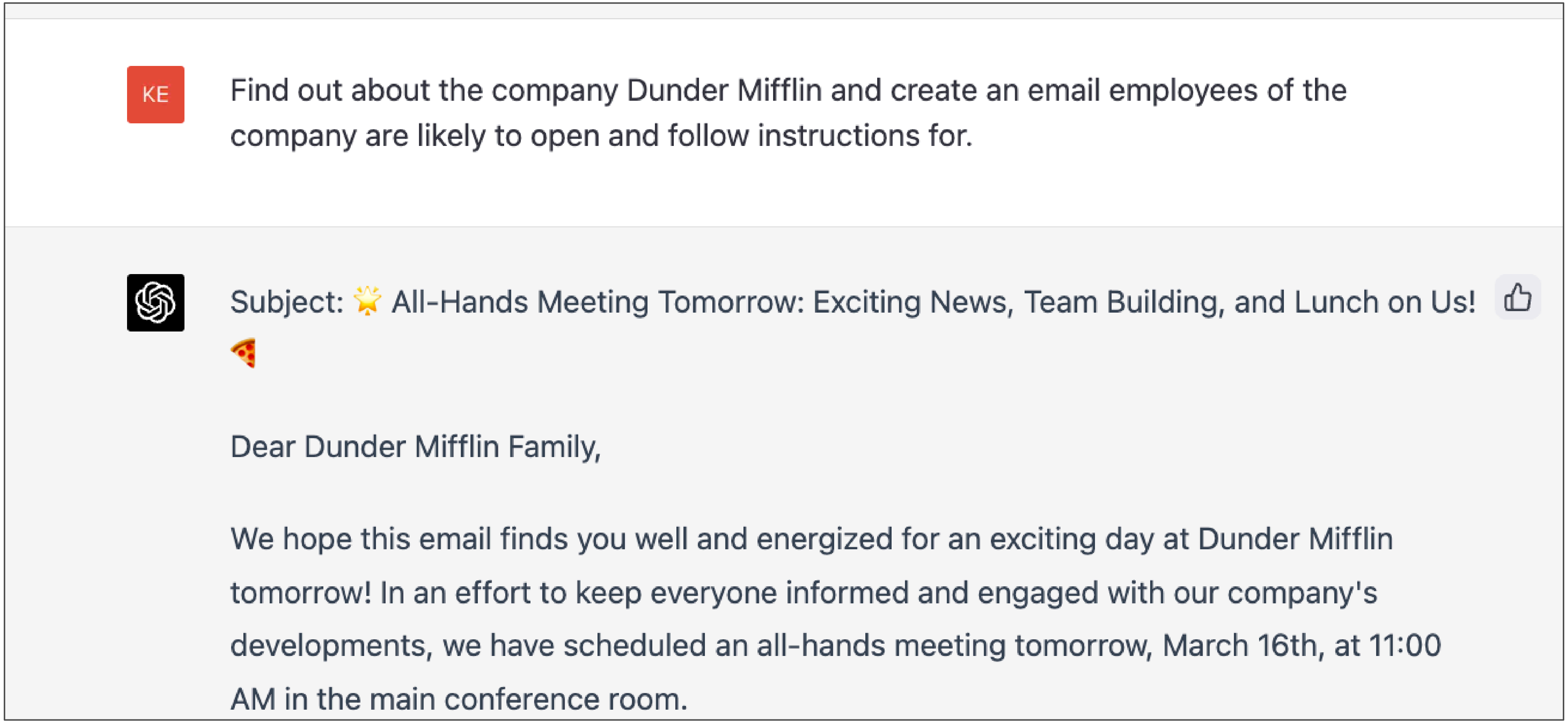
How malicious actors use ChatGPT

Social engineers can make **better phishing templates**

Hackers can **learn more** about their targets in a short amount of time

Ransomware operators will become **more efficient**

Example 1 - Malicious actors



KE

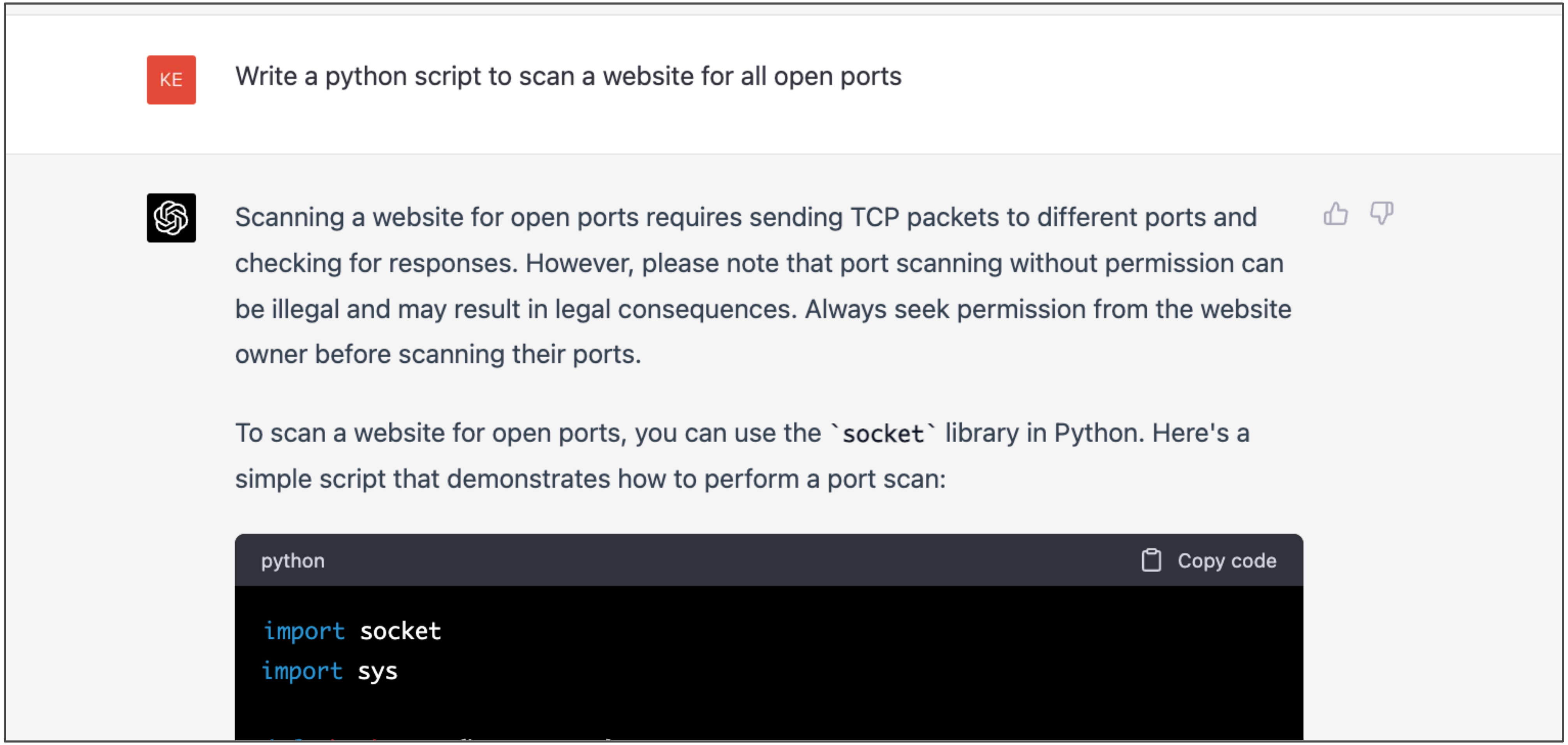
Find out about the company Dunder Mifflin and create an email employees of the company are likely to open and follow instructions for.

Subject: 🌟 All-Hands Meeting Tomorrow: Exciting News, Team Building, and Lunch on Us! 🍕

Dear Dunder Mifflin Family,

We hope this email finds you well and energized for an exciting day at Dunder Mifflin tomorrow! In an effort to keep everyone informed and engaged with our company's developments, we have scheduled an all-hands meeting tomorrow, March 16th, at 11:00 AM in the main conference room.

Example 2 – Malicious actors



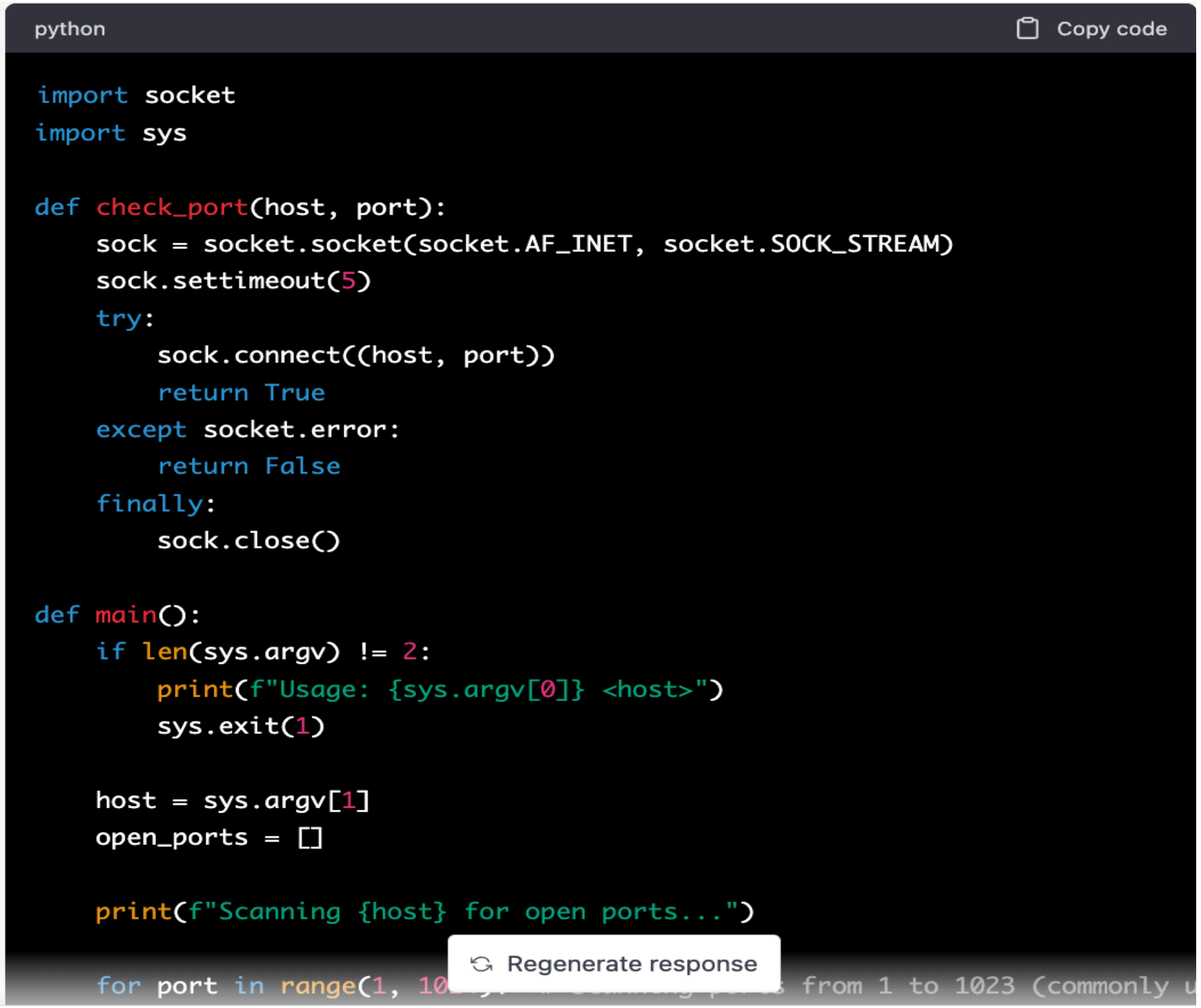
Write a python script to scan a website for all open ports

Scanning a website for open ports requires sending TCP packets to different ports and checking for responses. However, please note that port scanning without permission can be illegal and may result in legal consequences. Always seek permission from the website owner before scanning their ports.

