FISSEA 34th Annual Conference:
Refining Cybersecurity Culture: WIIFM*

May 14-15, 2024
Rockville, MD

*What’s in it for me?
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
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

#FISSEA | nist.gov/fissea
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
65% of all breaches involve the human element.
SECURITY AWARENESS MATURITY MODEL™

Your Roadmap to Managing Human Risk

- Non-Existence
- Compliance-Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainment & Cultural Change
- Strategic Metrics Framework
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
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. Even if 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 Wi-Fi network, such as your home Wi-Fi when online, consider shutting off the Wi-Fi option on your phone and use your data plan. Yes, it is 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 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, if 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 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 the holidays to spread 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 legitimate discounts or special offers. 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 are available to criminal 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.


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 using 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 your browsing history, so adding in your credit card information when 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. If you are wondering what might bring the latest 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 to 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

- WHY
- HOW
- WHAT
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.
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

1. **What Are My Top Human Risks & the Behaviors that Manage Those Risks?**
2. **Engage, Motivate & Train**
3. **Security Awareness Program**
4. **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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Click Rate</td>
<td>Number of people who fall victim to a phishing sensation (the definition of falling victim is clicking on the link or opening an attachment).</td>
<td>Phishing assessment</td>
<td>Monthly</td>
<td>Security Team</td>
<td>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.</td>
</tr>
<tr>
<td>Phishing Reporting</td>
<td>Number of people who detect and report a phishing email (regardless of whether it’s an assessment or real attack).</td>
<td>Phishing assessment</td>
<td>Monthly</td>
<td>Security Team</td>
<td>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.</td>
</tr>
<tr>
<td>Phishing Repeat Offenders</td>
<td>Number of workloads that repeatedly fall victim to phishing sensations. Those individuals are not changing behavior and represent a high risk.</td>
<td>Phishing assessment</td>
<td>Monthly</td>
<td>Security Awareness Team</td>
<td>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 another way.</td>
</tr>
<tr>
<td>Facility Physical Security</td>
<td>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 skipping those who are not.</td>
<td>Test monthly or weekly</td>
<td>Information Security or Physical Security</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Updated Devices</td>
<td>Percentage of devices that are updated and current.</td>
<td>When employees connect to an internal server or use an external service such as &lt;servername&gt;.guide.com</td>
<td>Monthly</td>
<td>Security or Technology Team</td>
<td>Measure whether people are keeping their devices updated and current, especially when connecting BYOD (Bring Your Own Device).</td>
</tr>
<tr>
<td>Lost/Stolen Devices</td>
<td>Number of devices (desktop, smartphones, tablets) that were lost or stolen. What percentage of those devices were encrypted?</td>
<td>Reports to security team or by physical asset audits</td>
<td>Monthly</td>
<td>Security Team or Asset Management</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Desktop</td>
<td>Number of employees who are securing their desk environment before leaving, as per organizational policy.</td>
<td>Nightly walkthrough</td>
<td>Monthly or weekly</td>
<td>Information Security or Physical Security Team</td>
<td>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.</td>
</tr>
<tr>
<td>Passwords</td>
<td>Number of employees using strong passwords.</td>
<td>Password brute forcing</td>
<td>Monthly or quarterly</td>
<td>Security Team</td>
<td>Security gains authorized access to system password database (such as AD or Unix server) and attempts to brute force or crack password hashes.</td>
</tr>
<tr>
<td>2FA / MFA (or Password Manager) Adoption</td>
<td>Measuring use or adoption of what percentage of accounts use MFA for strong authentication, outlined one of the most effective controls in protecting accounts/data.</td>
<td>Satisfactory sampling of any account protected with a password, to include individuals, system accounts.</td>
<td>Monthly</td>
<td>Security team or Operations</td>
<td>MFA is considered by many to be one of the most effective means of protecting system accounts and data. You want not only measure if employees and staff are using it, but for application accounts, system accounts, privileged accounts, etc.</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>Number of employees posting sensitive organizational information on social networking sites.</td>
<td>Online searches for key terms</td>
<td>Monthly</td>
<td>Security Team (or outsiders)</td>
<td>Do extensive searches on sites such as Facebook and LinkedIn to ensure employees are not posting sensitive organizational information.</td>
</tr>
<tr>
<td>Data Wiping or Destruction</td>
<td>Number of employees who are properly following data destruction practices.</td>
<td>Check digital devices that are disposed of for proper wiping. Check dumpsters for sensitive documents.</td>
<td>Random</td>
<td>Information Security or Physical Security</td>
<td>Any digital devices that are disposed of (donated, thrown out, recyled) may contain sensitive data. Check to ensure proper wiping procedures. Check any rubbish bins or dumpsters for any sensitive documents that were not destroyed.</td>
</tr>
<tr>
<td>Device Physical Security</td>
<td>Number of employees who left their devices unsecured in their cars in the organization’s parking lot.</td>
<td>Do a physical walkthrough of the parking lot and identify any cars that have devices that are visible on a car seat.</td>
<td>Monthly</td>
<td>Information Security or Physical Security</td>
<td>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.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Number of employees who can identify, stop, and report a social engineering attack.</td>
<td>Phone call assessments</td>
<td>Monthly</td>
<td>Security Team</td>
<td>Security team calls random employees, attacking them as a real cyber attacker would by attempting to social engineer the victim. An example could be pretending to be Microsoft support and having video download infected animations.</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Does workforce know and understand what is expected of them?</td>
<td>Knowledge assessments and online quizzes</td>
<td>Annual or after training</td>
<td>Learning Management or Security Awareness Team</td>
<td>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?</td>
</tr>
</tbody>
</table>
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
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
Cybersecurity Workforce Opportunities

