

SSA'S PHISH YOUR COLLEAGUE CYBERSECURITY AWARENESS MONTH PROGRAM



FOR MORE INFORMATION

OIS.INFORMATION.SECURITY.TRAINING@SSA.GOV



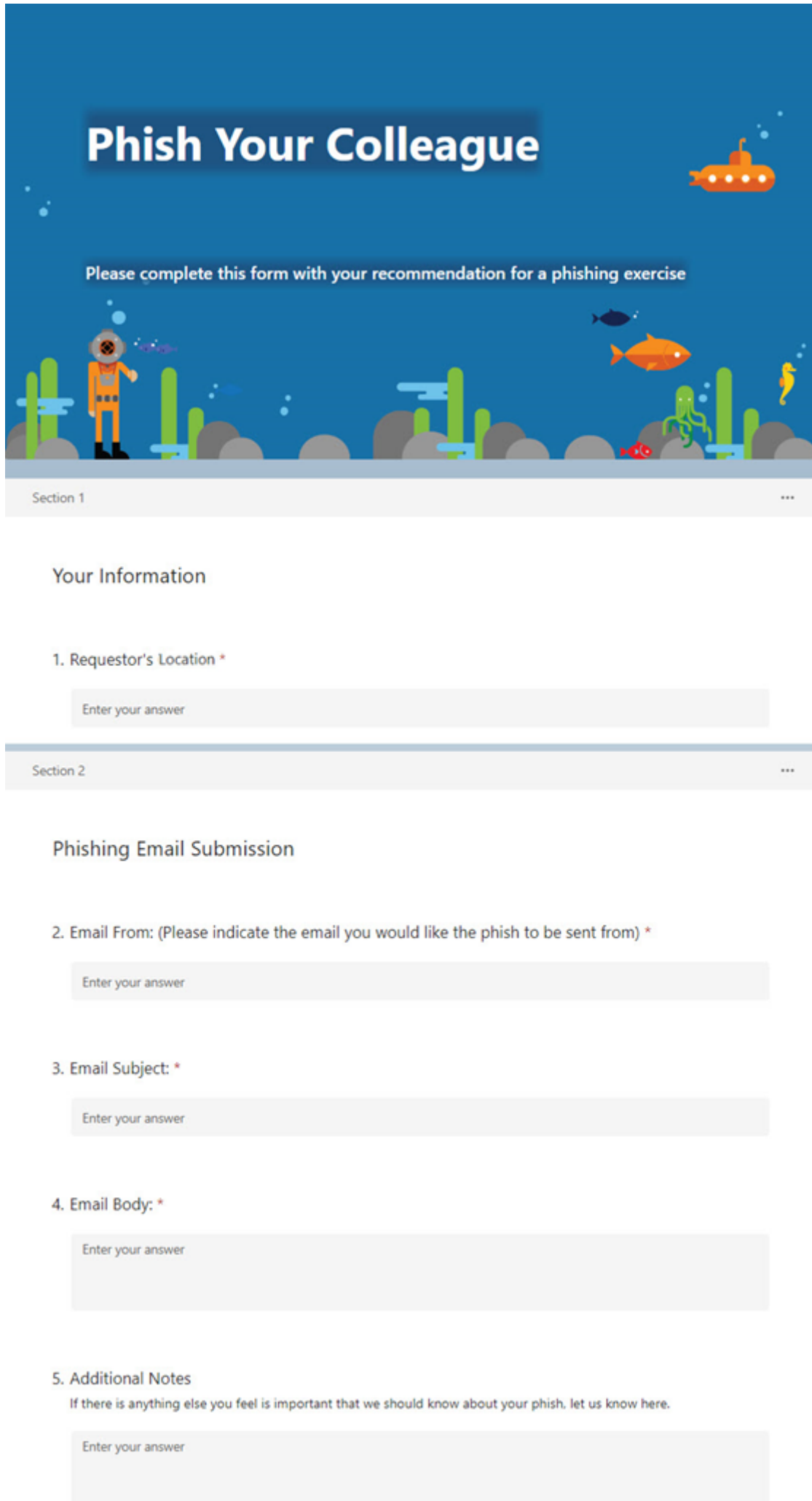
About Phish Your Colleague



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.

Submission Form

SSA users submitted their cleverest phishing attempts for “Phish Your Colleague” using an internally developed form. Users across the SSA shared their emails that they felt tested their coworkers’ vigilance.