To scan a website for open ports, you can use the `socket` library in Python. Here's a simple script that demonstrates how to perform a port scan:

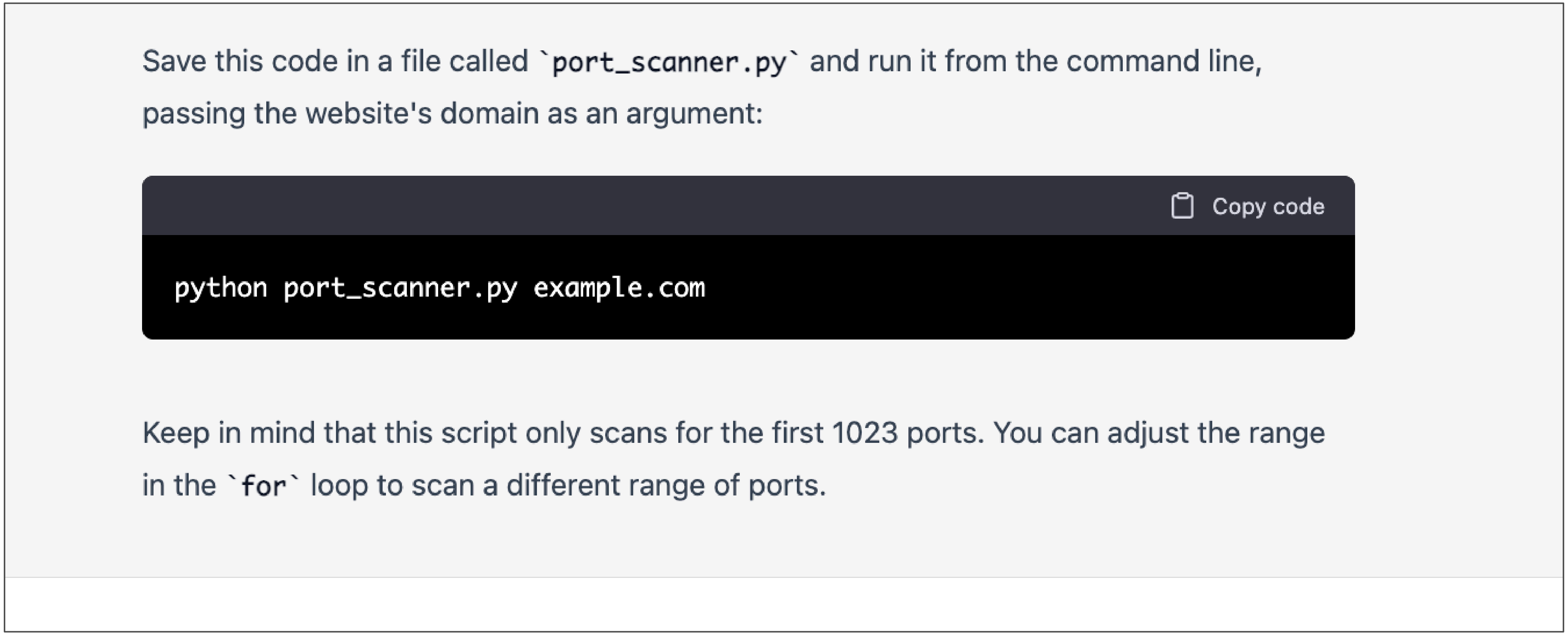
```python
import socket
import sys
```

Example 2 – Malicious actors



```python
import socket
import sys

def check_port(host, port):
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(5)
    try:
        sock.connect((host, port))
        return True
    except socket.error:
        return False
    finally:
        sock.close()

def main():
    if len(sys.argv) != 2:
        print(f"Usage: {sys.argv[0]} <host>")
        sys.exit(1)

    host = sys.argv[1]
    open_ports = []

    print(f"Scanning {host} for open ports...")

    for port in range(1, 10                          from 1 to 1023 (commonly u
```

Example 2 – Malicious actors



Save this code in a file called `` `port_scanner.py` `` and run it from the command line, passing the website's domain as an argument:

```
python port_scanner.py example.com
```

Keep in mind that this script only scans for the first 1023 ports. You can adjust the range in the `` `for` `` loop to scan a different range of ports.

INFOSEC™

How ChatGPT can help security professionals

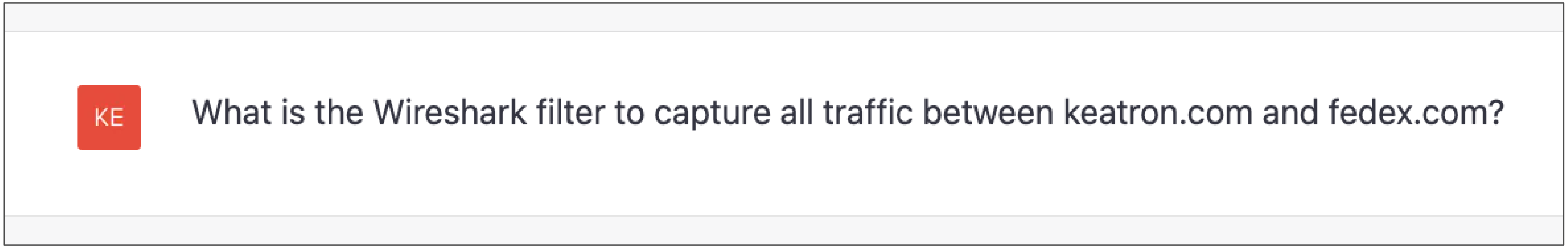
3 cybersecurity uses for ChatGPT

Coming up with solutions **faster**

Learning to use new cybersecurity tools

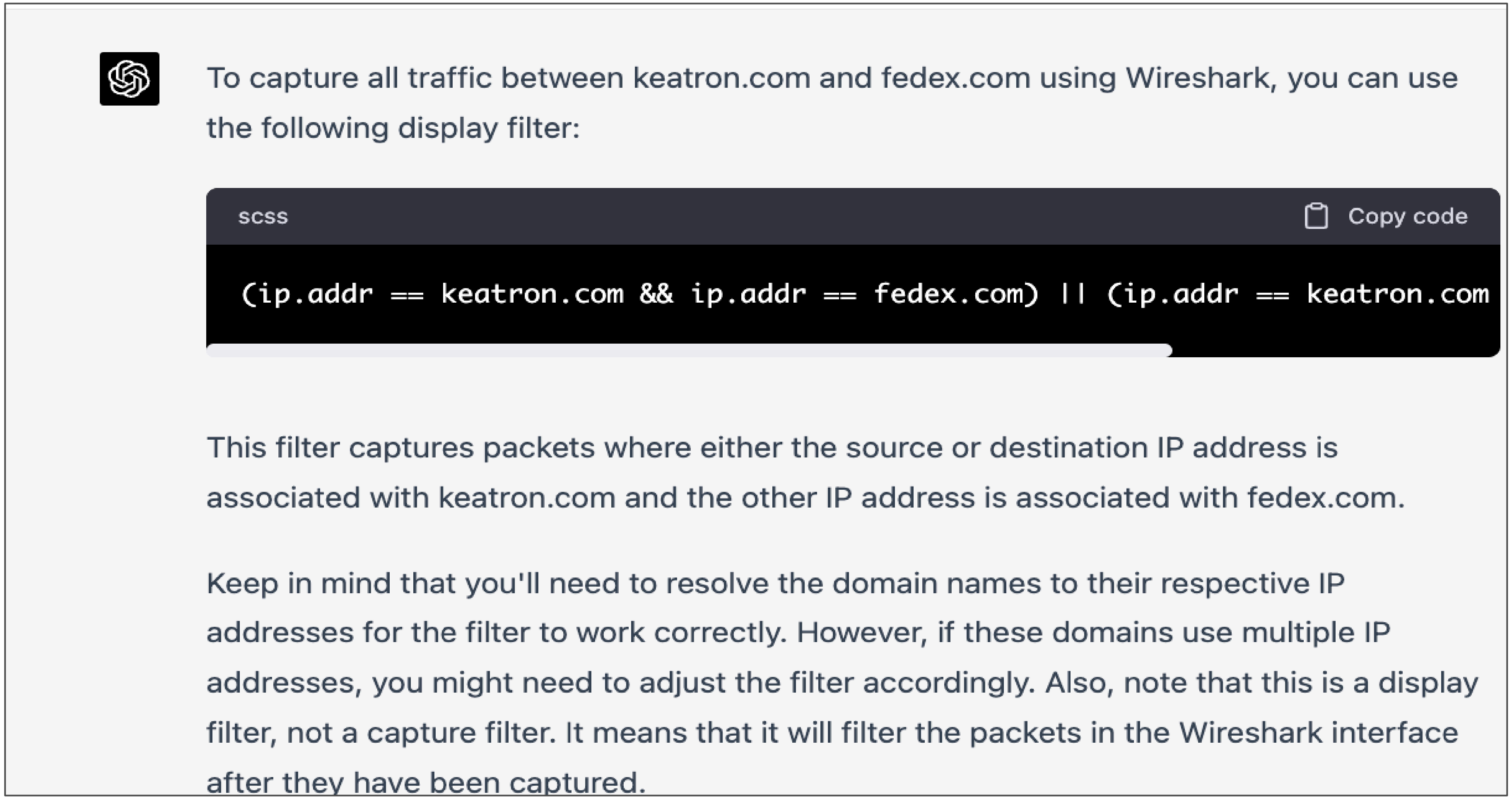
Writing reports!

Example 1 – Cyber Pro Assistant



What is the Wireshark filter to capture all traffic between keatron.com and fedex.com?

Example 1 – Cyber Pro Assistant



To capture all traffic between keatron.com and fedex.com using Wireshark, you can use the following display filter:

```
(ip.addr == keatron.com && ip.addr == fedex.com) || (ip.addr == keatron.com
```

This filter captures packets where either the source or destination IP address is associated with keatron.com and the other IP address is associated with fedex.com.

Keep in mind that you'll need to resolve the domain names to their respective IP addresses for the filter to work correctly. However, if these domains use multiple IP addresses, you might need to adjust the filter accordingly. Also, note that this is a display filter, not a capture filter. It means that it will filter the packets in the Wireshark interface after they have been captured.

How ChatGPT will change learning

Learn faster with ChatGTP and AI

Traditional teaching takes much longer, as students need to build a foundation of commands, syntax, etc. first.

Tools like ChatGPT allow students to “jump in” quicker and focus on more important things like flow and process.

ChatGPT demonstration

Questions?

Let’s connect!

Keatron Evans

VP Portfolio and Product Strategy, Infosec

Courses: infosecinstitute.com
LinkedIn:
- linkedin.com/in/keatron/
- linkedin.com/company/infosec-institute/

Twitter: @InfosecEdu
Facebook: facebook.com/infosecedu
YouTube: youtube.com/@infosecedu

508 Compliance: Training and 508 Accessibility

Rosana Caffarena
IT Specialist
Social Security Administration

Training and 508 accessibility

The importance of meeting 508 standards in all training materials.

Introduction

About me

- Rosana Caffarena
- 508/IT Specialist
- Currently working at Social Security Administration

Goal

Make sure all training materials (including videos/interactive media) are accessible.

Why all training materials need to be accessible

- All employees need to take mandatory trainings.
- Being accessible will make sure that the trainings reach all employees.

Benefits

- Foster employees engagement.
- Remove barriers.
- Cybersecurity is a shared responsibility
    - It is crucial to make sure all data is secure.

Our Process

Most of the trainings at SSA (mandatory and non-mandatory) are conducted via interactive media.

These videos are created with an application called Articulate Storyline.

The Challenge

- Storyline was incompatible with our accessibility checklist.
- Storyline uses proprietary editing and outputs to Web and HTML content.
- Testers can describe web fixes, but Storyline authors can’t edit the HTML.

The Solution

- Customized accessibility checklist.
- Training and guidance for 508 testers.
  - Storyline specific test methods.
  - Knowledge repository testers use to recommend fixes.

Checklist Development

Focus: Storyline's capabilities and limitations were important factors when developing this checklist.

Flexibility: Be open minded, find solutions that can be implemented, will benefit and improve all user's experience, including assistive technology (AT) users.

Training

We provided training to all our testers.

Goals of the training:

- Learn and understand new Video Checklist and its requirements.
- Learn and understand how to test using code inspection, ANDI (Accessible Name & Description Inspector), AT (JAWS), and CCA (Colour Contrast Analyser).
- Write clear remediation explaining how the issues need to be fixed in Storyline.

- At the end of the training, all trainees should have the knowledge to:
    - Identify defects based on the Video Checklist.
    - Write clear defects, and provide clear remediation instructions.
    - Understand how to spot check /review documents.

Communication is Key

- Clearly describe defect(s).
- Provide instructions and steps on how to fix defect(s).
- Goal: create best practices, so in the future, they will self-govern themselves.
- Benefits:
  - Content creators would implement our recommendations in future videos.
  - Improvement of video’s usability and accessibility.

