Federal Information Security Educators (FISSEA)

Fall Forum

September 30, 2025

1:00pm – 2:30pm ET

#FISSEA | nist.gov/fissea

NIST | FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Notes and Reminders

Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.

Webinar Recording: This webinar and the engagement tools will be recorded. An archive will be available at www.nist.gov/fissea.

CE/CPE credits: The CEU form will be available on the event page after the event.

Welcome and Opening Remarks

Latha Reddy

FISSEA Co-Chair
Vice President and Director of Technology and Cybersecurity
Spire Investment Partners, LLC

Joyce Mui

FISSEA Co-Chair
National Institute of Standards and Technology

Danielle Santos

Deputy Director of NICE
National Institute of Standards and Technology

Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@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
Email fissea@nist.gov

SAVE THE DATE

Federal Information Security Educators (FISSEA) Winter Forum

February 10, 2026

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Cybersecurity Awareness Month (October) Updates

Jennifer Cook

Senior Director of Marketing
National Cybersecurity Alliance

NATIONAL CYBERSECURITY ALLIANCE

Cybersecurity Awareness Month

2025

ABOUT US

We Empower a More Secure, Interconnected World.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.

CYBERSECURITY AWARENESS MONTH

convene

Data Privacy Week

AI FOOLS Stay Sharp!

CyberSecure MY BUSINESS

NEXT TIME KUBIKLE

SEE YOURSELF IN CYBER

About Cybersecurity Awareness Month

Began	When	Hosted by	Audience	Partners
2004	Oct 1 - 31	NCA and CISA	Everyone!	Public and Private Sector Organizations

Goal

Educate the general population about digital security and empower everyone to take actionable steps to protect their personal data

Objectives

- Ensure organizations have the resources and communications they need to talk to their employees and customers about staying safe online
- Collaborate between government and private industry to raise awareness

https://staysafeonline.org/programs/cybersecurity-awareness-month/

2024 Results

3,800 registrants

Organizations and individuals registered as Champions

27 sectors

Champions came from 27 different sectors, primarily technology, higher education, government and financial services.

18,550 social media users

Unique authors posted about the month on social media.

107 countries

Number of countries represented by registered Champions.

58 million people

Estimated reach of all Champion organizations.

45,612 posts

Posts used the hashtag #CybersecurityAwarenessMonth

Theme: Stay Safe Online

The Core 4

01 Use strong passwords and a password manager

02 Turn on multifactor authentication

03 Update your software

04 Recognize and report **scams**

Tone of Voice

- ☑ Simple (no jargon)
- ☑ Approachable and empathetic
- ☑ Back to basics
- ☑ Empowering

Why

From our research, we've learned...

46%

of people say trying to stay staying secure online is **frustrating**

44%

say security is **intimidating**

40%

say information on how to be secure is **confusing**

Source: Oh Behave! The Cybersecurity Attitudes and Behaviors Report 2024

Become a Champion

Receive a toolkit of free materials exclusively for registered Champions

- A campaign guide and sample content calendar
- Tip sheets on
  - Passwords
  - Password managers
  - Multifactor authentication
  - Software updates
  - Scams and Phishing
- Social media graphics
- Social media posts

- Four Animated videos
- Sample trivia questions
- Sample copy for a
  - Newsletter
  - Press release
  - Senior leadership announcement
  - Official proclamation
- Cybersecurity Awareness Month logos
- A 2025 Champion badge

https://www.staysafeonline.org/cybersecurity-awareness-month#champion

Kick-off Event Tomorrow!

Stay up to date on upcoming events:
https://www.staysafeonline.org/events

WEBINAR

Cybersecurity Awareness Month Kick-off

→ Wednesday, October 1
1 pm ET / 10 am PT

3 Create Your Campaign

How Partners Participated in 2024

Champions participated in the campaign a variety of ways, including:

- **Sending out an employee email (60%)**
- **Posting a blog or article (48%)**
- **Posting about the month on social media platforms (45%)**
  - ***Use #CybersecurityAwarenessMonth***
- **Holding a training or event for employees (40%)**

Sample Content Calendar

Late September: Pre-Promotions

- Let your audience know what to expect in October

Week 1: October 1 – 3: Cybersecurity Awareness Month Kick-off – Stay Safe Online

- Send internal and external announcements
- Launch a competition or phishing simulations

Week 2: October 6 – 10: Use strong passwords and a password manager

- Share toolkit resources on passwords
- Host an event

Week 3: October 13 – 17: Turn on multifactor authentication

- Share toolkit resources on MFA
- Add MFA how-tos to your internal portal or newsletter

Sample Content Calendar

Week 4: October 20 – 24: Update your software

- Share toolkit resources on updates
- Celebrate Cybersecurity Career Week

Week 5: October 27 – 31: Recognize and report scams

- Share toolkit resources on scams
- Educate employees on internal reporting tool

Wrap-up: November 3 - 7

- Send an email highlighting your activities, results, and successes.
- Recap best practices learned throughout the month.

CYBERSECURITY AWARENESS MONTH

Then & Now

SAFETY ADVICE FOR OLDER ADULTS AND THEIR CARETAKERS

TOPICS COVERED

- Scams and fraud
- Multifactor authentication
- Passwords and password managers
- Software updates

TYPES OF CONTENT

- An online workbook with physical copies available to order
- How-to videos on setting up cybersecurity best practices on popular platforms
- Articles specifically for older adults and their caretakers
- Hands-on live workshops upon request

thenandnow.info

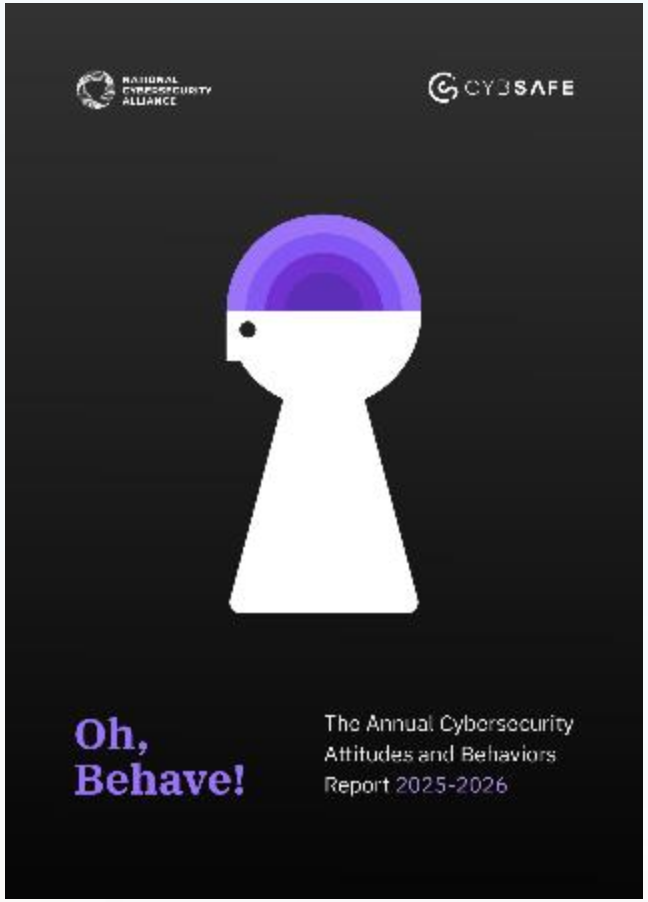
CYBERSECURITY AWARENESS MONTH

Oh, Behave! 2025

Out Today!

Surveying

- United States
- United Kingdom
- Germany
- Australia
- India
- Brazil
- Mexico



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2025-2026

https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2025

WEBSITE

StaySafeOnline.org

X

@staysafeonline

FACEBOOK

/staysafeonline

LINKEDIN

/national-cyber-security-alliance

INSTAGRAM

StaySafeOnlineNCA

YOUTUBE

@StaySafeOnlineNCA

EMAIL

info@staysafeonline.org

NATIONAL
CYBERSECURITY
ALLIANCE

FISSEA Fifteen: A Collaborative Discussion on Cybersecurity Awareness Activities

Susan Hansche

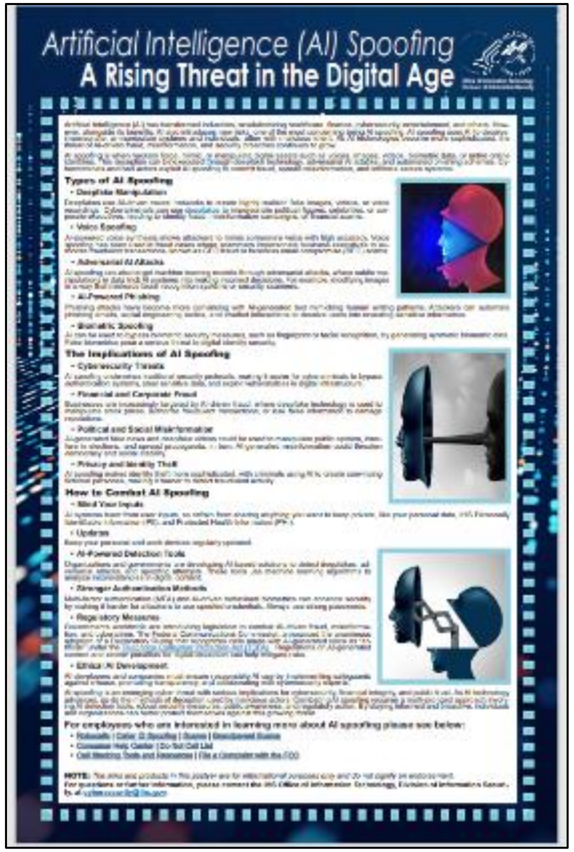
Training Manager
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FISSEA Awareness and Training Contest

- Poster or Brochure
- Website
- Multimedia (Blog, Video, Audio, Podcast, etc.)
- Email campaign and/or newsletter
- Miscellaneous – awareness materials, such as note pads, buttons, stickers
- Innovation Solution

FISSEA Contests & Awards | NIST

Past Winners - Poster or Brochure



Artificial Intelligence (AI) Spoofing
A Rising Threat in the Digital Age

[illegible]

Types of AI Spoofing

- Deepfake Manipulation

[illegible]

- Voice Spoofing

[illegible]

- Adversarial AI Attacks

[illegible]

- AI-Powered Phishing

[illegible]

- Biometric Spoofing

[illegible]

The Implications of AI Spoofing

- Cybersecurity Threats

[illegible]

- Financial and Corporate Fraud

[illegible]

- Political and Social Misinformation

[illegible]

- Privacy and Identity Theft

[illegible]

How to Combat AI Spoofing

- Mind Your Inputs

[illegible]

- Updates

Keep your personal and work devices regularly updated.

- AI-Powered Detection Tools

[illegible]

- Stronger Authentication Methods

[illegible]

- Regulatory Measures

[illegible]

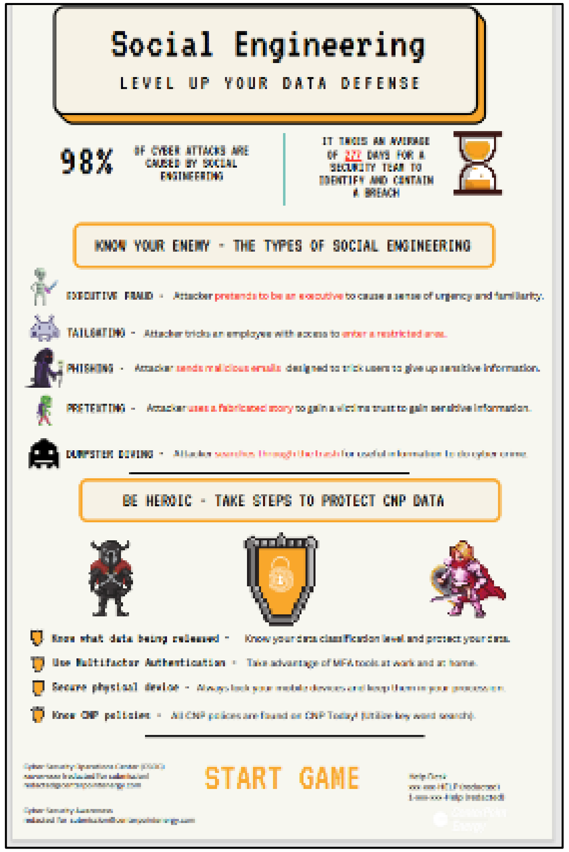
- Ethical AI Development

[illegible]

For employees who are interested in learning more about AI spoofing please see below:

[illegible]

2024 – Indian Health Services



Social Engineering
LEVEL UP YOUR DATA DEFENSE

98% OF CYBER ATTACKS ARE CAUSED BY SOCIAL ENGINEERING

IT TAKES AN AVERAGE OF 277 DAYS FOR A SECURITY TEAM TO IDENTIFY AND CONTAIN A BREACH

KNOW YOUR ENEMY - THE TYPES OF SOCIAL ENGINEERING

EXECUTIVE FRAUD - Attacker pretends to be an executive to cause a sense of urgency and familiarity.