Phish Your Colleague

Please complete this form with your recommendation for a phishing exercise

Section 1

Your Information

1. Requestor's Location *

Enter your answer

Section 2

Phishing Email Submission

2. Email From: (Please indicate the email you would like the phish to be sent from) *

Enter your answer

3. Email Subject: *

Enter your answer

4. Email Body: *

Enter your answer

5. Additional Notes

If there is anything else you feel is important that we should know about your phish, let us know here.

Enter your answer

Submission Repository

Our repository served as a centralized hub for analysis and evaluation by our cybersecurity team, allowing us to glean valuable insights about SSA's user population understanding of phishing attacks.

Email Subject: ▾	Email Body: ▾	Additional Notes ▾	Contender? ▾
PII Loss detected!	The PII Loss Prevention unit has detected an email sent from your computer that contained sensitive or confidential information. Please click on the link below to review the email and provide response.	Employees are reminded about PII on a consistent basis and are encouraged to follow proper procedures to secure email leaving the agency. I think being notified they had a PII email may override any phishing reminders they may have	Yes
unauthorized shopping on government equipment	Your computer has been detected using shopping portals that have been compromised. Please click on the below link to run a security scan to determine whether your PII has been leaked.		Yes
Taylor Swift tickets	Here is your chance to win a trip for 2 to see Taylor Swift. This includes round trip airfare and paid accommodations in Las Vegas. Click the following link and complete the form provided.		Yes
CAM Participant!	[Redacted]	[Redacted]	Winner
Time Sheet Correction	Your request to review your leave balances has been received; however, we cannot process your request without additional information. Please verify your date of birth (DOB) and the last four digits of your SSN. You will receive a confirmation email once the review has been		No
quick question	Hi, I hope you remember talking to me the other day about my claim. I need to speak to you as soon as you're able. I've attached the letter you sent me and I think it's wrong. can you look at it now?	With this message, I'd attach a document, per the email above, to make it look like the sender attached a letter (knowing that we shouldn't open emails from untrusted senders). Also, I made the email address look like it's coming from someone	Yes
[Redacted]	[Redacted]	[Redacted]	No
FW: 2023 Pennsylvania Commissioner's Virtual Award Ceremony	Did you see what John got? Surprising! --Dave From: [Redacted] >	This was crafted as an informal forward from a colleague. People are always interested in seeing what awards are given out, especially if it is surprising. "Virtual Award Ceremony" in the content would be linked to an external site. Users	Yes
You are eligible to register for a government refund	Please update your information so we can send you your refund.		Yes
[Redacted]	certificate		Yes
[Redacted]	[Redacted]	There should be a link for the person to click to "verify" their credential. There should also be a link available to open a "Help Desk ticket".	Yes
Your Meeting Notes	Congratulations! You've been selected to use meetingnotes a new program in the macrosift office sweet. This program will help you be more effecient with your meetings as well being able to track meeting attendences. Click the Link below to get reg'd.	This is because people often are just clicking through provide dead hyperlink that would lead people to a trap link. Bad spelling and, misnamed programs are often found in phishing emails.	Yes
Your password will expire soon, update immediately.	Hello, This email to notify you that your email password has expired. Please click the link below for further assistance.	[Redacted]	Yes
Do Not Wait Until the Last Day – Make Your Elections Now	(Picture/ Banner/ Make it look official)		No

Website

Our resource website serves as the central hub for all things related to cybersecurity awareness and education within our organization. Through strategic design and user-friendly navigation, we seamlessly direct users to our “Phish Your Colleague” submission form, where participants can showcase their phishing prowess.



The 2023 Phish Your Colleague event has concluded!

The Social Engineering Team would like to thank everyone who participated in the Phish Your Colleague program. We received over 300 submissions for phishing ideas! Everyone who submitted an entry has earned an [Org Chart badge](#) for helping to make this program a success!

2023 Winners

From the submissions, we selected 7 winners whose creative ideas were used in real live phishing exercises at the Agency! Below is the list of the winners along with the phishing emails they created!

Winners	Phishing Exercise
[Redacted]	OIS Rewards Program 🐟
[Redacted]	VPN update 🐟
[Redacted]	CAM Participant 🐟
[Redacted]	Sending pictures of my new baby girl 🐟
[Redacted]	Holiday Party Planning! 🐟
[Redacted]	Systems Account Termination - IMMEDIATE ACTION REQUIRED 🐟
[Redacted]	Reminder: OneDrive retention policy 🐟

Bait the Hook, Earn the Rewards

The "Phish Your Colleague" program invites all SSA employees to submit their own phishing ideas for an organization-wide competition. This program encourages you to think like scammers, explore their tactics, and understand how to protect yourself and the Social Security Administration from their malicious activities. The submitted ideas will be utilized in phishing tests to assess the Social Security Administration ability to identify and respond to phishing attacks.