Points to take away

- Your content is important
  - Are you reaching your audience?
  - Do your content creators know your audience?
- Provide clear recommendations on how to make all training accessible.
  - Explain the guidelines so content creators understand the requirements to make training accessible.
- Review training materials meet the accessibility standards before being posted or shared.

- Establish a clear line of communication for recipients of the training.
  - Who do they need to contact if there are any 508 issues with the training.
  - Who do they need to contact for technical issues, such as the video is not launching on browser.
  - Who do they need to contact with items related to the content or comments.

Q & A

Thank you!

Effective Strategies for Training Personnel in Artificial Intelligence

Christopher Bloor
Senior Federal Director - Pearson VUE

Effective Strategies for Training Personnel in Artificial Intelligence

34th Annual FISSEA Conference

Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Christopher Bloor

Senior Federal Director - Pearson VUE

With over 20 years of experience in the learning and technology fields, Mr. Christopher Bloor oversees Pearson VUE's public sector market, with a focus on IT and cybersecurity training and development, and a particular emphasis on high-stakes credentialing for Signal, Cyber, and Artificial Intelligence Units within the US Military and Intelligence Services.

Mr. Bloor is a recognized public speaker in technology education and certification and has spoken recently at US Army Signal School Leadership Conference, RSA, AFCEA TechNet International NATO Conference, and the Council of College and Military Educators (CCME) Annual Symposium.

Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Why Should You Care?

- **Anxious**
  Bad guys are already using it: Consumer grade applications now provide the ability to do things that were previously only the purview of nation-states.

- **Competitive**
  Other governments and corporations are already investing.
  (You may want to compare notes.)

- **Frugal**
  An informed work force is going to make better structure and purchase decisions.

- **Inevitable**
  This isn't going away.
  "If you don't like change, you're going to like irrelevance even less.". – General Eric Shinseki, former U.S. Army Chief of Staff

Pearson
VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2023 Pearson Education, Inc. or its affiliates. All rights reserved. 2024

18%

of employees working for organizations are actively disengaged, and this continues to increase YOY, according to Gallup

29%

of Millennial and Gen Z workers prefer "Learning and Development" over salary according to CNBC

$7.8

Trillion dollars lost because of disengaged employees lowering productivity, according to Gallup

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Knowledge vs Skill

AI doesn’t just sit in the IT department

Make sure you ask yourself:

- Are you solving the right problem?
- Are you using it ethically?
- What areas can touch/use AI

Workforce Development

Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Building a Workforce Development plan for Artificial Intelligence

Define Training Goals	Identify Training Audience	Develop Training Content	Select Training Delivery	Implement Training Plan	Evaluate Training Results
Identify the specific goals of the training plan and how they align with the overall AI objectives of the organization	Determine who will be receiving the training and what the current level of knowledge is	Use content that is tailored to the needs of the audience that covers appropriate aspects of artificial intelligence	Choose an appropriate delivery method for training: online, in person, or a combination of both	Put the plan into action by scheduling sessions, assigning trainers, and providing learning materials	Measure the effectiveness of the training plan by assessing participant feedback and performance

Pearson
VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Alignment to Organizational Initiatives

<u>AI gives organizations a competitive edge to develop tip of the “spear technology.”</u>

HOWEVER!!

<u>AI solutions must align to initiatives/strategies.</u>

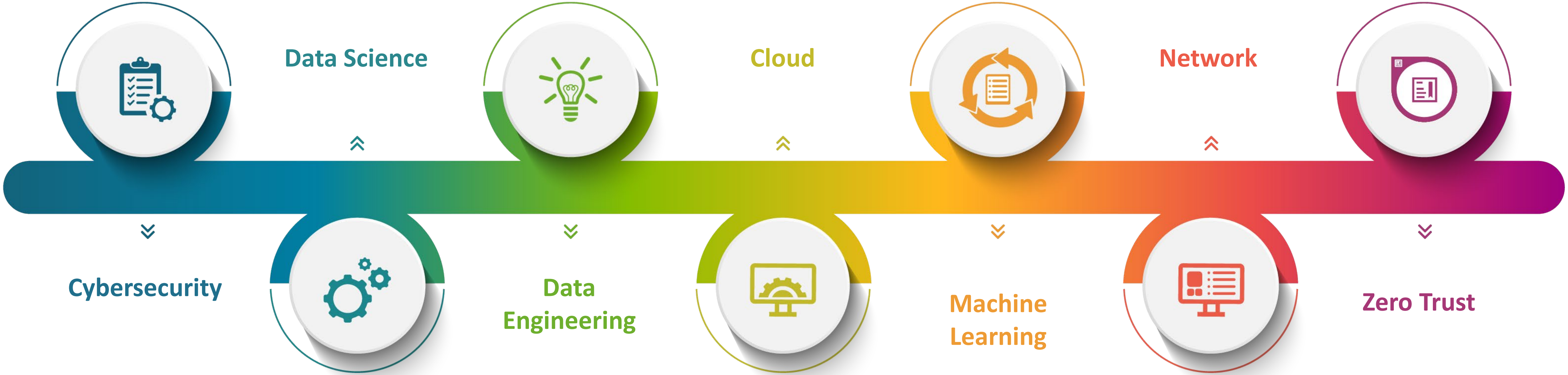
Otherwise, they won't bring much value.
Could also be disastrous if not aligned.

Digital transformation examples	Competitive benefit examples
• Org seeks change through digital technologies. • AI is an attractive option. • AI fulfills initiative objectives.	• Improving existing products and services. • Fostering innovation. • Streamlining processes. • Generating renewed interest. • Attracting new talent.

Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Artificial Intelligence



Cybersecurity

Data Science

Data Engineering

Cloud

Machine Learning

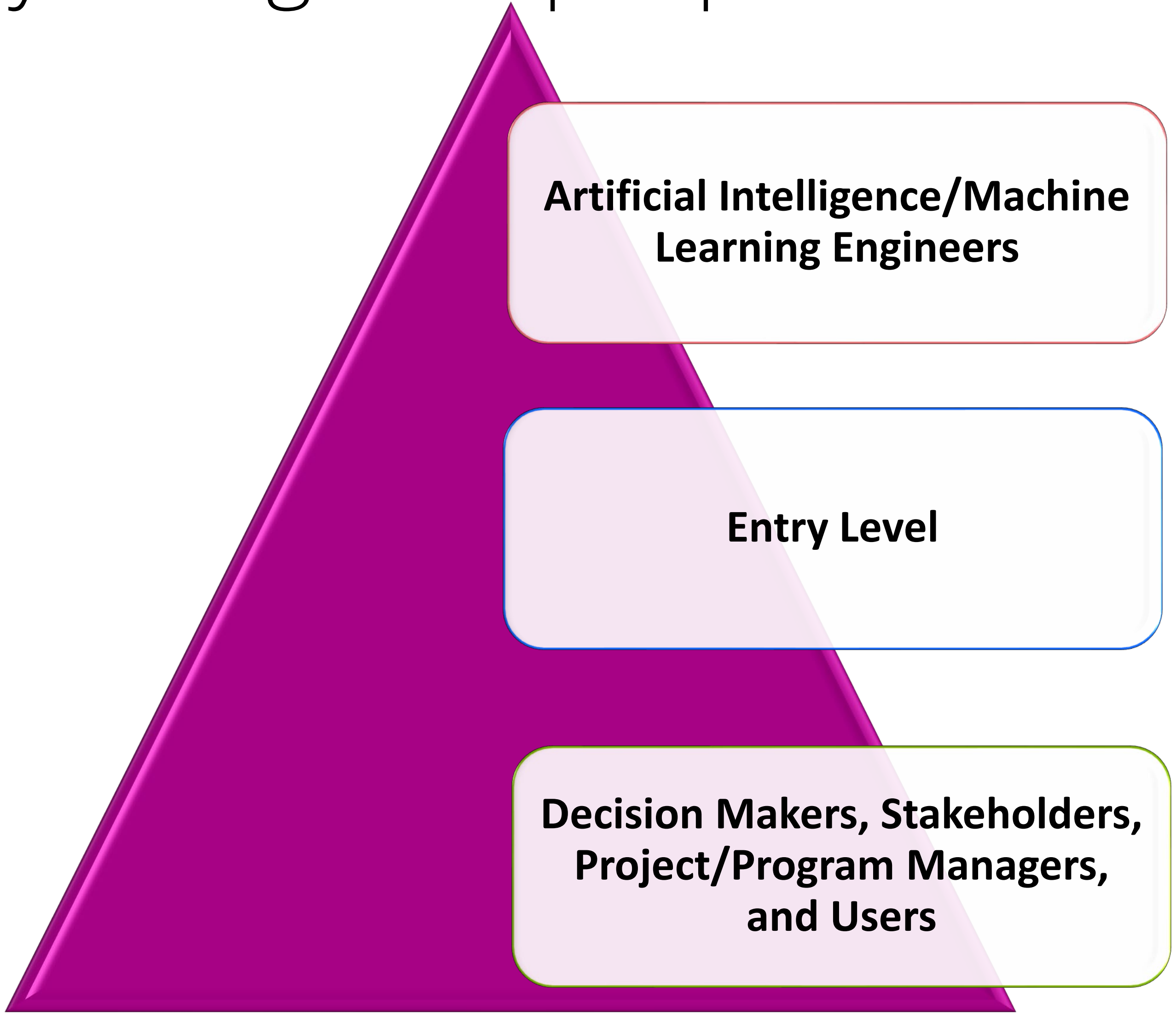
Network

Zero Trust

Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

How do you segment people to train?



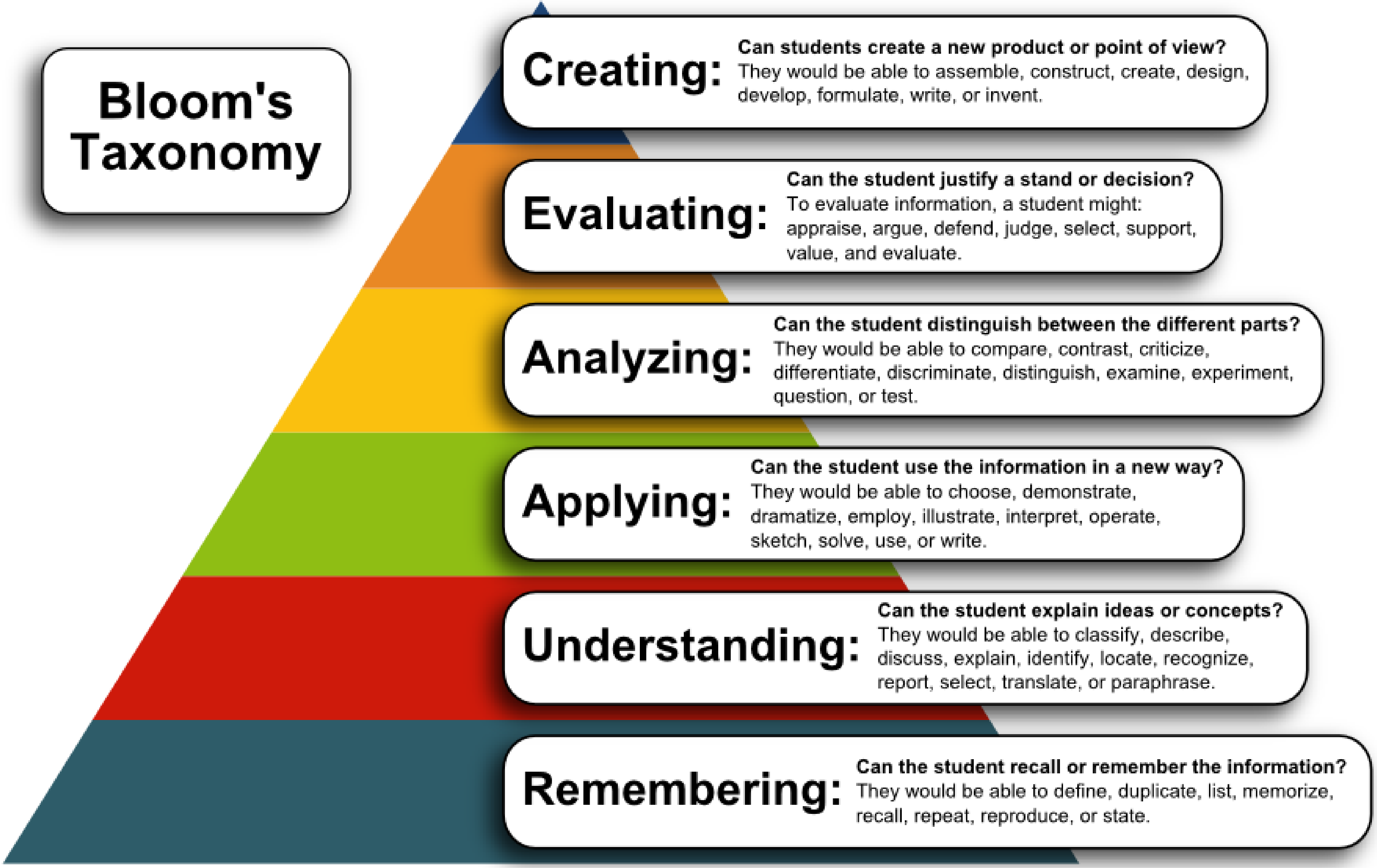
Artificial Intelligence/Machine Learning Engineers

Entry Level

Decision Makers, Stakeholders, Project/Program Managers, and Users

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Bloom's Taxonomy



Creating: **Can students create a new product or point of view?** They would be able to assemble, construct, create, design, develop, formulate, write, or invent.