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

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

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
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


- 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”
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*
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?**
34th Annual FISSEA Conference

Morning Networking Break and Exhibitor Showcase

10:30am-11:00am ET

#FISSEA | nist.gov/fissea
Welcome Back!

Brooke Crisp
FISSEA Co-Chair
The Human Firewall: Innovative Approaches for HR in Cybersecurity Training

Ani Banerjee
Chief Human Resource Officer
KnowBe4
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!
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
- Difficulty enforcing protocols
- Insecure Wi-Fi networks
- 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

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

HR
Legal
IT / InfoSec
Any Questions?

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

Anita Nikolich
University of Illinois
Media Literacy and Gamification

FISSEA May 14, 2024
Anita Nikolich
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 steps below to ensure you are not a victim of phishing.

- Step 3
  Urgent Action
  Watch out for calls to action with a deadline or a supposed time-sensitive update.

- Step 4
  Spelling Errors
  Spelling errors and poor grammar can be a red flag. Be wary of emails that contain spelling errors or poorly written content.

- Step 5
  "From:" Address
  Be wary of emails that claim to come from a legitimate source, but whose "From" address is not verified.

- Step 6
  Personal Information
  Beware of emails that request personal information, such as your Social Security Number or credit card information.

SDH Communications

Follow these general steps everytime you receive an email to prevent being hacked by a phishing scheme.
Project Origins

Trust and Authenticity in Communications Systems
(2021)
Team Expertise

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

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

Existing Resources Aren’t Enough
Target Audience

Age: 60+

Has a phone or tablet

Plays single player games to:
  • Relax
  • Keep the mind sharp
  • Socialize
Many believe games help their mental sharpness/brain health.
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??
Talking and Listening to Users

Pickens County, SC Flea Market
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
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!
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
Early Testing with Users

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

*Facebook, Instagram, under false name

*More items to generate

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

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 a 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  Intuitive
Creative  Average
Satisfying  Exciting
Childish  Masculine
Sophisticated  Cheap
Violent  Accessible
Fun  Time-consuming
Boring  Friendly
Cute  Irrelevant
Repetitive  Serves no function
Interesting  Entertaining
Technical  Feminine
Stressful  Annoying
Creative  Engaging
Predictable  Basic
Cool

Doesn't understand the purpose of play or how it connects to learning about "identity theft & fraud."
Designing the Game: Unity Game Engine
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.
Designing the Game: Missions and Special Operations

Mission 2
Paris, France

Your Score
018
Fang's Score
012

Dossier

Requests a Briefing

Contracts

Play

Moves: 0
Best: 0

Dossier

Turns Left: 6
“Older folks need things to be simple, practical, hands-on.”