TAILGATING - Attacker tricks an employee with access to enter a restricted area.

PHISHING - Attacker sends malicious emails designed to trick users to give up sensitive information.

PRETEXTING - Attacker uses a fabricated story to gain a victims trust to gain sensitive information.

DUMPSTER DIVING - Attacker searches through the trash for useful information to do cyber crime.

BE HEROIC - TAKE STEPS TO PROTECT CNP DATA

Know what data being released - Know your data classification level and protect your data.

Use Multifactor Authentication - Take advantage of MFA tools at work and at home.

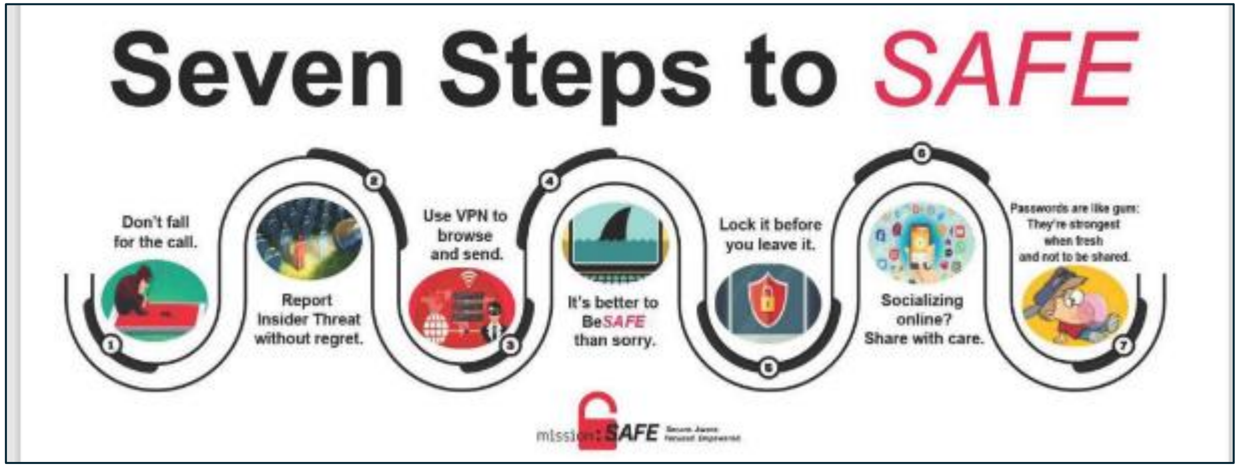
Secure physical device - Always lock your mobile devices and keep them in your possession.

Know CNP policies - All CNP polices are found on CNP Today! (Utilize key word search).

START GAME

[illegible]

2023 – CenterPoint Energy



Seven Steps to *SAFE*

1 Don't fall for the call.

2 Report Insider Threat without regret.

3 Use VPN to browse and send.

4 It's better to BeSAFE than sorry.

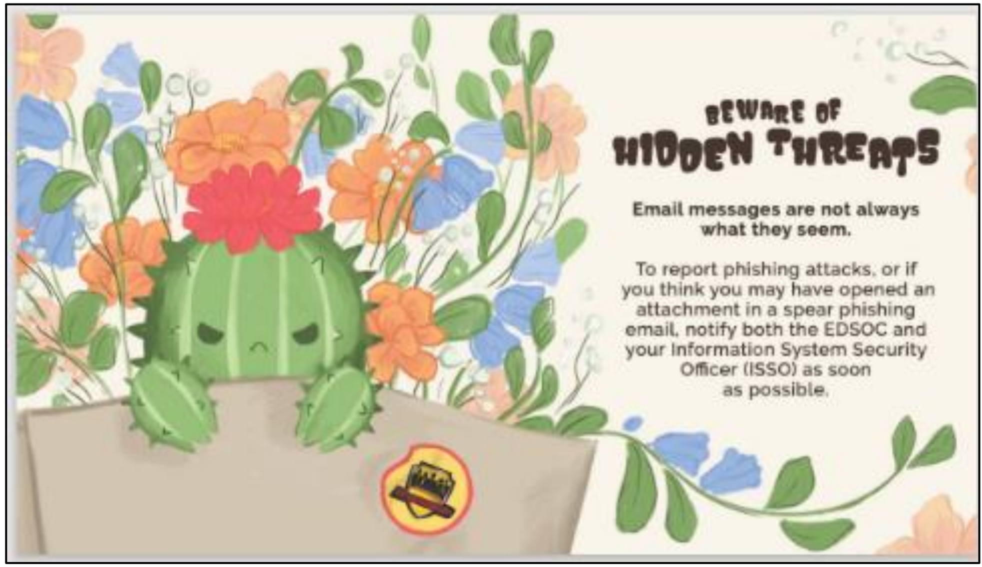
5 Lock it before you leave it.

6 Socializing online? Share with care.

7 Passwords are like gum: They're strongest when fresh and not to be shared.

mission:SAFE

2022 – LabCorp



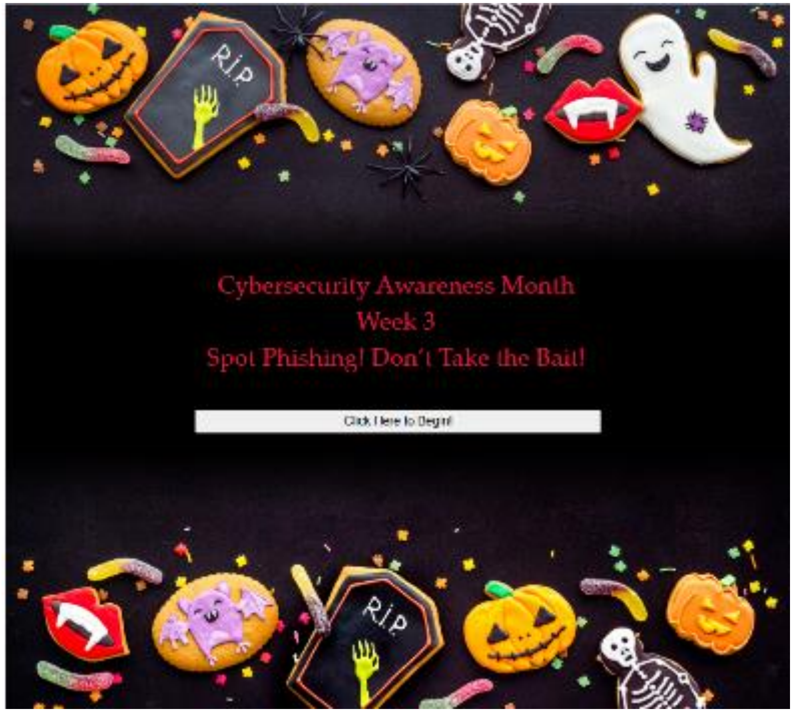
BEWARE OF HIDDEN THREATS

Email messages are not always what they seem.

To report phishing attacks, or if you think you may have opened an attachment in a spear phishing email, notify both the EDSOC and your Information System Security Officer (ISSO) as soon as possible.

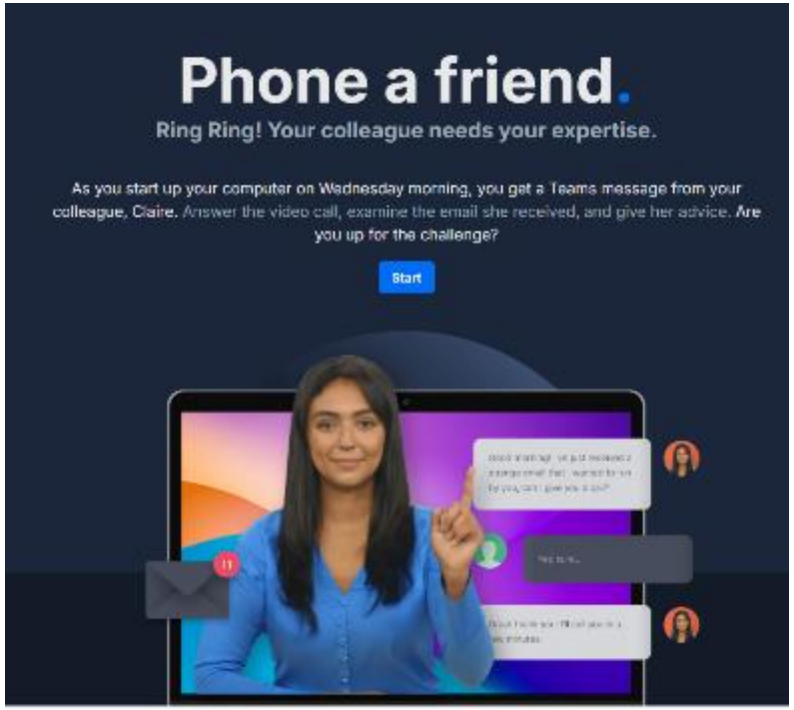
2023 – Dept. of Education – Peoples Choice Award

Past Winners - Website



Cybersecurity Awareness Month
Week 3
Spot Phishing! Don't Take the Bait!

2024 – Indian Health Services



Phone a friend.

Ring Ring! Your colleague needs your expertise.

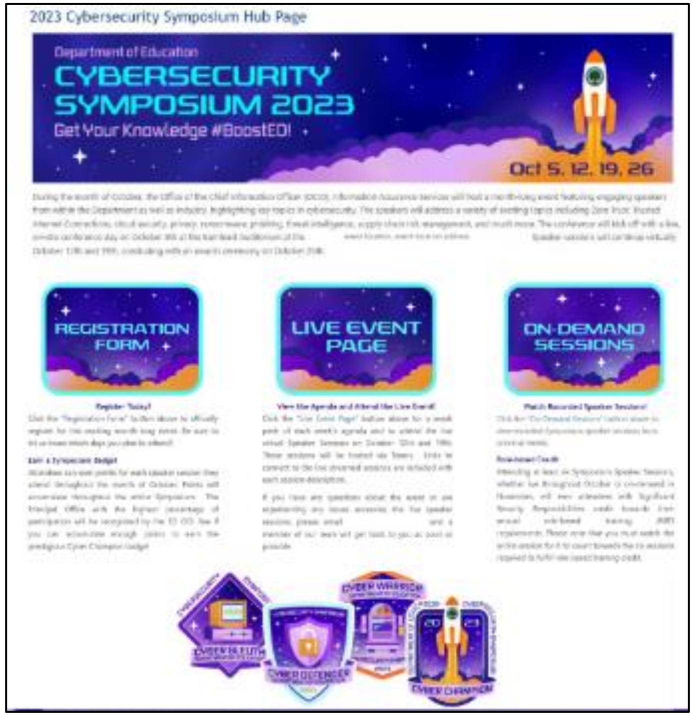
As you start up your computer on Wednesday morning, you get a Teams message from your colleague, Claire. Answer the video call, examine the email she received, and give her advice. Are you up for the challenge?

Good morning! I've just received a strange email that I wanted to run by you, can I give you a call?

Yes sure...

Great, thank you! I'll call you in a few minutes.

2023 – CenterPoint Energy



2023 Cybersecurity Symposium Hub Page

Department of Education
CYBERSECURITY SYMPOSIUM 2023
Get Your Knowledge #BoostED!
Oct 5, 12, 19, 26

During the month of October, the Office of the Chief Information Officer (OCIO), Information Assurance Services will host a month-long event featuring engaging speakers from within the Department as well as industry, highlighting key topics in cybersecurity. The speakers will address a variety of exciting topics including Zero Trust, Trusted Internet Connections, cloud security, privacy, ransomware, phishing, threat intelligence, supply chain risk management, and much more. The conference will kick off with a live, onsite conference day on October 5th at the [illegible] Auditorium at the [illegible] Speaker sessions will continue virtually October 12th and 19th, concluding with an awards ceremony on October 26th.

Register Today!

Click the "Registration Form" button above to officially register for this exciting month-long event. Be sure to let us know which days you plan to attend!

Earn a Symposium Badge

Attendees can earn points for each speaker session they attend throughout the month of October. Points will accumulate throughout the entire Symposium. The Principal Office with the highest percentage of participation will be recognized by the ED CIO. See if you can accumulate enough points to earn the prestigious Cyber Champion badge!