Evaluating: **Can the student justify a stand or decision?** To evaluate information, a student might: appraise, argue, defend, judge, select, support, value, and evaluate.

Analyzing: **Can the student distinguish between the different parts?** They would be able to compare, contrast, criticize, differentiate, discriminate, distinguish, examine, experiment, question, or test.

Applying: **Can the student use the information in a new way?** They would be able to choose, demonstrate, dramatize, employ, illustrate, interpret, operate, sketch, solve, use, or write.

Understanding: **Can the student explain ideas or concepts?** They would be able to classify, describe, discuss, explain, identify, locate, recognize, report, select, translate, or paraphrase.

Remembering: **Can the student recall or remember the information?** They would be able to define, duplicate, list, memorize, recall, repeat, reproduce, or state.

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Examples: How Can AI affect the workplace

Skill Enhancement:

Professionals are reskilling and upskilling to work alongside AI systems, acquiring skills in data analysis, AI programming, and understanding AI ethics.

Increased Automation:

Repetitive and routine tasks are being automated, freeing up human workers to focus on more creative and complex tasks.

New Job Roles:

AI is creating new job roles related to AI development, AI ethics, and AI maintenance.

Data-Driven Decision-Making:

AI is facilitating data-driven decision-making, helping professionals make more informed choices.

Improved Efficiency:

Businesses and industries are using AI to optimize processes, reduce costs, and increase efficiency.

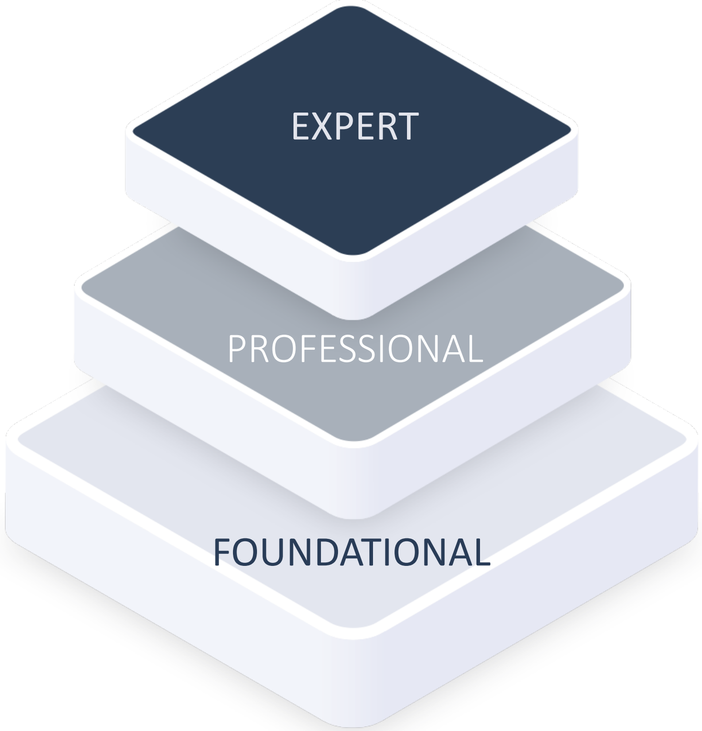
Data Privacy and Ethics:

Regulations and ethical guidelines are being developed to ensure responsible AI use and protect privacy.

Pearson
VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

How to address AI mastery/education



Mid-Career Specialty Skills

Effectively analyze, interpret, and utilize AI-generated data in decision-making processes

Entry-Level Specialty Skills

Hands-on experience in areas such as the fundamentals of AI, machine learning algorithms, data analytics, and computer vision

Skills Everyone Needs

Technical knowledge, critical thinking process, and ethical considerations

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Work Role Changes Examples

Data Analysts
AI is augmenting the work of data analysts by automating data cleaning, pattern recognition, and insights generation. Analysts are focusing more on strategy and decision-making.

IT Professionals
AI is used for network security, system administration, and troubleshooting. IT professionals are incorporating AI to enhance cybersecurity and streamline maintenance tasks.

Transportation Jobs
Autonomous vehicles are impacting jobs like truck driving and delivery services. New roles are emerging in vehicle maintenance, remote monitoring, and transportation logistics.

Manufacturing Workers
AI-driven robots and automation are used in manufacturing, which can lead to changes in job roles, such as focusing on robot maintenance and overseeing automated processes.

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

NOTE: Ethical Considerations

The successful integration of AI into these roles requires careful planning, training, and consideration of ethical and legal implications.

Human oversight and decision-making remain crucial to ensure the responsible and effective use of AI technologies in operations.

Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO)
Establishment of Ethical Principles

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Artificial Intelligence learning pathway

Foundational Concepts	Programming Fundamentals	Data Science Prerequisites	Vendor-Neutral Certification	Vendor-Specific Certification
AI for Business Professionals	Introduction to Programming with Python (PCEP)	Using Data Science Tools in Python Certified Data Science Practitioner	Certified AI Practitioner	AWS Certified Machine Learning Specialty Microsoft Certified: Azure Data Scientist Associate
Data Ethics for Business Professionals Generative AI credential for Business Professionals				

Notes:

- For individuals who expect they will require more intensive programming skills we would also recommend *Advanced Programming Techniques with Python (PCAP)*.
- Machine Learning utilizes mathematics – probability/statistics, linear algebra, and calculus. A participant does not require a degree in mathematics, but they should be familiar with advanced math concepts or have the aptitude to learn them along the way. A good free resource, if needed, can be found on OpenStax.org.

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

Summary

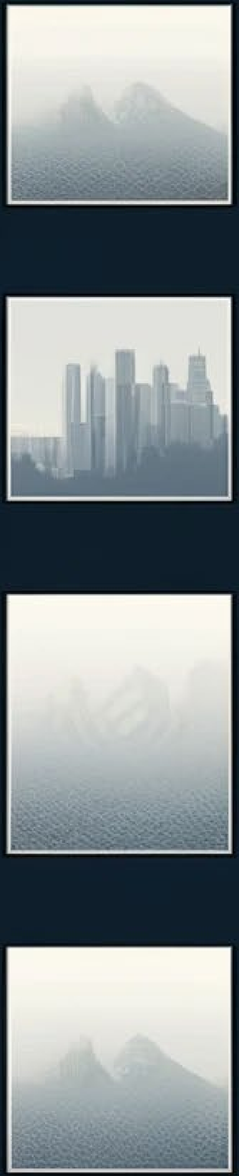
Pearson VUE

CONFIDENTIAL & PROPRIETARY Copyright © 2023 Pearson Education, Inc. or its affiliates. All rights reserved.

Building a Workforce Development plan for Artificial Intelligence

Define Training Goals	Identify Training Audience	Develop Training Content	Select Training Delivery	Implement Training Plan	Evaluate Training Results
Identify the specific goals of the training plan and how they align with the overall AI objectives of the organization	Determine who will be receiving the training and what the current level of knowledge is	Use content that is tailored to the needs of the audience that covers appropriate aspects of artificial intelligence	Choose an appropriate delivery method for training: online, in person, or a combination of both	Put the plan into action by scheduling sessions, assigning trainers, and providing learning materials	Measure the effectiveness of the training plan by assessing participant feedback and performance

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

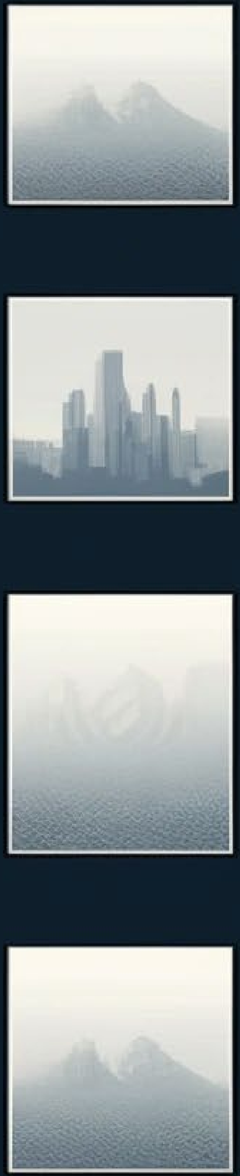


Knowledge vs Skill

AI doesn’t just sit in the IT department

Make sure you ask yourself:

- Are you solving the right problem?
- Are you using it ethically?
- What areas can touch/use AI



Information

Christopher.Bloor@Pearson.com

(952) 221-8990

CONFIDENTIAL & PROPRIETARY Copyright © 2024 Pearson Education, Inc. or its affiliates. All rights reserved.

34th Annual FISSEA Conference

Afternoon Networking Break and Exhibitor Showcase

2:45pm-3:15pm ET

#FISSEA | nist.gov/fissea

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

Welcome Back!

Frauke Steinmeier
FISSEA Co-Chair

Cyber Safety is Patient Safety: Navigating Cybersecurity Risks Through Enterprise Risk Management

Julie Chua

Director, Governance, Risk Management,
and Compliance Division
U.S. Department of Health and Human Services

HHS 405(d)
Aligning Health Care Industry Security Approaches

Cyber Safety is Patient Safety: Navigating Cybersecurity Risks through Enterprise Risk Management

2024

Visit Our Website
405d.hhs.gov

What We Do & Who We Are

The HHS 405(d) Program is a collaborative effort between the Health Sector Coordinating Council and the federal government to align healthcare industry security practices.

As the leading collaboration center of the Office of the Chief Information Officer, the 405(d) Program is focused on providing organizations across the nation with useful and impactful Healthcare and Public Health (HPH) focused resources, products, and tools that help educate, raise awareness, and provide vetted cybersecurity best practices which drive behavioral change and strengthen the sector's cybersecurity posture against cyber threats.

University Health System Cyber Attack

October 28, 2020, seemed like a normal day at a University Health system *until* a Ransomware Attack occurred.

Clinical impact perspective:

- Loss of access to network intranet servers, email communications, and clinical systems.
- Electronic medical record (EMR) protectively taken offline resulting in loss of access to production records including laboratory, pathology, pharmacy, and radiology.

Technical impact perspective:

- 1300 servers offline, hundreds of applications impacted, and over 5000 endpoints infected.
- Containment actions to disable internet, VPNs, and integrations and proactively take the EHR offline.

Planning and Next Steps

Although the health system had disaster recovery and business continuity plans in place for all major systems as well as third-party consultant on retainer to provide guidance in the event of a major cybersecurity incident, it was clear within hours that this was a severe ransomware attack with the potential to disrupt institutional provision of life-saving care.

Notified federal local law enforcement

Took the EMR offline

Cut off all internet and other access both to and from the health system

Severed connections to affiliates and other partners

Deployed EDR agents to all endpoints

Blocked traffic at internal segments

Patient Impact

Challenges to Care

- The loss of communication channels.
- The loss of the individualized EMR chemotherapy plan templates driving nursing and pharmacy processes to enable the safe delivery of systemic therapies to cancer patient population.
- Loss of a reliable encrypted email communications platform challenged efforts to organize and coordinate response amidst the COVID-19 pandemic, and prevented regular, large, and in-person meetings.

Making Ethical Decisions and Continuing Care in the Wake of a Cyber Attack

During a major cyber-attack serious decisions of patient care must be made. Basic patient safety tenets must be followed when delivering care during a ransomware attack:

- Maximization of lives saved
- Utilization of accepted medical prognostic criteria
- Equitable and fair assessment of all cases
- Transparency in decision-making process. Impartiality and neutrality of decision-makers

Cyber Impacts to Healthcare Facilities

Technology continues to increase in the healthcare sector and with it comes more risks and vulnerabilities.