“Just because they are retired doesn’t mean they aren’t busy.”

Community Center Activities Director
DART Academy
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.
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
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
Thank You

Visit us at DartCollective.net
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
3 ways ChatGPT and AI will change cybersecurity forever

Keatran Evans
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
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? – 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.
How is ChatGPT different from Google?

Google

• Google searches through large databases and returns pages with content related to the search.
• It doesn’t actually “perform” or create anything.

ChatGPT

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

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, 1024):  # Scanning ports from 1 to 1023 (commonly used ports)
        # Check if port is open

if __name__ == '__main__':
    main()
```
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.
How ChatGPT can help security professionals
3 cybersecurity uses for ChatGPT

- Coming up with solutions **faster**
- **Learning** to use new cybersecurity tools
- **Writing** reports!
| KE | 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:

``` CSS
(i.p.addr == keatron.com && i.p.addr == fedex.com) || (i.p.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.
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
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.
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
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.
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
Building a Workforce Development plan for Artificial Intelligence

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

Al gives organizations a competitive edge to develop tip of the “spear technology.”

**HOWEVER!!**

Al solutions must align to initiatives/strategies.

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

<table>
<thead>
<tr>
<th>Digital transformation examples</th>
<th>Competitive benefit examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Org seeks change through digital technologies.</td>
<td></td>
</tr>
<tr>
<td>• Al is an attractive option.</td>
<td></td>
</tr>
<tr>
<td>• Al fulfills initiative objectives.</td>
<td>• Improving existing products and services.</td>
</tr>
<tr>
<td></td>
<td>• Fostering innovation.</td>
</tr>
<tr>
<td></td>
<td>• Streamlining processes.</td>
</tr>
<tr>
<td></td>
<td>• Generating renewed interest.</td>
</tr>
<tr>
<td></td>
<td>• Attracting new talent.</td>
</tr>
</tbody>
</table>
How do you segment people to train?

- Artificial Intelligence/Machine Learning Engineers
- Entry Level
- Decision Makers, Stakeholders, Project/Program Managers, and Users
Bloom's Taxonomy

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

**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.

**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.

**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.

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

**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.
### Examples: How Can AI affect the workplace

<table>
<thead>
<tr>
<th>Skill Enhancement:</th>
<th>Increased Automation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professionals are reskilling and upskilling to</td>
<td>Repetitive and routine tasks are being</td>
</tr>
<tr>
<td>work alongside AI systems, acquiring skills in</td>
<td>automated, freeing up human workers to</td>
</tr>
<tr>
<td>data analysis, AI programming, and understanding</td>
<td>focus on more creative and complex tasks.</td>
</tr>
<tr>
<td>AI ethics.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Job Roles:</th>
<th>Data-Driven Decision-Making:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI is creating new job roles related to AI</td>
<td>AI is facilitating data-driven decision-making, helping professionals</td>
</tr>
<tr>
<td>development, AI ethics, and AI maintenance.</td>
<td>make more informed choices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improved Efficiency:</th>
<th>Data Privacy and Ethics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Businesses and industries are using AI to</td>
<td>Regulations and ethical guidelines are being</td>
</tr>
<tr>
<td>optimize processes, reduce costs, and increase</td>
<td>developed to ensure responsible AI use and</td>
</tr>
<tr>
<td>efficiency.</td>
<td>protect privacy.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to address AI mastery/education

**Expert**

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

**Mid-Career Specialty Skills**

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

**Foundational**

Technical knowledge, critical thinking process, and ethical considerations

**Professional**

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

**Entry-Level Specialty Skills**

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

**Expert**

Technical knowledge, critical thinking process, and ethical considerations

**Foundational**

Technical knowledge, critical thinking process, and ethical considerations

**Professional**

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

**Entry-Level Specialty Skills**

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

**Expert**

Technical knowledge, critical thinking process, and ethical considerations

**Foundational**

Technical knowledge, critical thinking process, and ethical considerations

**Professional**

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

**Entry-Level Specialty Skills**

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

**Expert**

Technical knowledge, critical thinking process, and ethical considerations

**Foundational**

Technical knowledge, critical thinking process, and ethical considerations

**Professional**

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

**Entry-Level Specialty Skills**

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

**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.

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

**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.
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.
Artificial Intelligence learning pathway