View the Agenda and Attend the Live Event!

Click the "Live Event Page" button above for a sneak peek of each week's agenda and to attend the live virtual Speaker Sessions on October 12th and 19th. These sessions will be hosted via Teams. Links to connect to the live streamed sessions are included with each session description.

If you have any questions about the event or are experiencing any issues accessing the live speaker sessions, please email [illegible] and a member of our team will get back to you as soon as possible.

Watch Recorded Speaker Sessions!

Click the "On-Demand Sessions" button above to view recorded Symposium speaker sessions from [illegible].

Role-based Credit

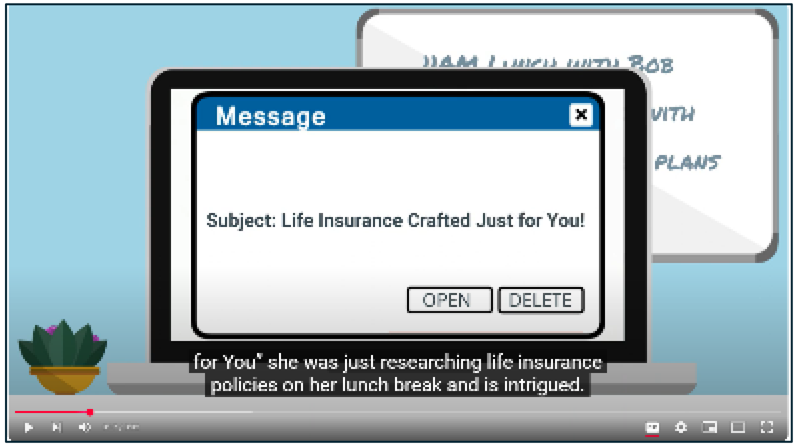
Attending at least six Symposium Speaker Sessions, whether live throughout October or on-demand in November, will earn attendees with Significant Security Responsibilities credit towards their annual role-based training (RBT) requirements. Please note that you must watch the entire session for it to count towards the six sessions required to fulfill role-based training credit.

2023 – Dept of Education Peoples Choice Award

Past Winners - Multimedia

2024– Cybersecurity Today TV Show (Securible)

2023– Federal Retirement Thrift Investment Board (FRTIB) 3-minute video



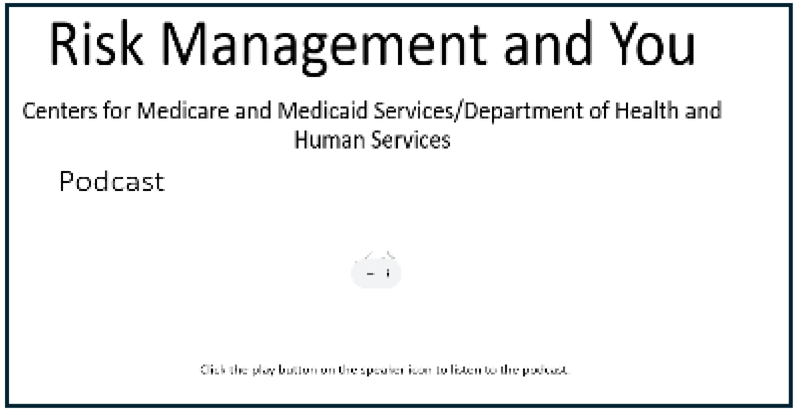
Subject: Life Insurance Crafted Just for You!

for You" she was just researching life insurance policies on her lunch break and is intrigued.

2023– Office of Personnel Management 3-minute video

The Jennifer Reacts Blog!

2023– Indian Health Services Blog



Risk Management and You

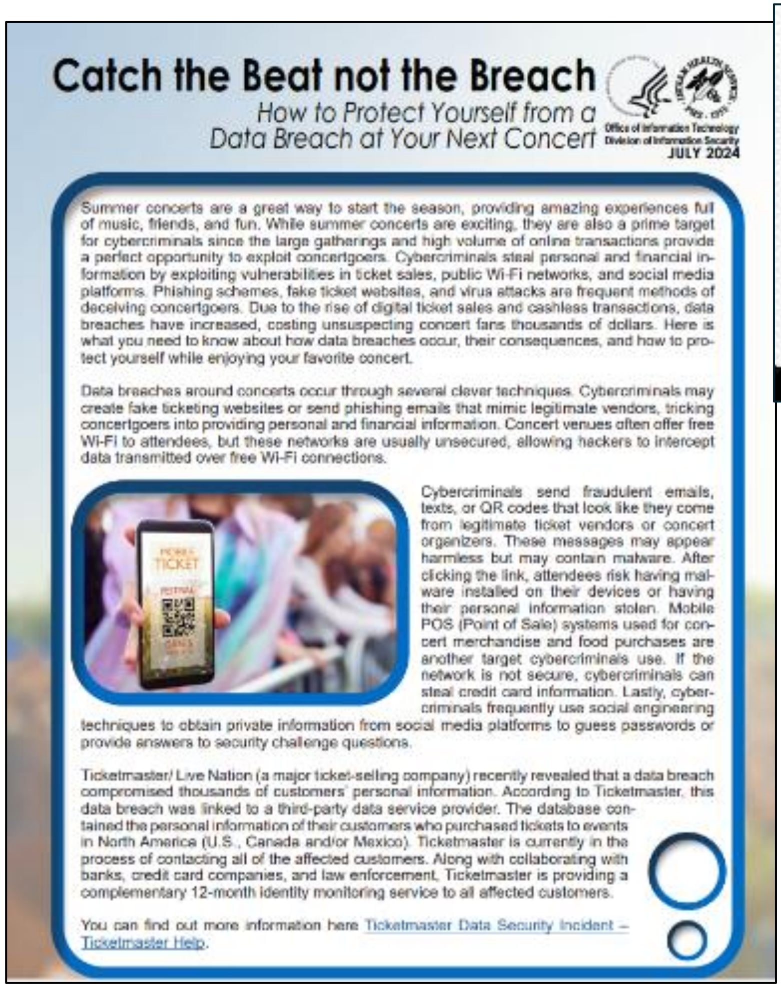
Centers for Medicare and Medicaid Services/Department of Health and Human Services

Podcast

Click the play button on the speaker icon to listen to the podcast.

2022– Centers for Medicare and Medicaid Podcast – Peoples Choice Award

Past Winners - Email campaign and/or newsletter, Innovative, Miscellaneous



Catch the Beat not the Breach

How to Protect Yourself from a Data Breach at Your Next Concert

Office of Information Technology
Division of Information Security
JULY 2024

Summer concerts are a great way to start the season, providing amazing experiences full of music, friends, and fun. While summer concerts are exciting, they are also a prime target for cybercriminals since the large gatherings and high volume of online transactions provide a perfect opportunity to exploit concertgoers. Cybercriminals steal personal and financial information by exploiting vulnerabilities in ticket sales, public Wi-Fi networks, and social media platforms. Phishing schemes, fake ticket websites, and virus attacks are frequent methods of deceiving concertgoers. Due to the rise of digital ticket sales and cashless transactions, data breaches have increased, costing unsuspecting concert fans thousands of dollars. Here is what you need to know about how data breaches occur, their consequences, and how to protect yourself while enjoying your favorite concert.

Data breaches around concerts occur through several clever techniques. Cybercriminals may create fake ticketing websites or send phishing emails that mimic legitimate vendors, tricking concertgoers into providing personal and financial information. Concert venues often offer free Wi-Fi to attendees, but these networks are usually unsecured, allowing hackers to intercept data transmitted over free Wi-Fi connections.

Cybercriminals send fraudulent emails, texts, or QR codes that look like they come from legitimate ticket vendors or concert organizers. These messages may appear harmless but may contain malware. After clicking the link, attendees risk having malware installed on their devices or having their personal information stolen. Mobile POS (Point of Sale) systems used for concert merchandise and food purchases are another target cybercriminals use. If the network is not secure, cybercriminals can steal credit card information. Lastly, cybercriminals frequently use social engineering techniques to obtain private information from social media platforms to guess passwords or provide answers to security challenge questions.

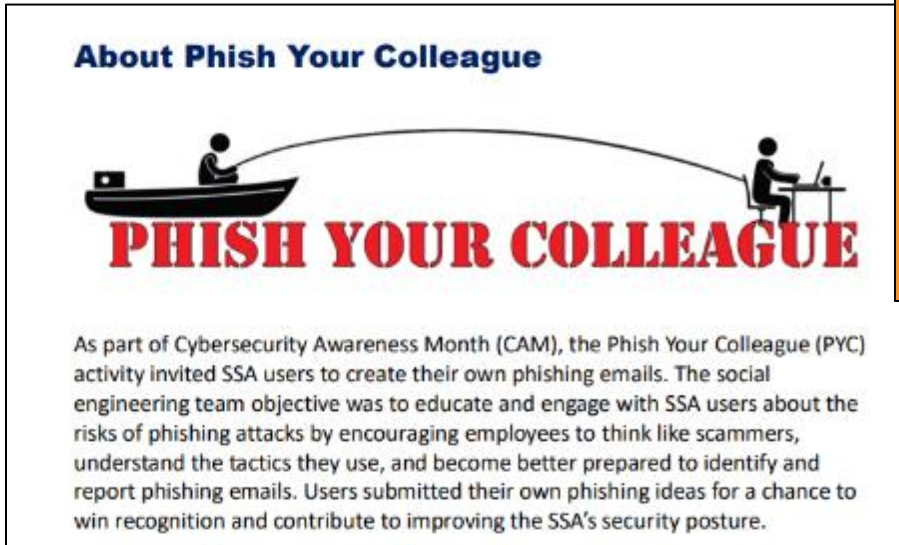
Ticketmaster/ Live Nation (a major ticket-selling company) recently revealed that a data breach compromised thousands of customers' personal information. According to Ticketmaster, this data breach was linked to a third-party data service provider. The database contained the personal information of their customers who purchased tickets to events in North America (U.S., Canada and/or Mexico). Ticketmaster is currently in the process of contacting all of the affected customers. Along with collaborating with banks, credit card companies, and law enforcement, Ticketmaster is providing a complementary 12-month identity monitoring service to all affected customers.

You can find out more information here Ticketmaster Data Security Incident – Ticketmaster Help.

2024 – Indian Health Services

President's Cup 7 Cybersecurity Competition

2024 – Cybersecurity & Infrastructure Agency

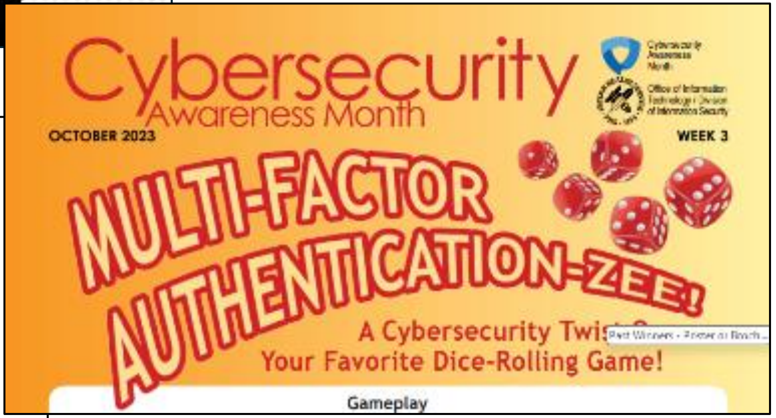


About Phish Your Colleague

PHISH YOUR COLLEAGUE

As part of Cybersecurity Awareness Month (CAM), the Phish Your Colleague (PYC) activity invited SSA users to create their own phishing emails. The social engineering team objective was to educate and engage with SSA users about the risks of phishing attacks by encouraging employees to think like scammers, understand the tactics they use, and become better prepared to identify and report phishing emails. Users submitted their own phishing ideas for a chance to win recognition and contribute to improving the SSA's security posture.

2023 – Social Security Administration



Cybersecurity Awareness Month

OCTOBER 2023

Cybersecurity Awareness Month

Office of Information Technology Division of Information Security

WEEK 3

MULTI-FACTOR AUTHENTICATION-ZEE!