Impacts to a practice in the event of a cyber incident:

- No access to patient electronic medical records
- No access to billing or scheduling software
- Practice closure
- No access to email systems
- No access to Network Connected Medical equipment
- In some cases, causes small practices to close for good

According to the HHS Office for Civil Rights (OCR), cyber incidents in health care are on the rise.

- From 2018-2022, there has been a 93% increase in large breaches reported to OCR (369 to 712), with a 278% increase in large breaches involving ransomware.

Change Healthcare Cyber Attack Impact

Change Healthcare

- Change Health reviews 15B medical claims annually and is the largest clearing house in the US
- Network impacted encompasses roughly 900,000 Physicians, 118,000 Dentists, 33,000 Pharmacies, 5,500 Hospitals, 600 Labs.
- Breach reportedly resulted in a $22M payout (Reuters)
- Ongoing federal investigation
- Congressional hearings
- **UnitedHealth estimates costs could reach $1.6 billion**

Source: Health Subcommittee Hearing: "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack" April 2024

Hospitals and Practices

- 55% of respondents had to use personal funds to cover practice expenses
- 78% have lost revenue from claims that they have been unable to submit
- **94% of hospitals reported some financial impact**
- 44% were unable to purchase supplies
- 31% were unable to make payroll
- 80% have lost revenue from unpaid claims

Source: American Health Association Change Healthcare Cyberattack Impact Survey, April 2024

Patients

- **74% of hospitals said the incident resulted in "direct patient care impact."**
- Almost 2 in 5 hospitals said that their patients are "having difficulty accessing care because of delays in processing of health plan utilization requirements (e.g. prior authorization)
- Inability to fulfill prescription drug care
- Forced to pay cash for prescriptions or denied use of discount coupons

Sources: American Health Association Change Healthcare Cyberattack Impact Survey, April 2024 and Washington Post, "How a health-care cyberattack may affect your prescription drug access," Mar 2024

Cyber incidents affecting hospitals and health systems have led to extended care disruptions, patient diversions to other facilities, and delayed medical procedures, all putting patient safety at risk. (HHS Press Release, Dec 2023)

Integrating Cybersecurity with Enterprise Risk Management

Cyber Risks are Healthcare Risks

Enterprise Risk Management

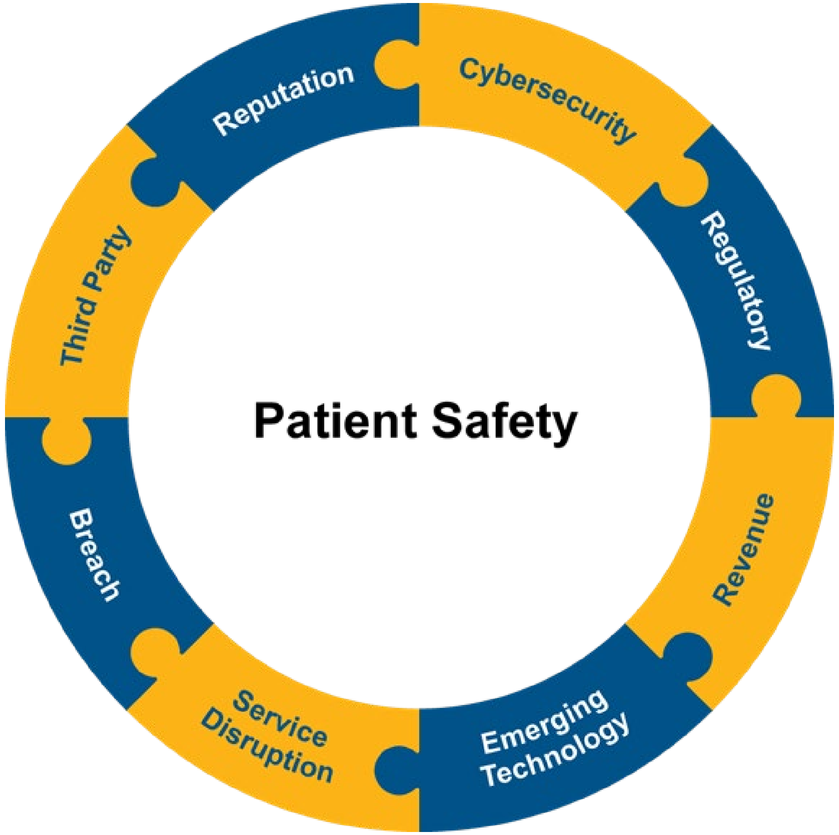
ERM is an effective organization-wide approach to addressing the full spectrum of the organization’s significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within siloes.

- Risks are interrelated
- ERM helps tie these into mission impacts
- ERM supports credible decision-making based on risk and opportunity information
- ERM normalizes risks across many domains to allow comparability

Cybersecurity Risk Management

Cybersecurity risks are one of many enterprise risks. These risks can affect every aspect of an organization including care delivery. The most important risk is to patient safety, which is the corner stone of every health organization.

- Integration is critical for informing senior leaders and business owners on cyber risks
- Focus on strategies to manage and respond to evolving cyber threat environments



AFERM Association for Federal Enterprise Risk Management

Cyber ERM CoI

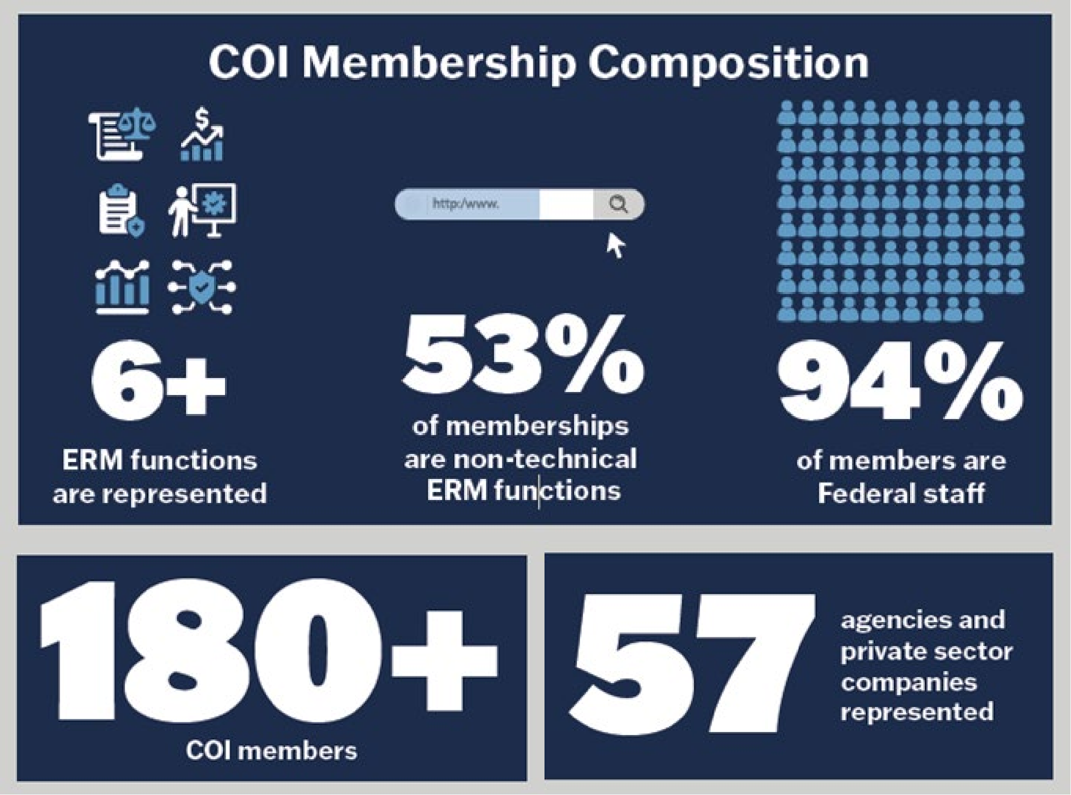
CYBERSECURITY ERM COMMUNITY of INTEREST

Cyber-ERM COI

- The Cyber-ERM COI is a diverse interagency platform for federal practitioners to collaborate, exchange ERM and cybersecurity federal guidance, best practices, and approaches to advance cyber-ERM integration.
- The COI membership diversity is a hallmark strength and is reflective in the curation of products developed and the array of keynote speakers over emerging cyber and ERM topics.
- The COI is guided by NISTIR 8286 series and SP800-221/221A.
- Enterprise Risk Management Playbook (Fall 2022) update, focusing on the special chapter on integrating agency ERM with information security and cybersecurity risk management.

Special Project: Cyber-ERM-Focused Working Groups

- Members identified areas of potential growth within their agency that could enhance Cyber-ERM integration.
- Three working groups were established, all led by COI members:
  - Cyber Risk Register Working Group
  - Risk Appetite and Risk Tolerance Working Group
  - Survey of Tools and Technology Working Group



COI Membership Composition

6+ ERM functions are represented

53% of memberships are non-technical ERM functions

94% of members are Federal staff

180+ COI members

57 agencies and private sector companies represented

HHS 405(d) Program Resources for the Healthcare and Public Health Sector

HICP 2023 Edition

405(d)'s Cornerstone Publication

Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.

Top 5 Cybersecurity Threats and 10 Mitigating Practices

- Social Engineering
- Ransomware
- Loss or Theft of Equipment or Data
- Insider Accidental or Malicious Data Loss
- Attacks Against Network Connected Medical Devices

1. **Email Protection Systems**
2. **Endpoint Protection Systems**
3. **Access Management**
4. **Data Protection and Loss Prevention**
5. **Asset management**
6. **Network Management**
7. **Vulnerability Management**
8. **Incident Response**
9. **Medical Device Security**
10. **Cybersecurity Policies**

Knowledge on Demand Trainings Offered

Social Engineering

This training offers an overview of Social engineering tactics including email phishing, smishing, and more and tips on how to recognize them

Ransomware

This training provides an overview of the ransomware threat and helps people understand the key ways in which attackers gain control of a network

Loss or Theft of Equipment or Data

This training provides an overview of best practices on securing equipment and data

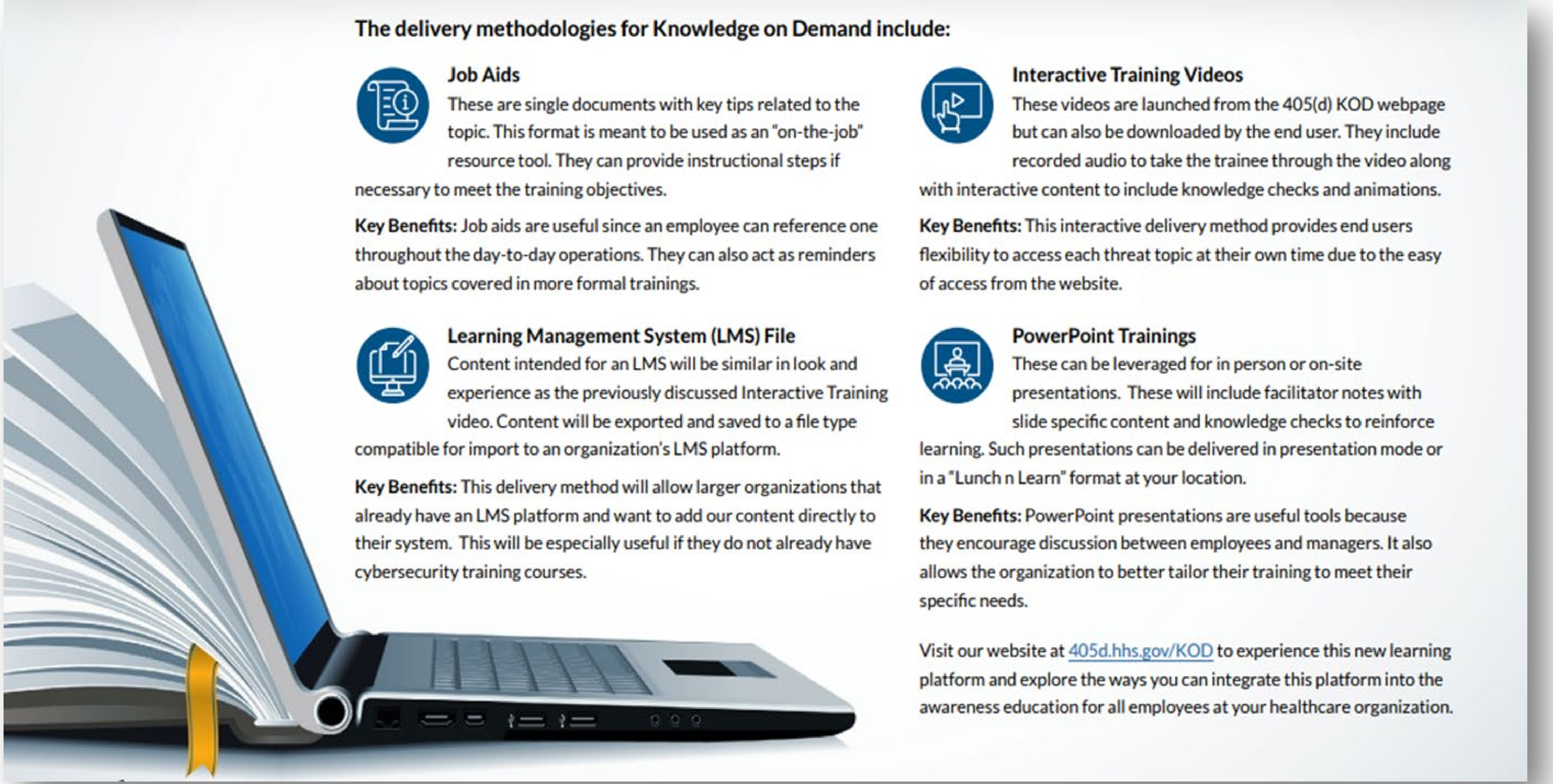
Insider Accidental or Malicious Data Loss