Characteristics of Phishing Messages

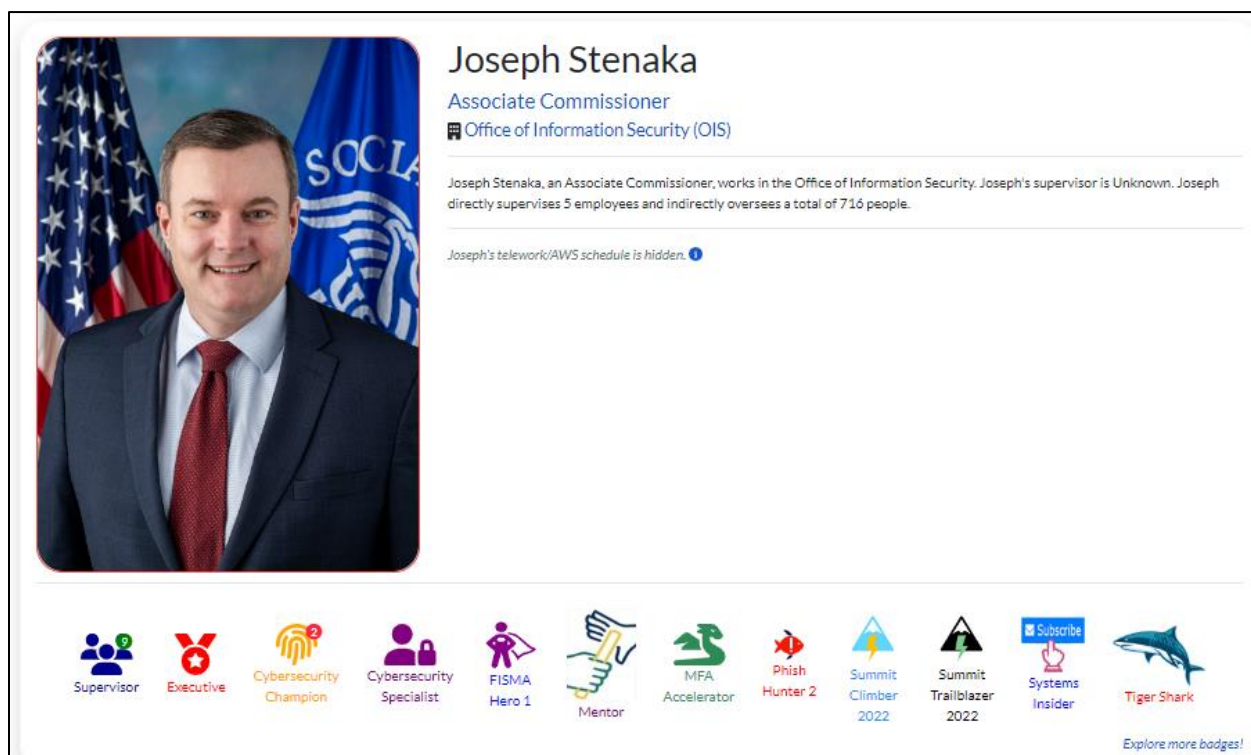
Understanding the characteristics of phishing messages is crucial to identifying and reporting them effectively. Here are some common traits to look out for:

- **Deceptive sender information:** Pay attention to the email address, display name, or any suspicious details that may indicate an impersonation attempt.
- **Urgency and pressure:** Phishing emails often create a sense of urgency, making you feel the need to act quickly without thinking.
- **Requests for personal information:** Legitimate organizations rarely ask for personal information via email. Be cautious when providing sensitive data.
- **Unusual links and attachments:** Hover over links to verify their legitimacy before clicking. Be wary of unexpected attachments or downloads.
- **Poor grammar and spelling:** Phishing emails often contain grammar mistakes or awkward language usage.

Thank you for your dedication to the security of the SSA. Together, we can build a strong defense against phishing attacks and create a safer digital environment for everyone. For any questions or concerns regarding the "Phish Your Colleague" program, please reach out to [Redacted]

Profile Badges

Our profile pages platform serves as dynamic visual representation of our organization's structure and hierarchy. In addition to its traditional role, we've innovatively integrated a badge system to recognize and showcase individuals' achievements. Through this system, users earn badges based on their participation and success in events like "Phish Your Colleague" demonstrating their commitment to enhancing our collective security posture. These badges are displayed on users' ongoing engagement in our cybersecurity initiatives.