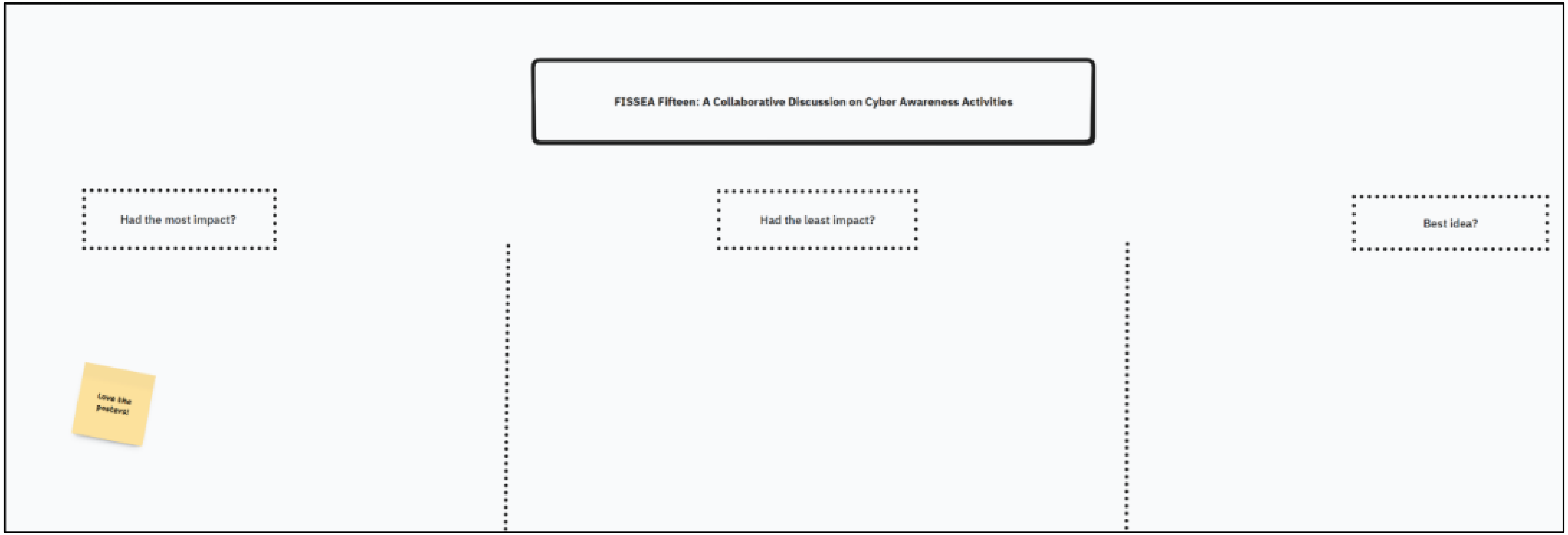
A Cybersecurity Twis

Your Favorite Dice-Rolling Game!

Gameplay

2023 – Indian Health Services

Your Turn – Let’s Share Some Thoughts



FISSEA Fifteen: A Collaborative Discussion on Cyber Awareness Activities

Had the most impact?

Love the posters!

Had the least impact?

Best idea?

Reducing Risk Through Awareness and Training

Aman Bhardwaj

SOC Analyst
Cydeo

Reducing Risk Through Awareness and Training

Empowering People: Reducing Risk Through Cybersecurity Awareness and Training

Aman Bhardwaj | SOC Analyst

Why Awareness Matters

- 📊 **Did You Know?**
- Verizon 2023 DBIR: ~74% of breaches involve the human element.
- Verizon 2024 DBIR: ~68% of breaches tied to employee mistakes, phishing, or misuse.
- IBM Security study: ~95% of cyber incidents trace back to human error (historical).

68%+ of incidents start with human error (phishing, weak passwords, misconfigurations).

Technology alone cannot stop threats.

Humans are the first line of defense.

Sources: Verizon Data Breach Investigations Report (DBIR) 2023 & 2024; IBM Security Report

NIST’s Perspective

Aligned with NIST Cybersecurity Framework (CSF):

Identify → Protect → Detect → Respond → Recover

Awareness & Training (PR.AT) is foundational under 'Protect'

Source : NIST Cybersecurity Framework (CSF).

Awareness & Training Comparison: NIST, ISO, GDPR, HIPAA

Framework	Awareness & Training Requirements
NIST (SP 800-53 / CSF)	Requires regular security awareness & role-based training; ongoing updates as threats evolve.
ISO 27001	Mandatory information security awareness programs; training integrated into ISMS; competence documented.
GDPR (Art. 39, 47)	Requires awareness for staff handling personal data; training to ensure compliance with privacy principles.
HIPAA (164.308(a)(5))	Security awareness & training program required for all workforce members; includes reminders & incident procedures.

Sources: NIST Special Publication 800-53; ISO/IEC 27001; GDPR Articles 39 & 47; HIPAA Security Rule 45 CFR § 164.308

Common Human Risk Factors

Weak or reused passwords easily guessable, not rotated regularly

Clicking on suspicious links falling for phishing or social engineering attempts

Sharing sensitive information accidentally disclosing data via email or chat

Lack of incident reporting employees ignore or fail to escalate suspicious activity

Shadow IT using unauthorized apps or tools that bypass security controls

Overconfidence assuming 'it won’t happen to me' and ignoring security best practices

Building an Effective Program

Risk Assessment Spot the biggest human risks (phishing, weak passwords, poor reporting).

Training Curriculum Build role-based, scenario-driven learning everyone can relate to.

Delivery Methods

Mix it up: e-learning, short videos, phishing simulations, team sessions.

Leadership
Buy-in Culture starts at the top; leaders should model secure behavior.

Measure & Improve Track click rates, reporting frequency, and response times; adapt as needed.

Embedding Training in Culture

Gamify training use leaderboards, badges, or small rewards for spotting phishing emails.

Make it part of daily work secure actions (like MFA or reporting) should feel natural.

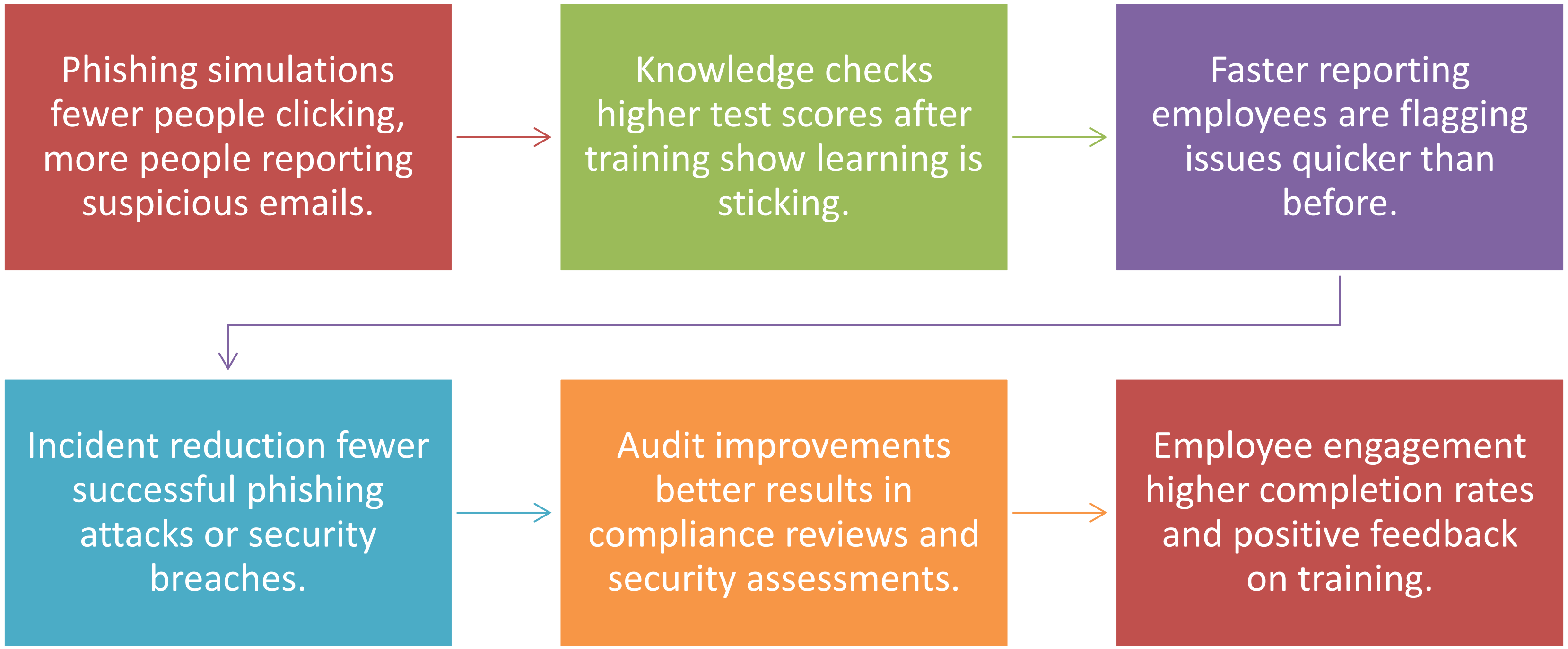
Recognize the good celebrate employees who practice strong security habits.

Keep communication simple share quick tips via newsletters, intranet, or team huddles.

Empower peer champions security ambassadors in teams can lead by example.

Listen and adapt create feedback channels so staff feel involved in improving security.

Measuring Success



Phishing simulations fewer people clicking, more people reporting suspicious emails.

Knowledge checks higher test scores after training show learning is sticking.

Faster reporting employees are flagging issues quicker than before.

Incident reduction fewer successful phishing attacks or security breaches.

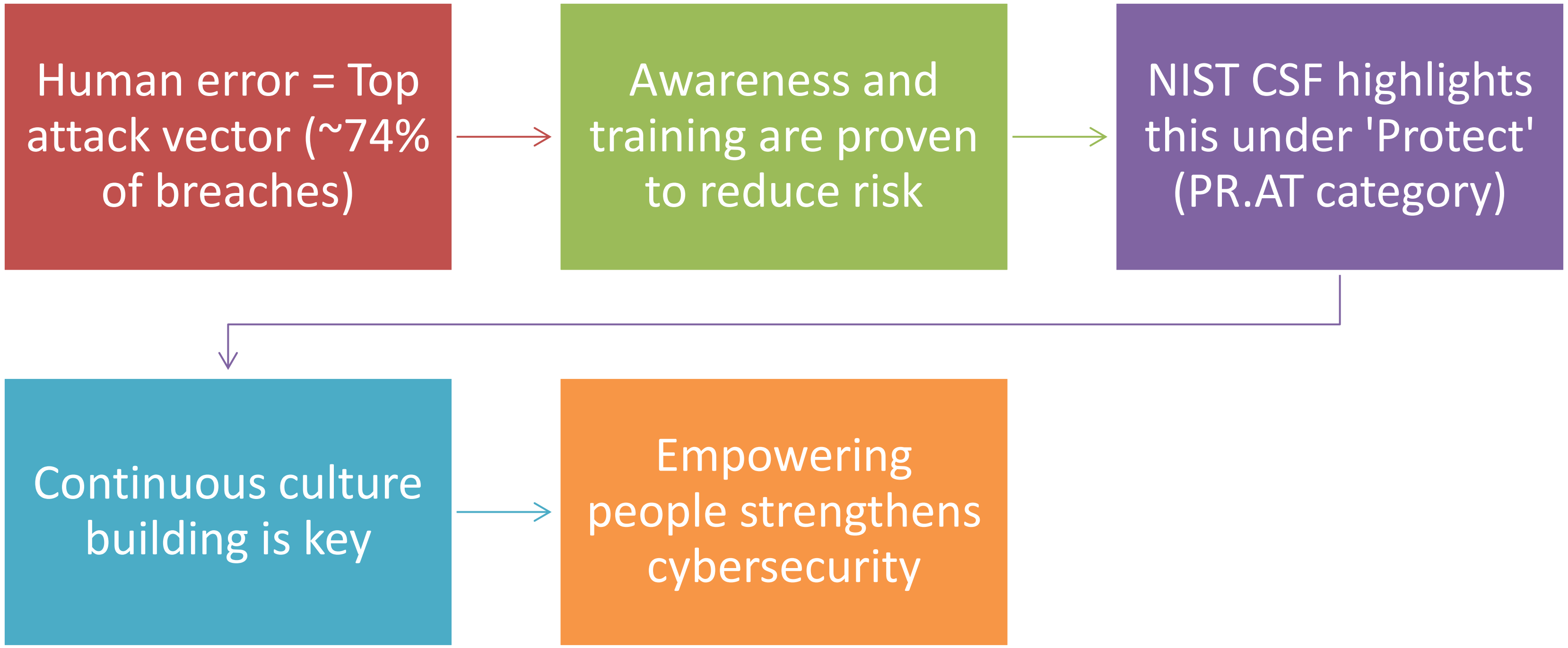
Audit improvements better results in compliance reviews and security assessments.

Employee engagement higher completion rates and positive feedback on training.