This training provides an overview of insider data loss accidents and ones with malicious intent

Attacks Against Connected Medical Devices

This training provides an overview of the importance of securing network connected medical devices

Knowledge on Demand



The delivery methodologies for Knowledge on Demand include:

Job Aids

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

Key Benefits: Job aids are useful since an employee can reference one throughout the day-to-day operations. They can also act as reminders about topics covered in more formal trainings.

Learning Management System (LMS) File

Content intended for an LMS will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

Key Benefits: This delivery method will allow larger organizations that already have an LMS platform and want to add our content directly to their system. This will be especially useful if they do not already have cybersecurity training courses.

Interactive Training Videos

These videos are launched from the 405(d) KOD webpage but can also be downloaded by the end user. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

Key Benefits: This interactive delivery method provides end users flexibility to access each threat topic at their own time due to the easy of access from the website.

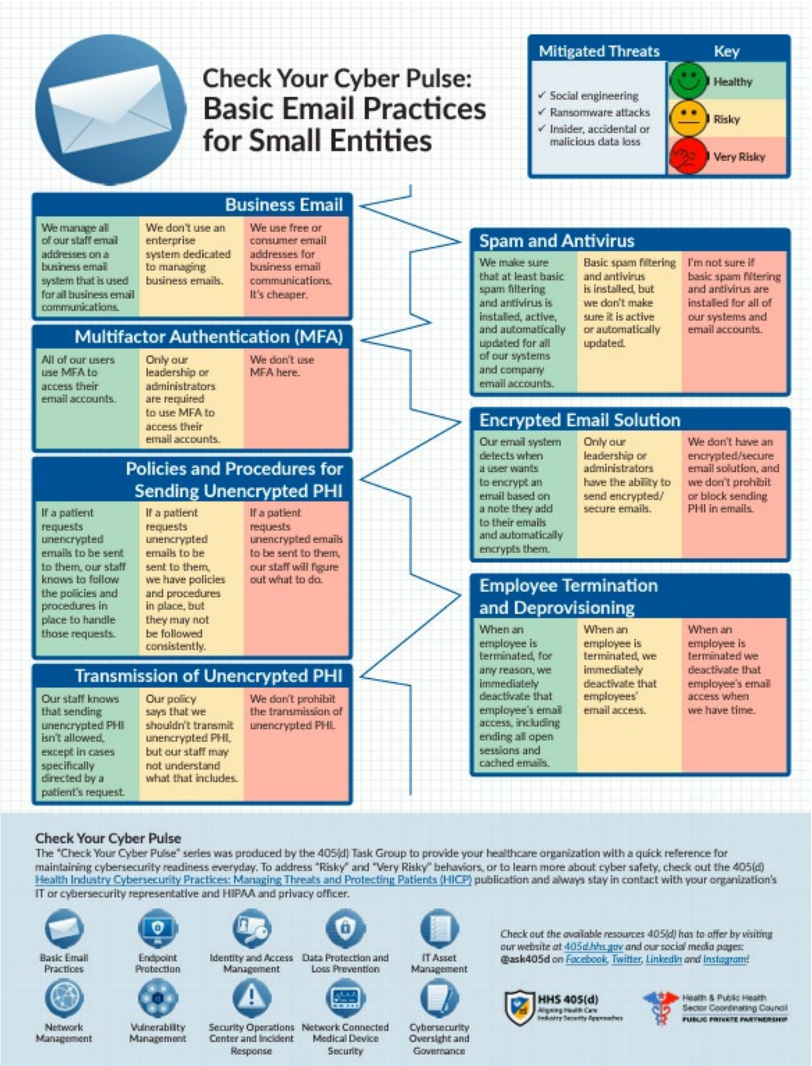
PowerPoint Trainings

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

Key Benefits: PowerPoint presentations are useful tools because they encourage discussion between employees and managers. It also allows the organization to better tailor their training to meet their specific needs.

Visit our website at 405d.hhs.gov/KOD to experience this new learning platform and explore the ways you can integrate this platform into the awareness education for all employees at your healthcare organization.

Check Your Cyber Pulse



Check Your Cyber Pulse: Basic Email Practices for Small Entities

Mitigated Threats

- ✓ Social engineering
- ✓ Ransomware attacks
- ✓ Insider, accidental or malicious data loss

Key

🟩	Healthy
🟨	Risky
🟥	Very Risky

Business Email

We manage all of our staff email addresses on a business email system that is used for all business email communications.	We don't use an enterprise system dedicated to managing business emails.	We use free or consumer email addresses for business email communications. It's cheaper.

Multifactor Authentication (MFA)

All of our users use MFA to access their email accounts.	Only our leadership or administrators are required to use MFA to access their email accounts.	We don't use MFA here.

Policies and Procedures for Sending Unencrypted PHI

If a patient requests unencrypted emails to be sent to them, our staff knows to follow the policies and procedures in place to handle those requests.	If a patient requests unencrypted emails to be sent to them, we have policies and procedures in place, but they may not be followed consistently.	If a patient requests unencrypted emails to be sent to them, our staff will figure out what to do.

Transmission of Unencrypted PHI

Our staff knows that sending unencrypted PHI isn't allowed, except in cases specifically directed by a patient's request.	Our policy says that we shouldn't transmit unencrypted PHI, but our staff may not understand what that includes.	We don't prohibit the transmission of unencrypted PHI.

Spam and Antivirus

We make sure that at least basic spam filtering and antivirus is installed, active, and automatically updated for all of our systems and company email accounts.	Basic spam filtering and antivirus is installed, but we don't make sure it is active or automatically updated.	I'm not sure if basic spam filtering and antivirus are installed for all of our systems and email accounts.

Encrypted Email Solution

Our email system detects when a user wants to encrypt an email based on a note they add to their emails and automatically encrypts them.	Only our leadership or administrators have the ability to send encrypted/ secure emails.	We don't have an encrypted/secure email solution, and we don't prohibit or block sending PHI in emails.

Employee Termination and Deprovisioning

When an employee is terminated, for any reason, we immediately deactivate that employee's email access, including ending all open sessions and cached emails.	When an employee is terminated, we immediately deactivate that employees' email access.	When an employee is terminated we deactivate that employee's email access when we have time.

Check Your Cyber Pulse

The "Check Your Cyber Pulse" series was produced by the 405(d) Task Group to provide your healthcare organization with a quick reference for maintaining cybersecurity readiness everyday. To address "Risky" and "Very Risky" behaviors, or to learn more about cyber safety, check out the 405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and always stay in contact with your organization's IT or cybersecurity representative and HIPAA and privacy officer.

- Basic Email Practices
- Endpoint Protection
- Identity and Access Management
- Data Protection and Loss Prevention
- IT Asset Management
- Network Management
- Vulnerability Management
- Security Operations Center and Incident Response
- Network Connected Medical Device Security
- Cybersecurity Oversight and Governance

Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*

HHS 405(d) Aligning Health Care Industry Security Approaches

Health & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

This series was produced by the 405(d) Task Group to provide small to medium healthcare organizations a quick reference for maintaining cybersecurity readiness every day. Use this resource to assess if your organization is Health, Risky, or Very Risky!

How does it work?

1. Download the Check Your Cyber Pulse resource from 405d.hhs.gov

2. The Check Your Cyber Pulse resource uses the ten mitigating practices located in HICP as a guide for you to see how "Risky" your organization is. Go through each items and select if you are "Healthy" "Risky" or "very Risky"

3. For items you scored "Risky" or "Very Risky" check out the HICP Technical Volumes to find out how to address these items

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Questions?

Visit Our Website
405d.hhs.gov

Do you follow us on social media?

Update to NIST SP 800-50

Marian Merritt
Deputy Director of NICE
National Institute of Standards and Technology

Susan Hansche
Training Manager
Department of Homeland Security

Brenda Ellis
Service Element Lead for Awareness and Training/NASA OCIO
Cybersecurity Service Line

NIST SP 800-50 update

Panel:

Brenda Ellis, NASA

Susan Hansche, CISA

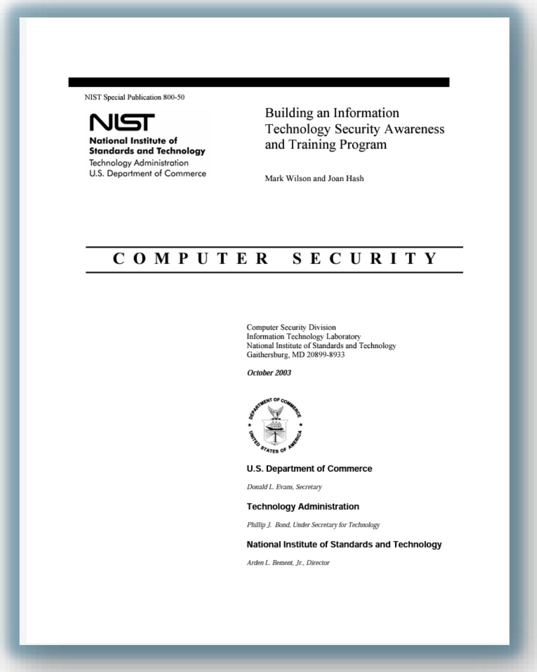
Marian Merritt, NIST

Additional NIST Special Publication 800-50 Authors:
Kevin Sanchez-Cherry, DOT
Julie Snyder, MITRE
Don Walden, IRS

NIST SP 800-50 rev 1

- Building an Information Technology Security Awareness & Training Program - 2003 (20 years ago)
- Revision draft made public August 28, 2023
- Comments through October 27, 2023
- Co-authoring team from several Federal agencies

- Goals:
  - Leverage NIST guidance
  - Develop consistent language
  - Reflect research from FISSEA community
  - Address challenges such as measuring impact



NIST Special Publication 800-50

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

Building an Information
Technology Security Awareness
and Training Program

Mark Wilson and Joan Hash

C O M P U T E R   S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

NIST SP 800-50 rev 1, cont.