Joseph Stenaka
Associate Commissioner
Office of Information Security (OIS)

Joseph Stenaka, an Associate Commissioner, works in the Office of Information Security. Joseph's supervisor is Unknown. Joseph directly supervises 5 employees and indirectly oversees a total of 716 people.

Joseph's telework/AWS schedule is hidden.

Supervisor Executive Cybersecurity Champion Cybersecurity Specialist FISMA Hero 1 Mentor MFA Accelerator Phish Hunter 2 Summit Climber 2022 Summit Trailblazer 2022 Systems Insider Tiger Shark

Explore more badges!

Participant Badge



Winner Badge



Communications

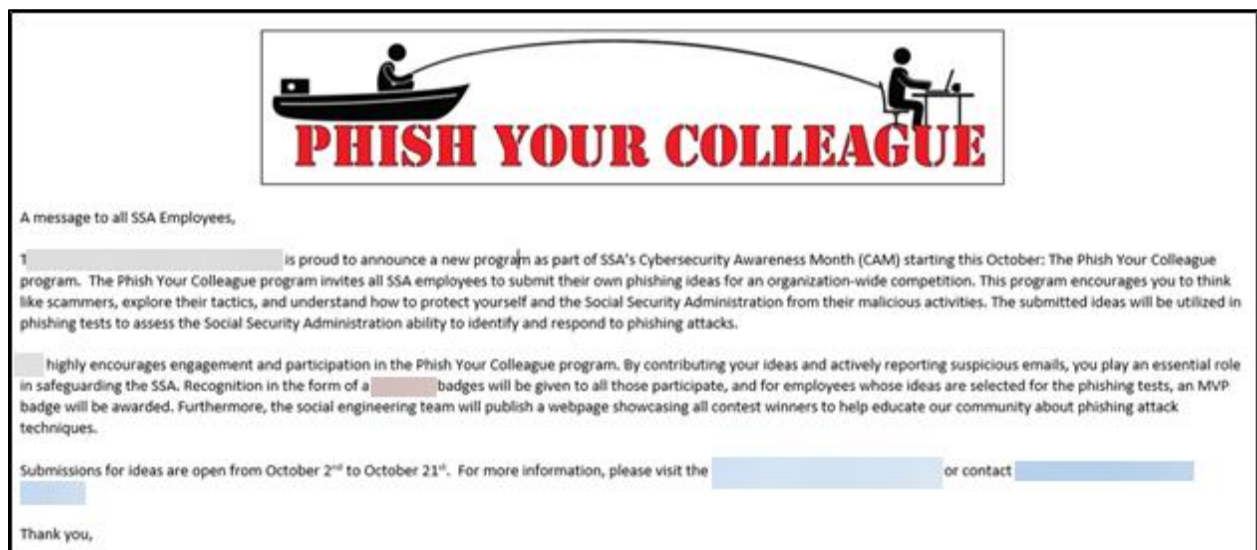
We kept users informed about events like “Phish Your Colleague” and badge awards through emails, internal messages, and our resource site.

Example of Blurbs:

🌊 Dive into the deep end of cybersecurity fun during Cybersecurity Awareness Month with our "Phish Your Colleague" event – it's a feeding frenzy of creativity!


👤 From October 2nd to October 21st, 2023, we're challenging all SSA employees to unleash their inner cyber-sharks and whip up their most ingenious phishing ideas. 🦈 Sink your teeth into the competition, and if your idea gets picked, watch as it takes center stage in a thrilling phishing exercise that will have those digital predators swimming in circles! ✨🔒 Plus, participants will snag an exclusive badge, while those whose ideas are selected will earn a rare badge that's truly a fintastic catch! 🏆 Let's show 'em who rules the cyber-reef and keep our waters safe together by diving in here {Link} 🌐🛡️

Example of Email Communications #1




Example of Email Communications #2

OCTOBER IS CYBERSECURITY AWARENESS MONTH



Welcome to the agency's first week of Cybersecurity Awareness Month (CAM) 2023 activities!

REGISTER NOW for Cybersecurity Jeopardy-LIVE!



We are registering NOW for participants in our LIVE, interactive Cybersecurity Jeopardy game being held on Tuesday, October 17th from 12pm-1pm! Head over to the [CAM Homepage](#) and register to be a team captain, team member or audience member! Registration will close on 10/12, or once we reach the max number of participants, so ACT FAST, there are only a small number of slots available!! Hope to see you there!