Example Healthcare Phishing Defense

- A mid-sized healthcare provider faced repeated phishing attempts targeting employees.
- Introduced quarterly phishing simulations and mandatory awareness refreshers.
- Staff trained to spot red flags (suspicious links, urgent tone, sender mismatches).
- Within 6 months:
- Reporting rate improved by 45%
- Successful phishing incidents reduced by 60%
- Result: Strengthened patient data protection and improved compliance posture.

Key Takeaways



Human error = Top attack vector (~74% of breaches)

Awareness and training are proven to reduce risk

NIST CSF highlights this under 'Protect' (PR.AT category)

Continuous culture building is key

Empowering people strengthens cybersecurity

Sources: Verizon Data Breach Investigations Report (DBIR) 2023 & 2024; IBM Security Report

Thank You

Cybersecurity is everyone’s responsibility.

Aman Bhardwaj | SOC Analyst
aman.bhardwaj1231@gmail.com

Stop the Hacker – A Cybersecurity Awareness Game

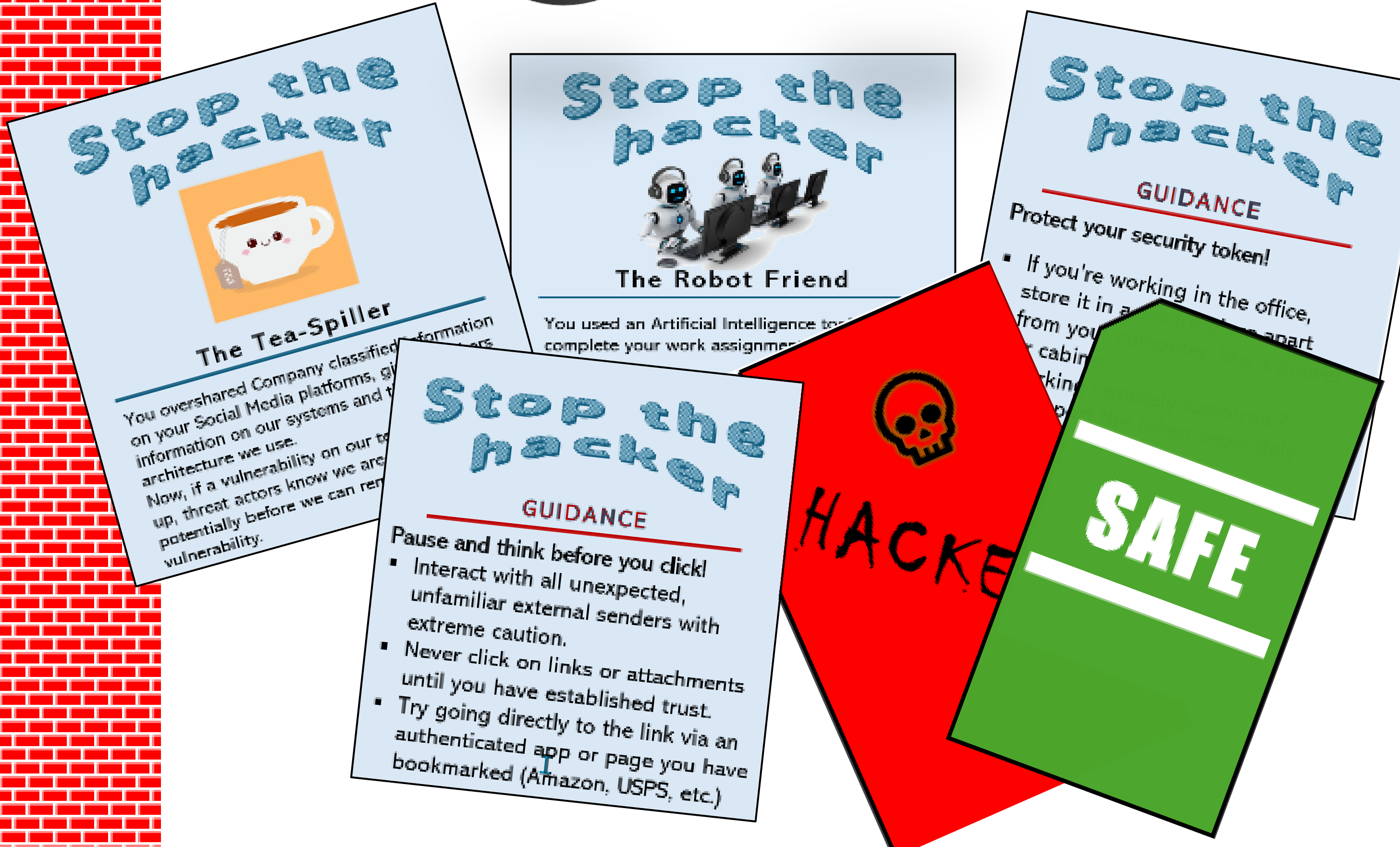
Sarae Winnicki

Federal Reserve Bank of New York

Ashley Smith

Federal Reserve Bank of New York

Stop the hacker:
A Cybersecurity Awareness Game



The Tea-Spiller

You overshared Company classified information on your Social Media platforms, gi information on our systems and t architecture we use.
Now, if a vulnerability on our te up, threat actors know we are potentially before we can rem vulnerability.

The Robot Friend

You used an Artificial Intelligence to complete your work assignmen

GUIDANCE

Protect your security token!

- If you're working in the office, store it in a apart from you cabin rkin

GUIDANCE

Pause and think before you click!

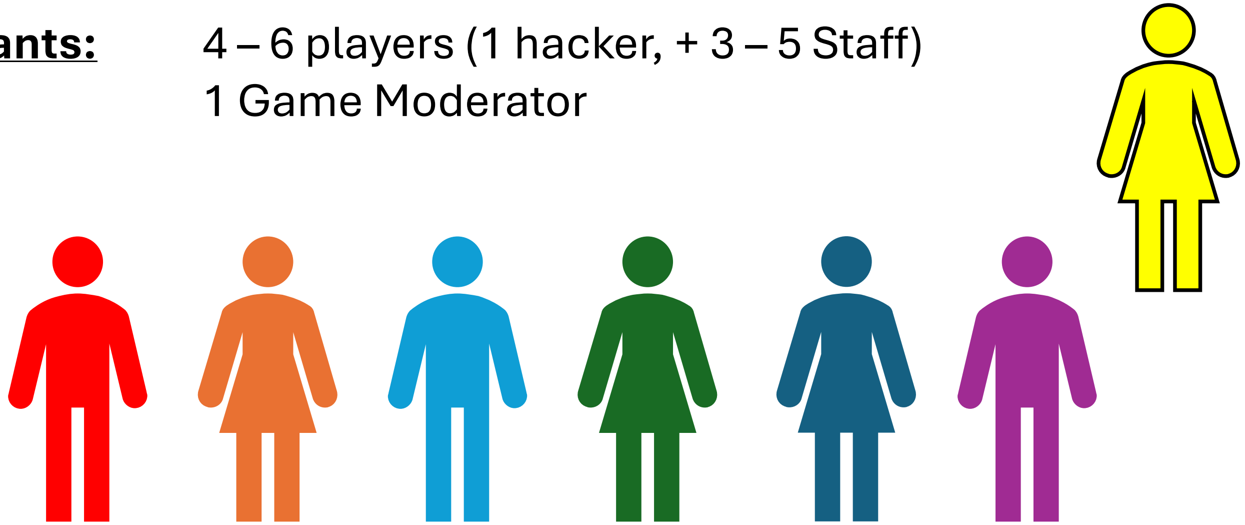
- Interact with all unexpected, unfamiliar external senders with extreme caution.
- Never click on links or attachments until you have established trust.
- Try going directly to the link via an authenticated app or page you have bookmarked (Amazon, USPS, etc.)

Stop the hacker

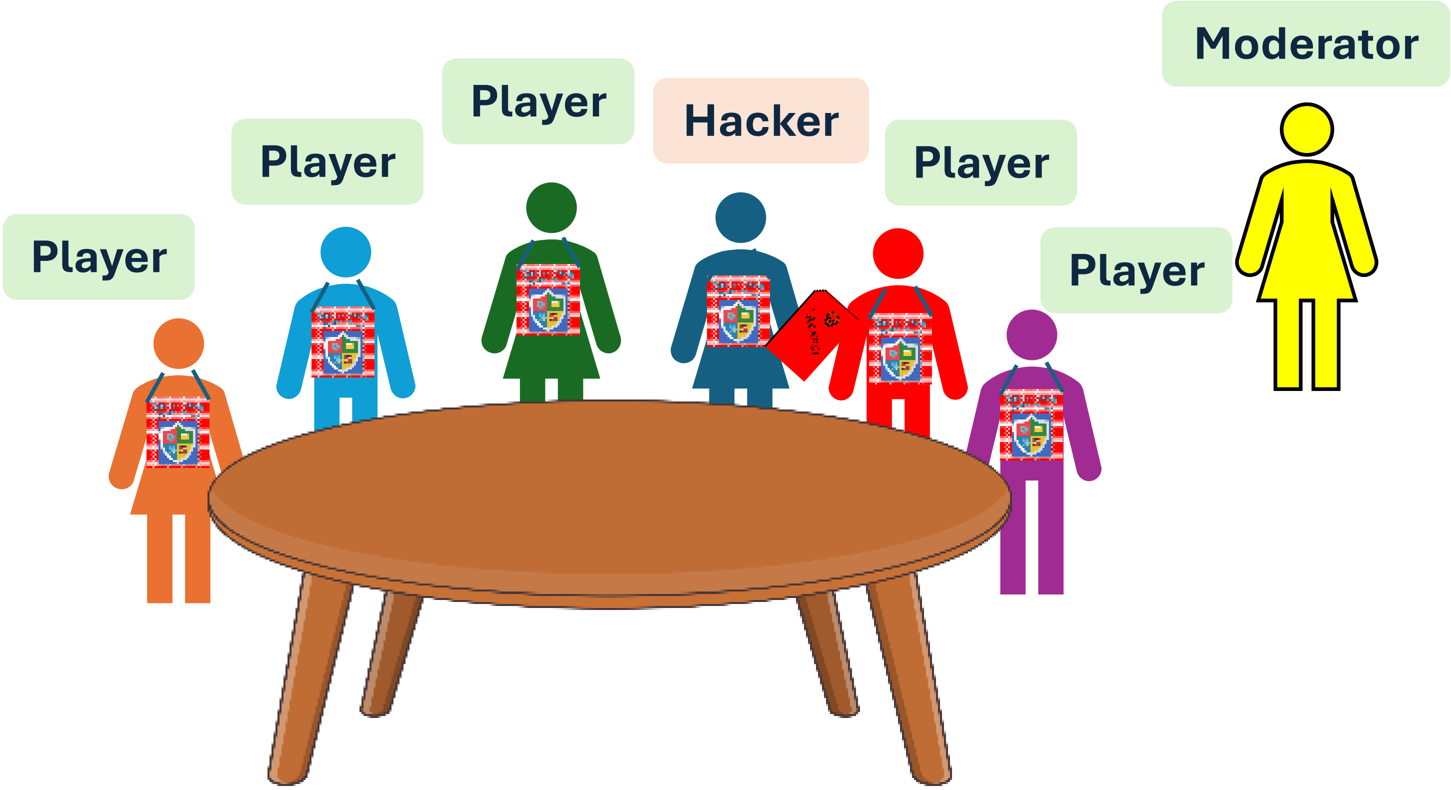
Overview: Each player is targeted by the hacker and must choose the correct solution to prevent a successful exploitation.

Purpose: By playing ***Stop the hacker***, players show their knowledge of cybersecurity best practices where user behavior protects the organization. The game will re-iterate the impact of user behavior to protect the organization from cyber threats.