Goals, continued:

- Describe a cyclical, iterative, and responsive model
- Consolidates 800-16, incorporates NICE Framework
- Intended to be collaborative, flexible, scalable (work for small and very large organizations)
- Intended for federal agencies and organizations

Adding Privacy

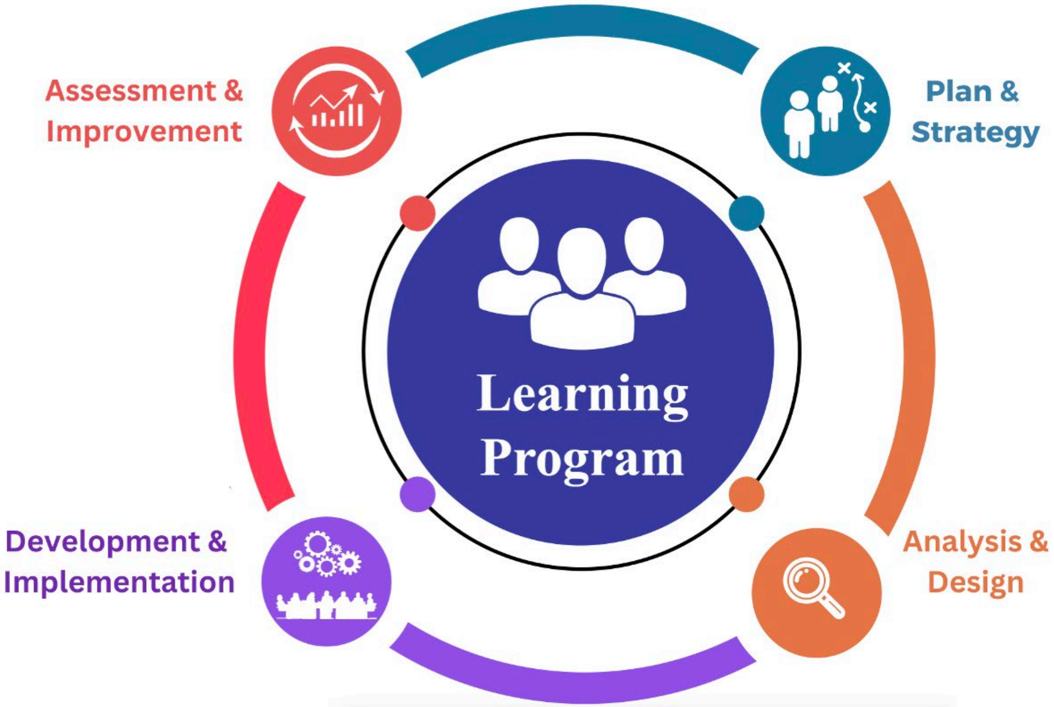
- Background to the Privacy Act of 1974
- Requirements of OMB Circular A-130
- Leverage and reference the NIST Privacy Framework

What SP 800-50 r1 is:

- “Building a Cybersecurity and Privacy Learning Program”
- Enterprise-wide awareness, training, and education program - Cybersecurity and Privacy Learning Program (CPLP)
- The learning program supports a culture of respect for employees
- Everyone plays some type of role in managing the organization’s cybersecurity and privacy risk

The Learning Program is…

- a cyclical, iterative model that adapts to each agency’s needs and situation
- Intended to be collaborative, flexible, scalable
- A way to encourage cross-functional cooperation with senior leadership

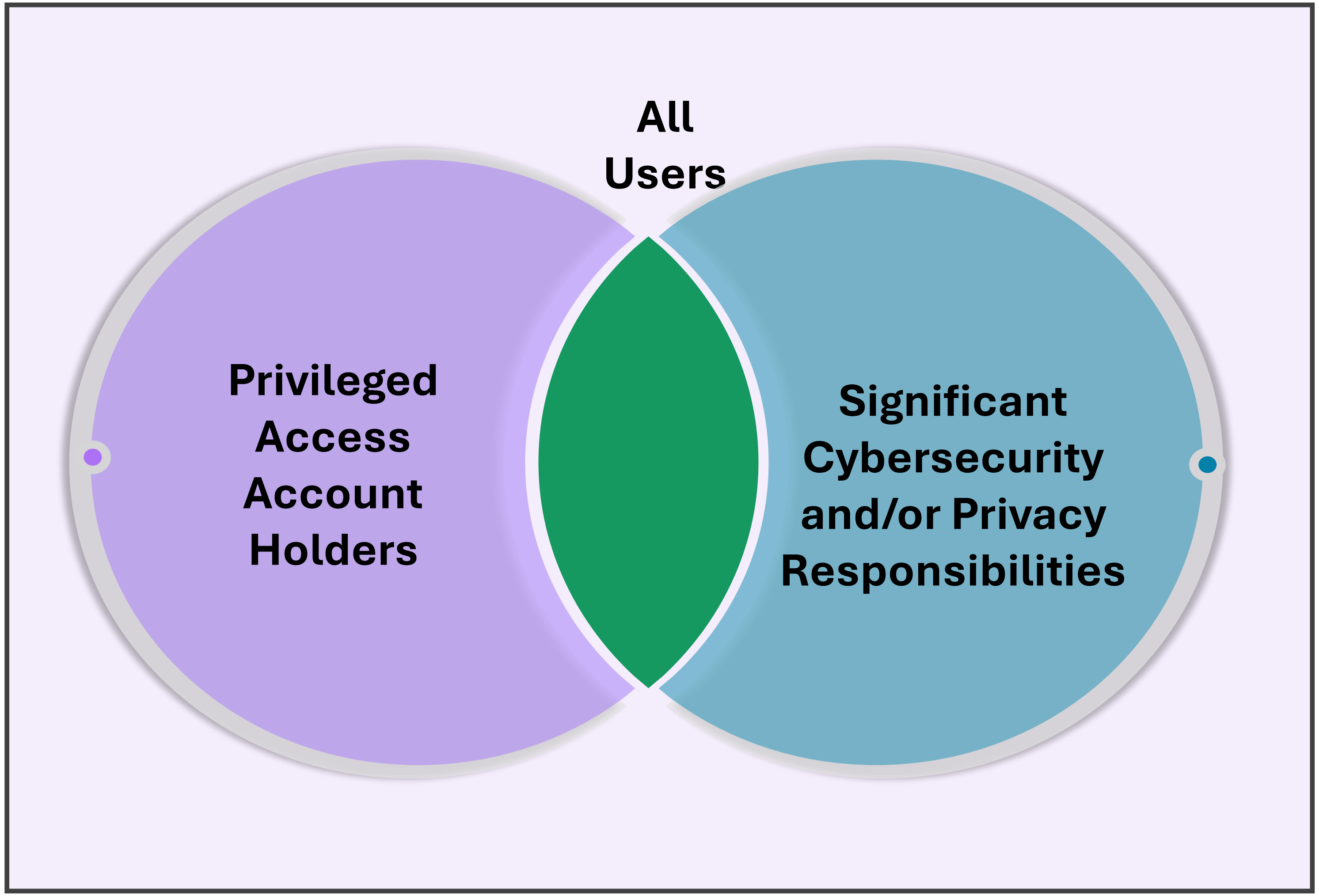


Key sections of 800-50

- Introduction
  - Purpose, Scope, the CPLP Life Cycle
  - Developing a Cybersecurity and Privacy Culture
  - Privacy and Cybersecurity: the relationship, key concepts, how to coordinate learning for both efforts
  - Key roles and responsibilities

- CPLP Plan and Strategy
  - Goals, Objectives, Tactics
  - Measurements and Metrics
  - Audience Types

Learning Program Audience Types


All Users
Privileged Access Account Holders
Significant Cybersecurity and/or Privacy Responsibilities

All Users
Onboarding training, acceptable use policies, annual learning program, or awareness campaigns

Privileged Access Account Holders
E.g. system, network, web, and/or application training

Significant Cybersecurity and/or Privacy Responsibilities
Determined by individual development plan, manager, or work role

Privileged Access Account Holders with Significant Cybersecurity and/or Privacy Responsibilities

Key sections of 800-50, continued

- Types of activities: awareness, experiential learning, training
- Setting priorities
- Establishing a budget, determining staff needs
- Analysis and Design: what works, where is change needs, being nimble
- Design phases, from the initial document through setting requirements
- Development and Implementation of the CPLP
- Developing and testing new material
- Assessing and improving the program

Senior Leadership

- 800-50 r1 recommends forming a Senior Leadership committee or advisory board
  - CIO, CPO, etc
  - Human Resources
  - Communications
- Strategy and Budget Planning
- Regular Program review and discussion
- Program support and participation

What SP 800-50 r1 is NOT

- Details on designing or developing new training elements
- How to create a change management or cultural program
- An enterprise-wide human risk management program
- Who should do what work in the organization
- How to create an enterprise-wide metrics program
- How to identify employees in your workforce according to the NIST

SP 800-181 work roles

What comes next…

- ~~Final editing to incorporate comments~~
- Internal NIST editorial review
- Publish to the public-facing NIST website

Q&A

Thank you!

Journey to the Cybersecurity Framework Version 2.0

Amy Mahn

International Policy Specialist

National Institute of Standards and Technology

NIST Cybersecurity Framework 2.0
Overview & Updates

Amy Mahn
Applied Cybersecurity Division
April 2024

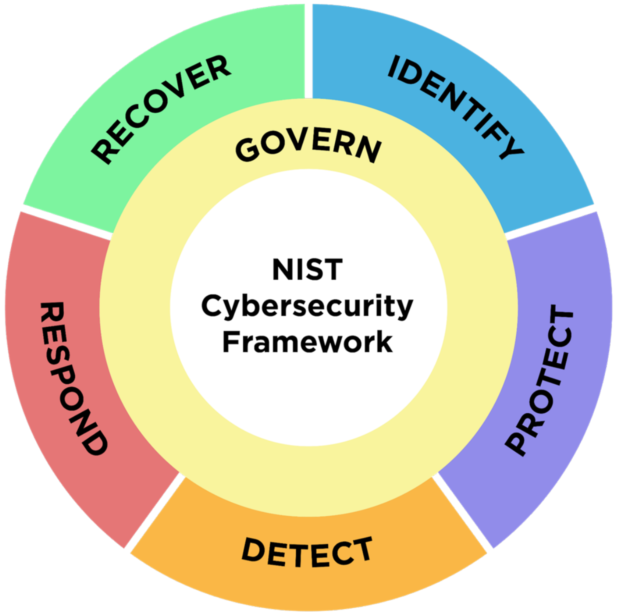
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CSF 2.0 Overview

NIST has updated the widely used Cybersecurity Framework (CSF)—its landmark guidance document for **reducing cybersecurity risk**.

Six Functions — **Govern, Identify, Protect, Detect, Respond,** and **Recover.** Together, they provide a comprehensive view for managing cybersecurity risk.

The Framework is also comprised of:
CSF Core
CSF Organizational Profiles
CSF Tiers



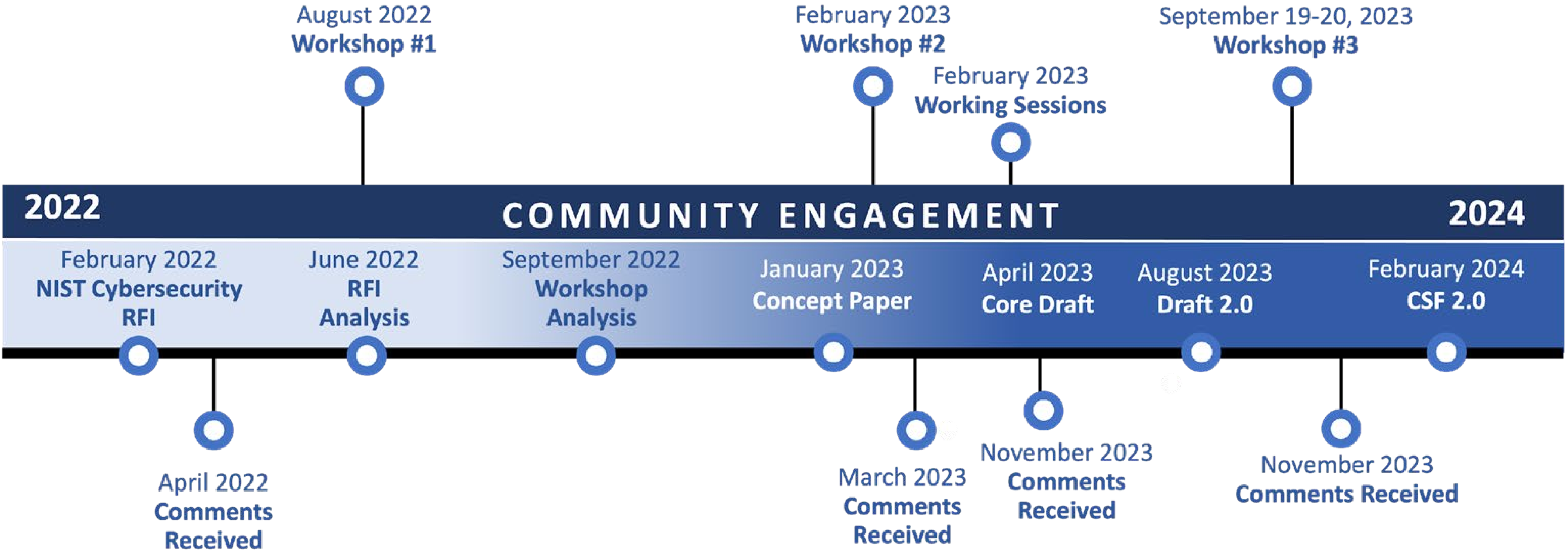
Quote from the NIST Director

“The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats. CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization’s cybersecurity needs change and capabilities evolve.”