<table>
<thead>
<tr>
<th>Foundational Concepts</th>
<th>Programming Fundamentals</th>
<th>Data Science Prerequisites</th>
<th>Vendor-Neutral Certification</th>
<th>Vendor-Specific Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI for Business Professionals</td>
<td>Introduction to Programming with Python (PCEP)</td>
<td>Using Data Science Tools in Python Certified Data Science Practitioner</td>
<td>Certified AI Practitioner</td>
<td>AWS Certified Machine Learning Specialty Microsoft Certified: Azure Data Scientist Associate</td>
</tr>
</tbody>
</table>

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.
Summary
Define Training Goals

Identify the specific goals of the training plan and how they align with the overall AI objectives of the organization.

Identify Training Audience

Determine who will be receiving the training and what the current level of knowledge is.

Develop Training Content

Use content that is tailored to the needs of the audience that covers appropriate aspects of artificial intelligence.

Select Training Delivery

Choose an appropriate delivery method for training: online, in person, or a combination of both.

Implement Training Plan

Put the plan into action by scheduling sessions, assigning trainers, and providing learning materials.

Evaluate Training Results

Measure the effectiveness of the training plan by assessing participant feedback and performance.

Building a Workforce Development plan for Artificial Intelligence
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
34th Annual FISSEA Conference

Afternoon Networking Break and Exhibitor Showcase

2:45pm-3:15pm ET

#FISSEA | nist.gov/fissea
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
Cyber Safety is Patient Safety: Navigating Cybersecurity Risks through Enterprise Risk Management

2024
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.
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.

- Deployed EDR agents to all endpoints
- Took the EMR offline
- Severed connections to affiliates and other partners
- Cut off all internet and other access both to and from the health system
- Blocked traffic at internal segments
- Notified federal local law enforcement
### 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
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 silos.
- 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 cornerstone 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
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
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

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

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

**Insider Accidental or Malicious Data Loss**
This training provides an overview of insider data loss accidents and ones with malicious intent.

**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.

**Attacks Against Connected Medical Devices**
This training provides an overview of the importance of securing network connected medical devices.

**Loss or Theft of Equipment or Data**
This training provides an overview of best practices on securing equipment and data.
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.

**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.

**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.

**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](http://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

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 item 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
Questions?

Visit Our Website
405d.hhs.gov

Do you follow us on social media?
Check us at 405d.hhs.gov
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

#FISSEA | nist.gov/fissea
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 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**
  - 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**

---

All Users

Privileged Access Account Holders

Significant Cybersecurity and/or Privacy Responsibilities

Learning Program Audience Types
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
Thank you!
NIST Cybersecurity Framework 2.0
Overview & Updates

Amy Mahn
Applied Cybersecurity Division
April 2024
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
“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?

COMMUNITY ENGAGEMENT

2022

- February 2022 NIST Cybersecurity RFI
- June 2022 RFI Analysis
- September 2022 Workshop Analysis
- April 2022 Comments Received

2023

- February 2023 Workshop #2
- Working Sessions
- January 2023 Concept Paper
- April 2023 Core Draft
- March 2023 Comments Received
- November 2023 Comments Received

2024

- September 19-20, 2023 Workshop #3
- August 2023 Draft 2.0
- February 2024 CSF 2.0

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.
Suite of Resources Snapshot

NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE

Navigating NIST’s CSF 2.0 Quick Start Guides

Resource and Overview Guide

Quick Start | Small Business
Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

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.

Quick Start | Enterprise Risk Management
How ERM practitioners can leverage the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

The NIST Cybersecurity Framework (CSF) 2.0

Institution’s cybersecurity risk management strategy, expectations, and policy

Security risk to the organization

Cybersecurity incident

Security attacks and compromises

Cybersecurity and Privacy Reference Tool (CPRT)

Download Information Reference in the Case

Rational Institute of Standards and Technology
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](http://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
STAY IN TOUCH

CONTACT US

nist.gov/cyberframework  @NISTcyber
Email us: cyberframework@nist.gov
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAU@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