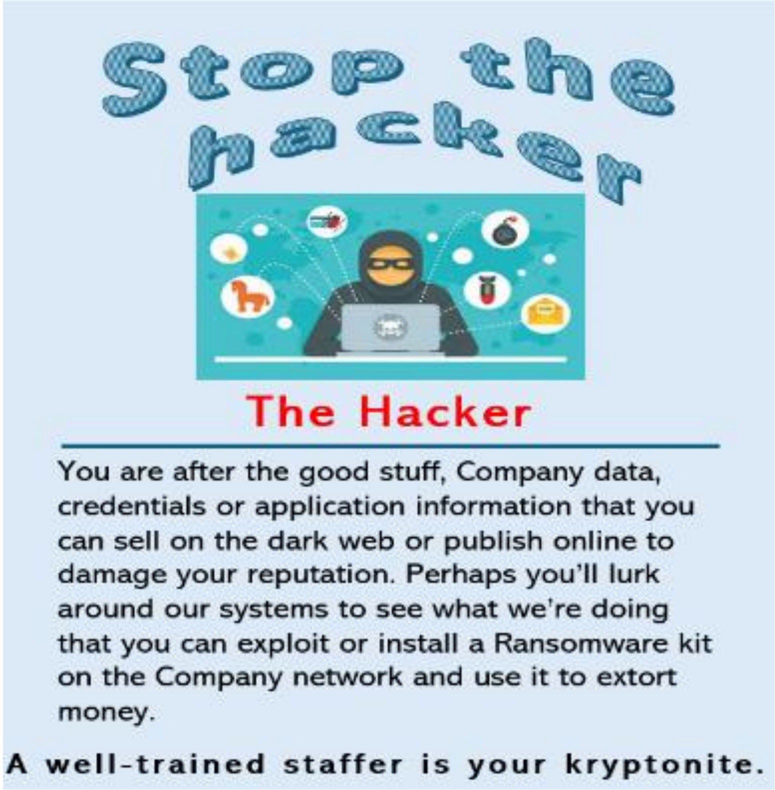
Participants: 4 – 6 players (1 hacker, + 3 – 5 Staff)
1 Game Moderator



Stop the hacker



Moderator hands out cards which indicate player roles



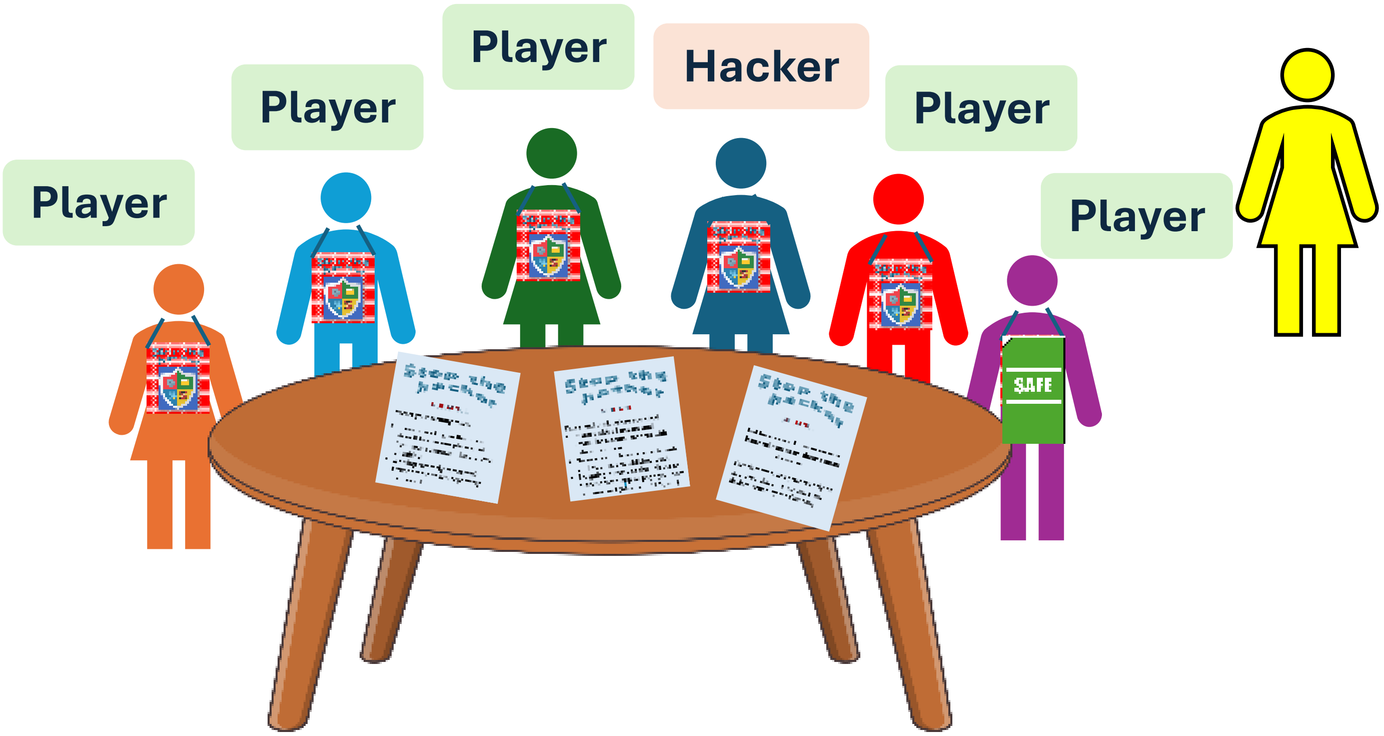
Stop the hacker

The Hacker

You are after the good stuff, Company data, credentials or application information that you can sell on the dark web or publish online to damage your reputation. Perhaps you'll lurk around our systems to see what we're doing that you can exploit or install a Ransomware kit on the Company network and use it to extort money.

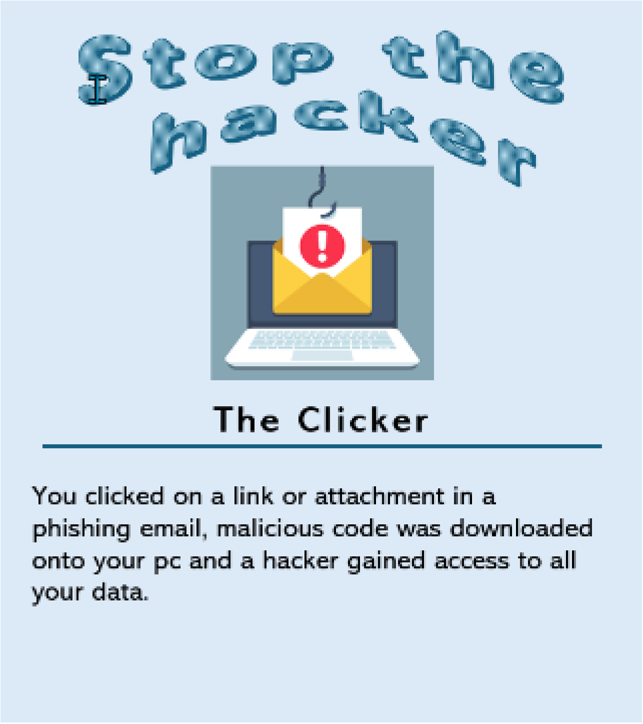
A well-trained staffer is your kryptonite.

Stop the hacker



Hacker targets a staff member. Staff reads out the scenario on their card.

Moderator (aka the *Trainer*) offers options to prevent the exploitation

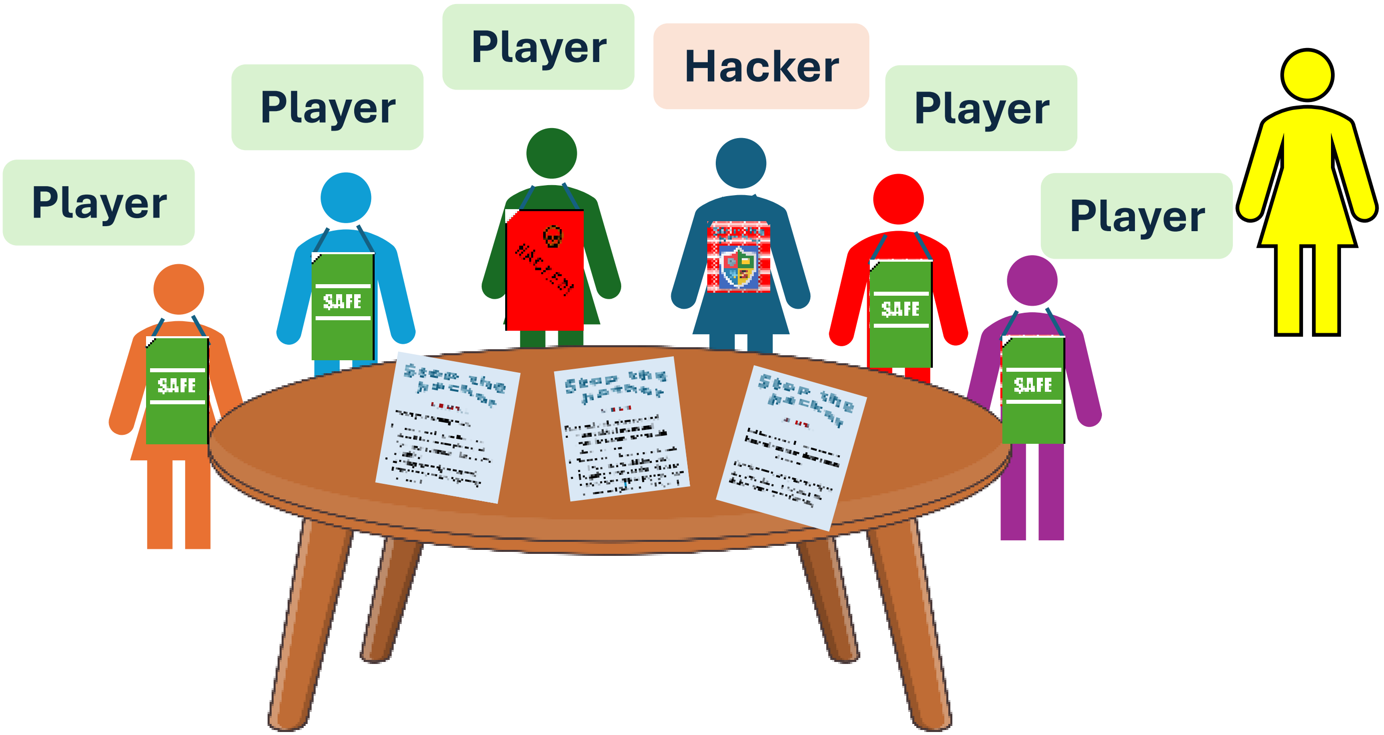


Stop the hacker

The Clicker

You clicked on a link or attachment in a phishing email, malicious code was downloaded onto your pc and a hacker gained access to all your data.

Stop the hacker

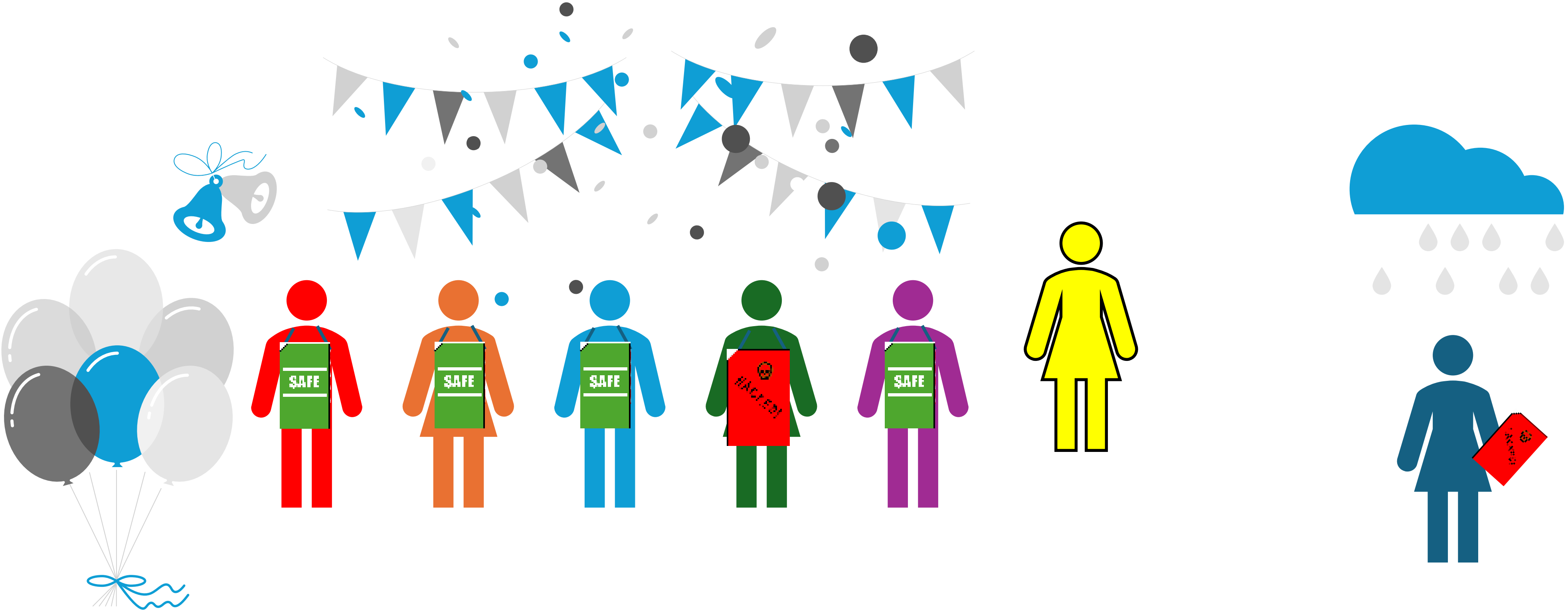


Correct answers earn a "Safe" lanyard.