~ **Laurie E. Locascio**

Under Secretary of Commerce for Standards and Technology
& NIST Director

How Did We Get Here?



August 2022
Workshop #1

February 2023
Workshop #2

February 2023
Working Sessions

September 19-20, 2023
Workshop #3

2022

COMMUNITY ENGAGEMENT

2024

February 2022
NIST Cybersecurity RFI

June 2022
RFI Analysis

September 2022
Workshop Analysis

January 2023
Concept Paper

April 2023
Core Draft

August 2023
Draft 2.0

February 2024
CSF 2.0

April 2022
Comments Received

March 2023
Comments Received

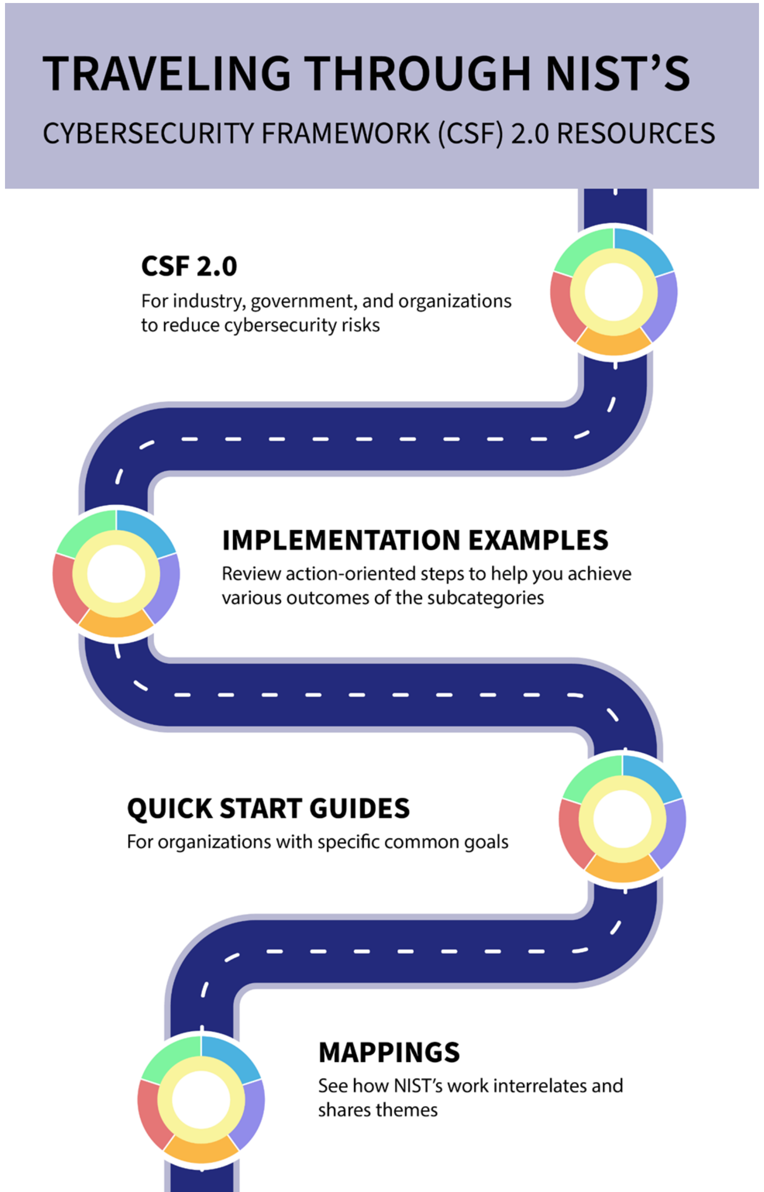
November 2023
Comments Received

November 2023
Comments Received

Visit our CSF 2.0 Website: www.nist.gov/cyberframework

CSF 2.0 | What Makes it Different?

- CSF 2.0 can help **all organizations** – not just those in critical infrastructure – manage and reduce risks.
- It improves on prior versions; we listened to your feedback, made key updates, **developed new resources and tools**, and adjusted our guidance based on today's cybersecurity environment.
- NIST's suite of resources offers **practical and actionable suggestions** to help organizations immediately improve their cybersecurity posture (focus on *how* the CSF can be implemented).
- The CSF 2.0 is about a **suite of resources** that aims to help **all organizations** – not just those in critical infrastructure – manage and reduce risks.



TRAVELING THROUGH NIST'S

CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES

CSF 2.0

For industry, government, and organizations to reduce cybersecurity risks

IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve various outcomes of the subcategories

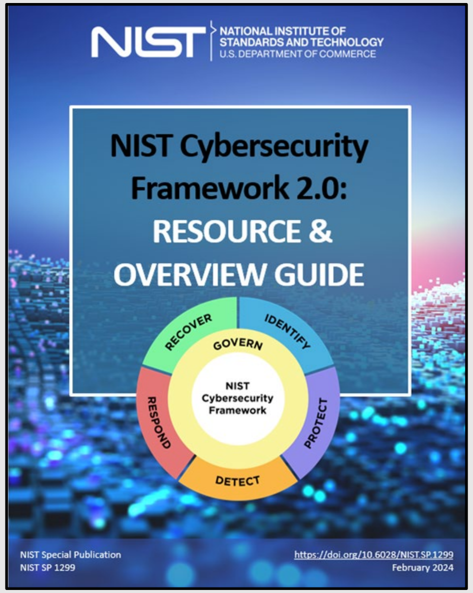
QUICK START GUIDES

For organizations with specific common goals

MAPPINGS

See how NIST's work interrelates and shares themes

Suite of Resources Snapshot



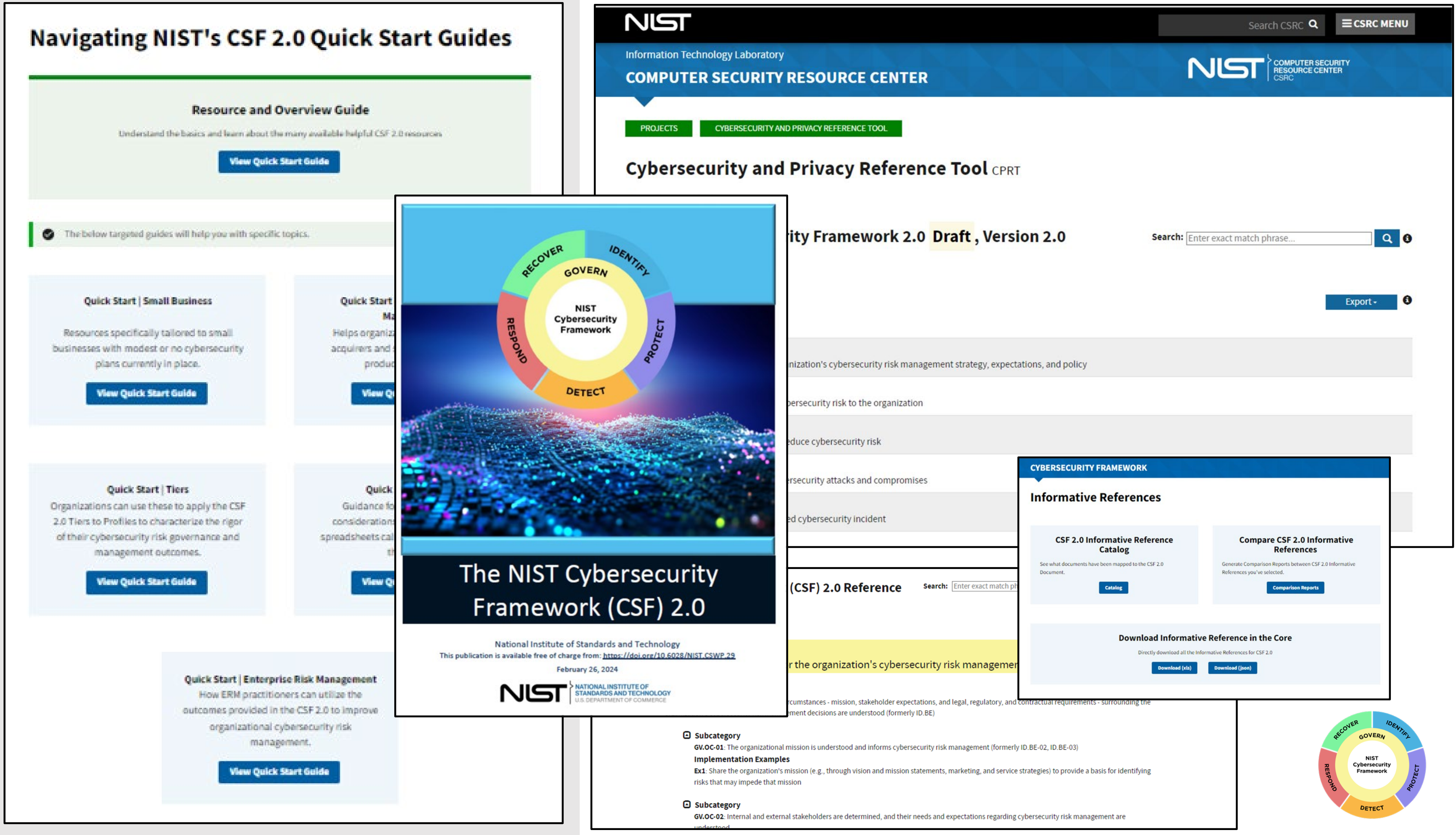
NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:
RESOURCE & OVERVIEW GUIDE

NIST Special Publication
NIST SP 1299
https://doi.org/10.6028/NIST.SP.1299
February 2024

NIST Cybersecurity Framework 2.0:
Small Business Quick-Start Guide

NIST Cybersecurity Framework 2.0:
Quick-Start Guide for Creating and Using Organizational Profiles



Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

Understand the basics and learn about the many available helpful CSF 2.0 resources

View Quick Start Guide

The below targeted guides will help you with specific topics.

Quick Start | Small Business

Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

View Quick Start Guide

Quick Start | Tiers

Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

View Quick Start Guide

Quick Start | Enterprise Risk Management

How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

View Quick Start Guide

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

Cybersecurity and Privacy Reference Tool CPRT

ity Framework 2.0 Draft, Version 2.0

Search: Enter exact match phrase...

nization's cybersecurity risk management strategy, expectations, and policy
ersecurity risk to the organization
educe cybersecurity risk
rsecurity attacks and compromises
ed cybersecurity incident

CYBERSECURITY FRAMEWORK

Informative References

CSF 2.0 Informative Reference Catalog
See what documents have been mapped to the CSF 2.0 Document.
Catalog

Compare CSF 2.0 Informative References
Generate Comparison Reports between CSF 2.0 Informative References you've selected.
Comparison Reports

Download Informative Reference in the Core
Directly download all the Informative References for CSF 2.0
Download (xls) Download (json)

(CSF) 2.0 Reference Search: Enter exact match p

r the organization's cybersecurity risk managemen

rcumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the
ment decisions are understood (formerly ID.BE)

Subcategory
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)
Implementation Examples
Ex1: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission

Subcategory
GV.OC-02: Internal and external stakeholders are determined, and their needs and expectations regarding cybersecurity risk management are understood

Global Impact of CSF 2.0

- The CSF is used widely **internationally**.
- CSF versions 1.1 and 1.0 have been translated into 13 languages (*CSF 2.0 translations anticipated soon*).
- NIST's work with the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), over the last 11 years has been expansive.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

Learn About Our Global Impact: www.nist.gov/cyberframework

What is Next?

We hope that the CSF 2.0 suite of documents and tools will make a difference in managing and reducing cybersecurity risks.

NIST continues to encourage candid, constructive discussions and other engagements about organizations’ experiences with the CSF .

Remember, cybersecurity risk management is always a journey – and the CSF 2.0 is a navigational guide that can help make that journey more successful.

See NIST’s Suite of CSF 2.0 Resources: www.nist.gov/cyberframework

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

STAY IN TOUCH

CONTACT US

nist.gov/
cyberframework

@NISTcyber

Email us: cyberframework@nist.gov

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 2025
Email fissea@list.nist.gov

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

SAVE THE DATE

Federal Information Security Educators (FISSEA) Summer Forum

September 17, 2024

#FISSEA | nist.gov/fissea

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