Incorrect answers receive a "Hacked" lanyard.

Each player gets to respond to their scenario.

Stop the hacker



Game ends when all players have worked together to STOP THE HACKER!

Stop the hacker

Purpose: By playing ***Stop the hacker***, players show their knowledge of cybersecurity best practices where user behavior protects the organization. The game will re-iterate the impact of user behavior to protect the organization from cyber threats.

Outcomes:

- Stressed to participants that their behavior is the foundation protecting our organization
- Reinforced understanding that they have control over all the risky behaviors presented in the game
- Gave players a *fun* and *novel* way to engage with training material

Success:

- The game is designed to be winnable to encourage good cybersecurity habits.
- Over 300 people attended the 2024 Cybersecurity Awareness Month event, with many of them playing *Stop the hacker*
- Asked to reprise the game at other Technology showcase events
- Easy to run, ~7 minutes per game

Stop the hacker – any questions

CISA's 7th Annual President's Cup Cybersecurity Competition

Brittney Thomas

Federal Program Manager, President’s Cup Cybersecurity Competition (PCCC)
Cybersecurity and Infrastructure Security Agency (CISA)

PRESIDENT'S CUP

CYBERSECURITY COMPETITION

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Welcome to President's Cup 7!

Overview of the 7th annual cybersecurity competition

Key dates and competition structure

Theme and challenges

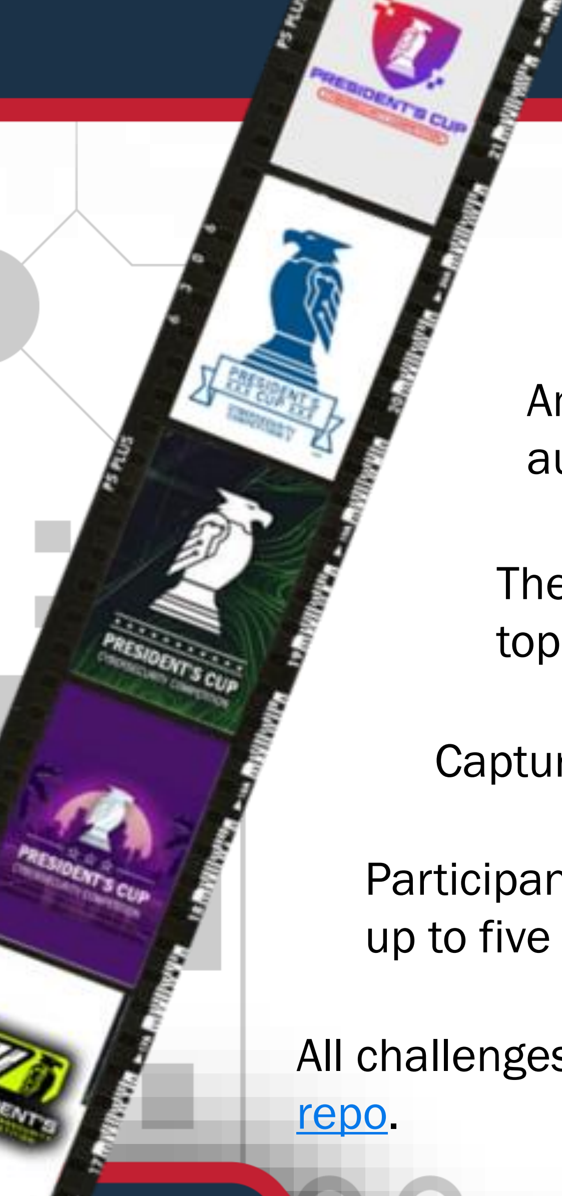
New competition platform

Registration and eligibility details

New eligibility cap and Hack of Fame

Participation benefits

Game of the Month initiative



What is the President’s Cup Cybersecurity Competition?

America’s Cybersecurity Workforce E.O. 13870 and FY23 NDAA authorizes CISA to hold the competition annually.

The goal of the competition is to identify, challenge, and reward the top cybersecurity talent in the federal workforce.

Capture the Flag format with three rounds over 3 months.

Participants can compete as an Individual and/or on a Team of up to five members.

All challenges made available on the Practice Area and CISA GitHub repo.

PC7 Highlights

3 TRACKS

- Individuals Defensive
- Individuals Offensive
- Teams

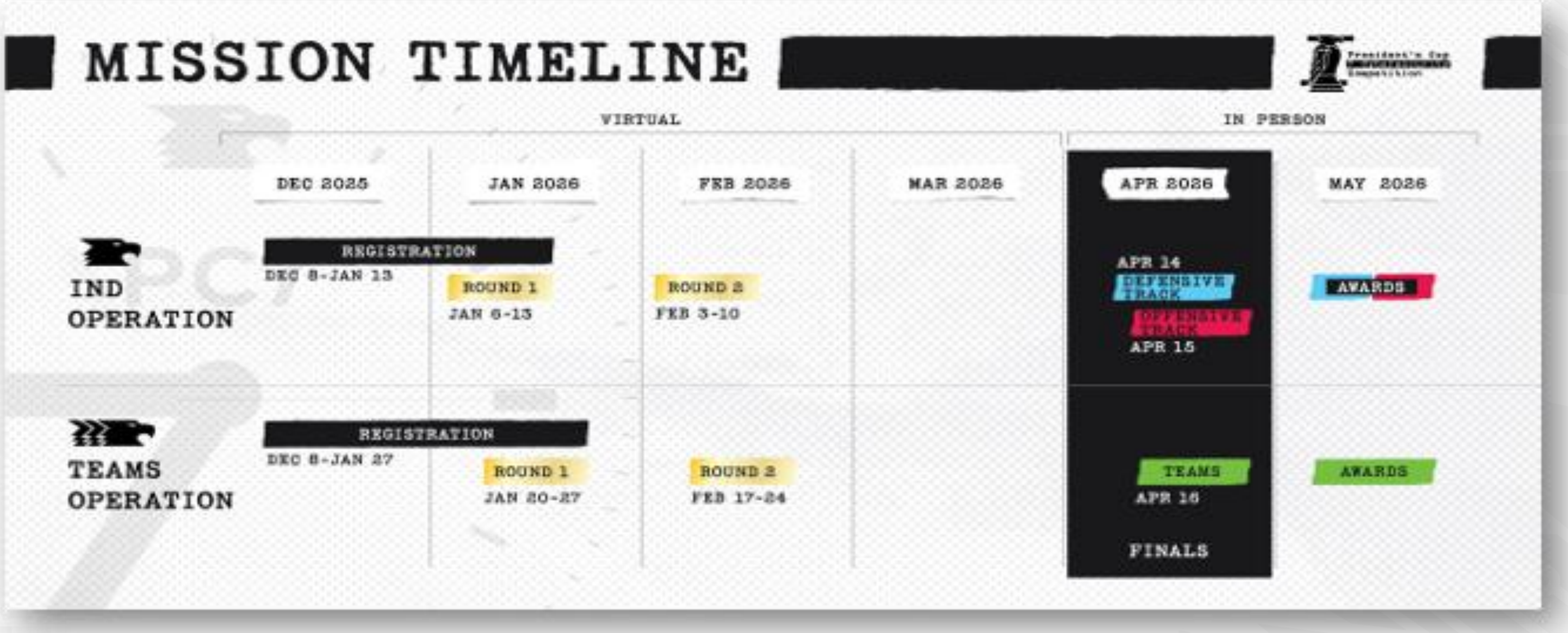
3 ROUNDS

- 2 Virtual Qualifying Rounds
- In Person Finals

AWARDS CEREMONY

- Hosted by Office of the National Cyber Director (ONCD) at the Eisenhower Executive Office Building (EEOB) of the White House.

Competition Timeline



MISSION TIMELINE

	VIRTUAL				IN PERSON	
	DEC 2025	JAN 2026	FEB 2026	MAR 2026	APR 2026	MAY 2026
IND OPERATION	REGISTRATION DEC 8-JAN 13	ROUND 1 JAN 6-13	ROUND 2 FEB 3-10		APR 14 DEFENSIVE TRACK OFFENSIVE TRACK APR 15	AWARDS
TEAMS OPERATION	REGISTRATION DEC 8-JAN 27	ROUND 1 JAN 20-27	ROUND 2 FEB 17-24		TEAMS APR 16 FINALS	AWARDS

- **First Round:**
  - Open to all federal employees/uniformed service members
- **Second Round:**
  - Individuals: Top 100 scores
  - Teams: Top 33% based on scores
- **Finals:**
  - Top 10 Individuals in Offensive/Defensive Tracks
  - Top 5 Teams

New Competition Platform

New Platform Debut

Transitioning from virtual machines (VMs) to containers for improved performance and scalability.

Enhanced features and improved user experience.

Designed to support complex challenges and provide a seamless competition environment.

Account Creation

All returning members will need to re-create their accounts.

Federal and military members with PIV cards can use SSO to create their accounts.

All others will create usernames and passwords.

Transition Period

The old platforms will remain available while we transition previous challenges to the new platform

Participants are encouraged to download any saved certificates from the practice area or expo

Eligibility Cap

- Competitors may place in the top 3 a maximum of three times total, across all competition years and tracks beginning with PC7.
- At least one of those placements must be a 1st place finish to qualify for the eligibility cap.
- Once competitors reach the eligibility cap, they are no longer eligible to place and receive awards in Individual tracks but may continue to participate in the Teams track.
- Teams may include no more than one member that has reached the eligibility cap.

Hack of Fame

- A distinction recognizing elite performers with at least one first-place finish among their three top 3 placements.
- Provides continued engagement opportunities through mentorship, challenge development, panel participation, exhibition-based competitions, and red team activities.
- Recognition applied from President’s Cup I onward, with participation restrictions taking effect beginning with President’s Cup 7 (PC7).

Registration and Preparation

How to Register:

Visit cisa.gov/presidentscup
Create a new login
Review revised rules and guidelines

Prepare and Practice:

All challenges and solution guides are available on the Practice Area and CISA GitHub repo

Competition Participation Benefits

Skill Development

Hands-on experience in cybersecurity
NICE Framework alignment

Career Advancement

Recognition and awards
Networking opportunities

Continuous Learning

Access to past challenges and resources, including completion certificates

Game of the Month

- Each quarter the PC Team will identify a specific NICE work role
- Monthly challenges tied to that NICE work role to enhance skill.
- Each month the challenges identified will become progressively more difficult
- Leveraging challenges from past competitions and hosted in our practice area

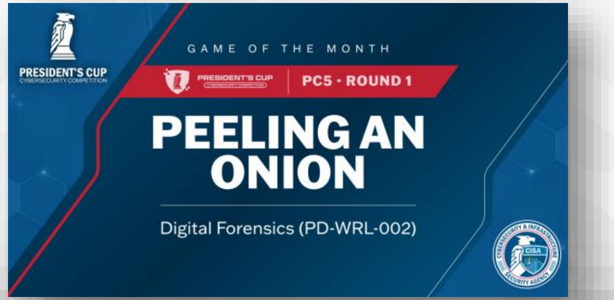
Why Participate?

☑ Boost your career by working on NICE framework tasks.

☑ Develop key cybersecurity skills.

☑ Challenge yourself with real-world cyber incident scenarios

Visit the <u>Game of the Month</u> on the President's Cup website for participation stats, Game of the Month details, and more.



Your Mission Awaits

Visit: cisa

Email: presidentscup@cisa.dhs.gov

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

Creating a Cybersecurity Tip of the Month

Rebecca D. Martin

IT Cybersecurity Specialist
Social Security Administration

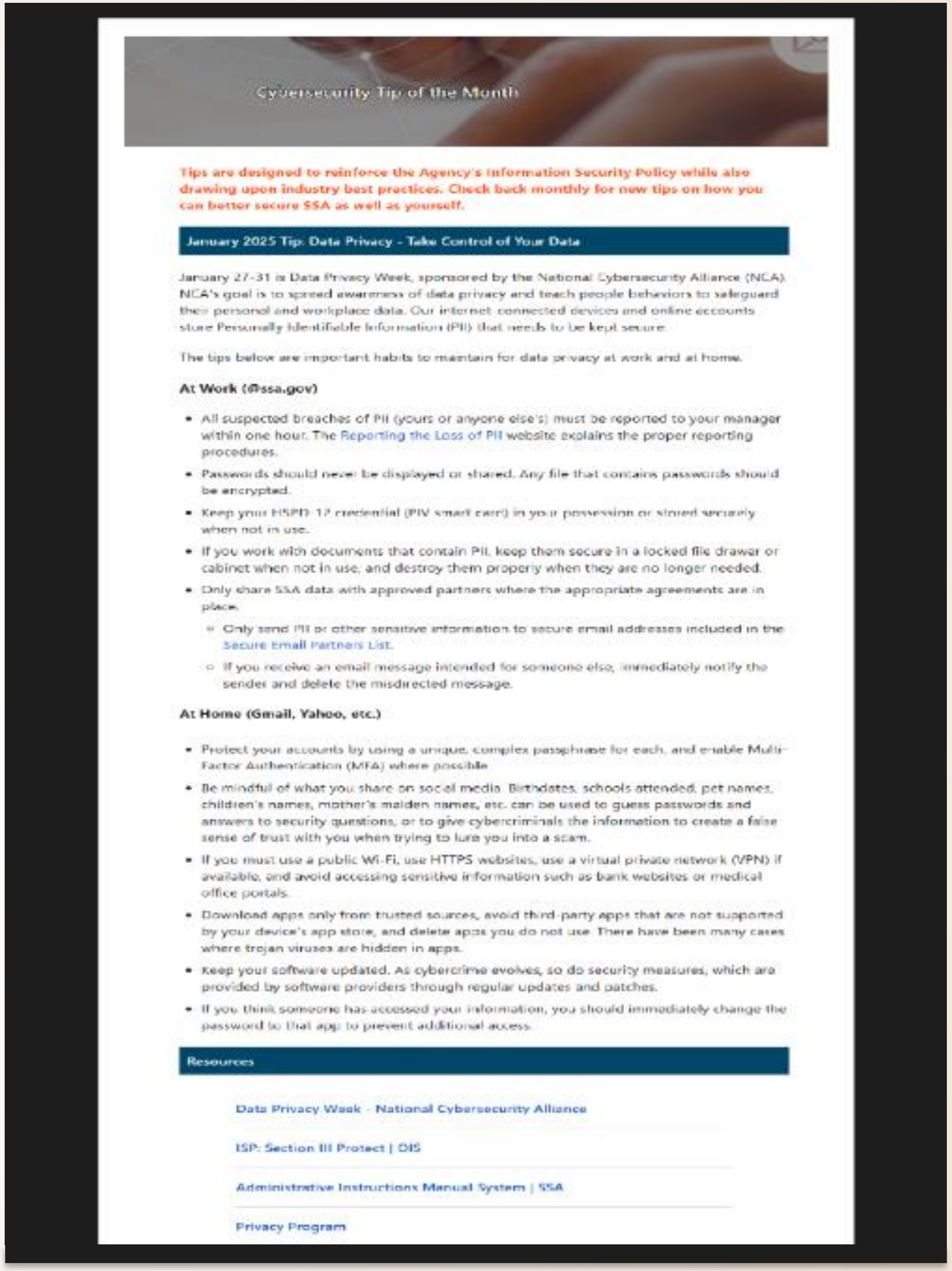
Creating a Cybersecurity Tip of the Month

September 30, 2025

Securing today
and tomorrow

SSA's Cybersecurity Tip of the Month

- A webpage updated monthly
- Hosted on the Information Security website
- The library of prior tips are stored on the same website.
- Other publications can link to these tips as an additional resource



Cybersecurity Tip of the Month

Tips are designed to reinforce the Agency's Information Security Policy while also drawing upon industry best practices. Check back monthly for new tips on how you can better secure SSA as well as yourself.

January 2025 Tip: Data Privacy - Take Control of Your Data

January 27-31 is Data Privacy Week, sponsored by the National Cybersecurity Alliance (NCA). NCA's goal is to spread awareness of data privacy and teach people behaviors to safeguard their personal and workplace data. Our internet-connected devices and online accounts store Personally Identifiable Information (PII) that needs to be kept secure.

The tips below are important habits to maintain for data privacy at work and at home.

At Work (@ssa.gov)

- All suspected breaches of PII (yours or anyone else's) must be reported to your manager within one hour. The Reporting the Loss of PII website explains the proper reporting procedures.
- Passwords should never be displayed or shared. Any file that contains passwords should be encrypted.
- Keep your HSPD-12 credential (PIV smart card) in your possession or stored securely when not in use.
- If you work with documents that contain PII, keep them secure in a locked file drawer or cabinet when not in use, and destroy them properly when they are no longer needed.
- Only share SSA data with approved partners where the appropriate agreements are in place.
  - Only send PII or other sensitive information to secure email addresses included in the Secure Email Partners List.
  - If you receive an email message intended for someone else, immediately notify the sender and delete the misdirected message.

At Home (Gmail, Yahoo, etc.)

- Protect your accounts by using a unique, complex passphrase for each, and enable Multi-Factor Authentication (MFA) where possible
- Be mindful of what you share on social media. Birthdates, schools attended, pet names, children's names, mother's maiden names, etc. can be used to guess passwords and answers to security questions, or to give cybercriminals the information to create a false sense of trust with you when trying to lure you into a scam.
- If you must use a public Wi-Fi, use HTTPS websites, use a virtual private network (VPN) if available, and avoid accessing sensitive information such as bank websites or medical office portals.
- Download apps only from trusted sources, avoid third-party apps that are not supported by your device's app store, and delete apps you do not use. There have been many cases where trojan viruses are hidden in apps.
- Keep your software updated. As cybercrime evolves, so do security measures, which are provided by software providers through regular updates and patches.
- If you think someone has accessed your information, you should immediately change the password to that app to prevent additional access.

Resources

Data Privacy Week - National Cybersecurity Alliance

ISP: Section III Protect | OIS

Administrative Instructions Manual System | SSA

Privacy Program

Benefits

Provides:

- Monthly cybersecurity reminders
- Additional education on cybersecurity topics
- Information based on current best practices
- Topics that fall outside of mandatory annual training
- Links to external articles and internal policy for additional information

Topics

Eight fundamental topics are used every year:

- Data Privacy Week in January
- World Backup Day in March
- CAM in October
- Password safety in May
- Insider Threat
- Internet Safety
- Identity Theft
- Social Engineering

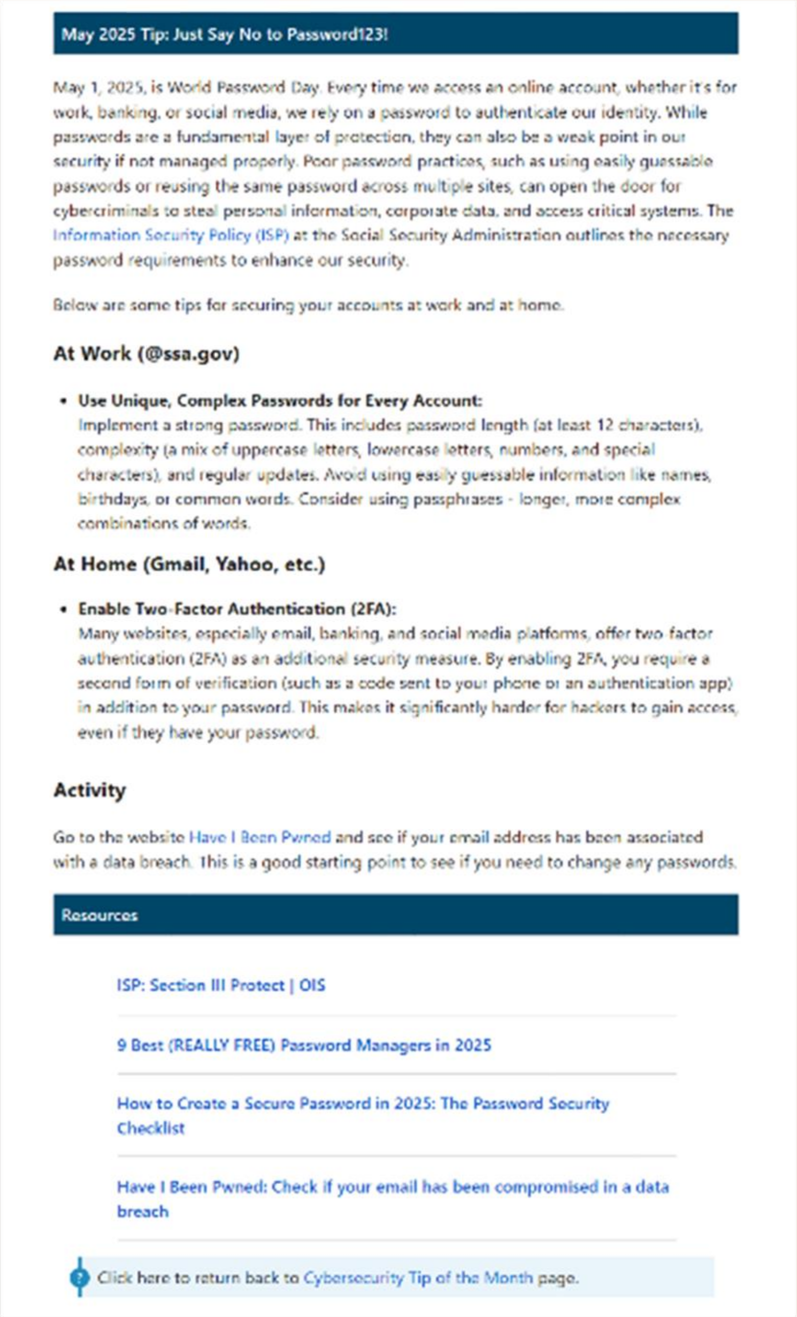
The other four months explore additional topics

Examples:

- Firewalls and VPNs
- Data classification
- Federal guidelines
- Securing Mobile Devices
- Cloud Security
- Malware

Basic Template

1. Descriptive paragraph
2. List of 5 bullet points for **tips at work**
3. List of 5 points for **tips at home**.
4. Activity
5. References



May 2025 Tip: Just Say No to Password123!

May 1, 2025, is World Password Day. Every time we access an online account, whether it's for work, banking, or social media, we rely on a password to authenticate our identity. While passwords are a fundamental layer of protection, they can also be a weak point in our security if not managed properly. Poor password practices, such as using easily guessable passwords or reusing the same password across multiple sites, can open the door for cybercriminals to steal personal information, corporate data, and access critical systems. The Information Security Policy (ISP) at the Social Security Administration outlines the necessary password requirements to enhance our security.

Below are some tips for securing your accounts at work and at home.

At Work (@ssa.gov)

- **Use Unique, Complex Passwords for Every Account:**
  Implement a strong password. This includes password length (at least 12 characters), complexity (a mix of uppercase letters, lowercase letters, numbers, and special characters), and regular updates. Avoid using easily guessable information like names, birthdays, or common words. Consider using passphrases - longer, more complex combinations of words.

At Home (Gmail, Yahoo, etc.)

- **Enable Two-Factor Authentication (2FA):**
  Many websites, especially email, banking, and social media platforms, offer two-factor authentication (2FA) as an additional security measure. By enabling 2FA, you require a second form of verification (such as a code sent to your phone or an authentication app) in addition to your password. This makes it significantly harder for hackers to gain access, even if they have your password.

Activity

Go to the website Have I Been Pwned and see if your email address has been associated with a data breach. This is a good starting point to see if you need to change any passwords.

Resources

ISP: Section III Protect | OIS

9 Best (REALLY FREE) Password Managers in 2025

How to Create a Secure Password in 2025: The Password Security Checklist

Have I Been Pwned: Check if your email has been compromised in a data breach

Click here to return back to Cybersecurity Tip of the Month page.

Questions?

Securing today
and tomorrow

SocialSecurity.gov

Estimate your benefits • Open a *my* Social Security account • Apply online

Email: Rebecca.D.Martin@ssa.gov

Closing Remarks

Joyce Mui
FISSEA Co-Chair
National Institute of Standards and Technology

THANK YOU

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

https://www.surveymonkey.com/r/2025fisseafallforum

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA

Get Involved

✉ Subscribe to the FISSEA Mailing List
FISSEAUpdates+subscribe@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
Email fissea@nist.gov

SAVE THE DATE

Federal Information Security Educators (FISSEA) Winter Forum

February 10, 2026

#FISSEA | nist.gov/fissea

NIST FEDERAL INFORMATION SECURITY EDUCATORS FISSEA