Phish Your Colleague


Dive into the deep end of cybersecurity fun during Cybersecurity Awareness Month with our "Phish Your Colleague" event - it's a feeding frenzy of creativity! From October 2nd to October 21st, 2023, we're challenging all SSA employees to unleash their inner cyber-sharks and whip up their most ingenious phishing ideas. Sink your teeth into the competition, and if your idea gets picked, watch as it takes center stage in a thrilling phishing exercise that will have those digital predators swimming in circles! Plus, participants will snag an exclusive badge, while those whose ideas are selected will earn a rare badge that's truly a fintastic catch! Let's show 'em who rules the cyber-reef and keep our waters safe together by diving in here [here](#)

Cybersecurity Tip of the Month

Please be sure to visit [Cybersecurity Tip of the Month](#) for advice on how to stay secure both at work and at home.

Earning Your Cybersecurity Champion Badge

You can become a Cybersecurity Champion! We will reward your participation in this year's CAM events and activities with a Cybersecurity Champion badge for your [profile](#). To earn the badge, you must attend at least one of the four CAM events and complete the survey you receive at the end of the month. Responses are important and will aid in future CAM activity planning. For those who earned the badge last year, you will keep your badge, but you will gain a counter to your badge indicating your participation, for example, a 2 for your second year of participation, a 3 for your third and so on.



CAM 2023 Weekly Events Calendar

As a reminder OIS is hosting the following weekly events. Please visit the [CAM Homepage](#) to register for each activity you would like to attend, and you will receive an invitation email to add the event to your calendar. Participation subject to supervisory approval.

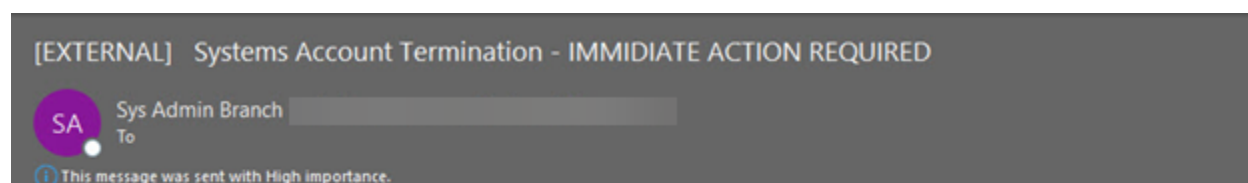
Date	SSA Event	Time
Wednesday, 10/04	Cybersecurity Awareness Month - Keynote Address	1:00pm - 2:00pm EST
Wednesday, 10/11	Presentation on The State of Privacy Across the Federal Space	1:00 pm - 2:00 pm EST
Tuesday, 10/17	Cybersecurity Jeopardy-LIVE! Lunch and Learn	12:00pm - 1:00pm EST
Wednesday, 10/18	Systems Talk - Penetration Testing	1:00 pm - 2:00 pm EST
Wednesday, 10/25	Presentation Highlighting the 4 Key Pillars of Cybersecurity Awareness Month	1:00pm - 2:00pm EST

QUESTIONS

Please visit the [CAM Homepage](#) to learn more about the events and initiatives the agency is hosting to raise awareness about cybersecurity. Feel free to let us know what you thought about this week's tip and activity or if you have additional questions email [\[redacted\]](#)

Phishing Email Submission Winners

Hundreds of submissions were sent in from across the agency. We grouped the submitters by role and region, and selected winners for each group. The winning submissions were sent to the colleagues from that group as phishing exercises.



Good Day,

It has come to are attention that you attempt to access protected PI files on your company issued computer. Please use link below to see log of activity and set up meeting to discuss PENDING termination for your account with system admin branch team lead director.

[System Account Log and Meeting Invitation](#)

Thanks,
System Admin Branch Team Lead Director



SSA is implementing a new reward program for exceptional work. Your manager had submitted your name entering you into the drawing to win a free PlayStation 5.

Congratulations, you've won!! Click [here](#) to claim your prize! Be sure to fill out the form before November 17th or you will be withdrawn from the contest.

Thank you from everyone at SSA for your exceptional work!!



Thank you for your interest in partaking in this years Cyber Awareness Month activities!

As Social Security Employees; stewards of the nations critical data, it is paramount that we remain vigilant in our Cyber Hygiene.

In order to receive credit for your efforts and to attain your badge(s), please follow this link and register: [CAM Registry](#)



Hi!

We started planning this year's holiday party already, can you believe it is already almost holiday time? We need more information for people in office so they can be invited. Would you kindly fill in your information on [the document at this link](#) so everyone can be involved? The information must be in the document by the end of the day, or you will miss out on the fun this party will bring! Also on document is space for you to put in your purchase information since we purchase gifts for everyone this year, we will all chip in! Just put in your credit card or bank info and we will handle buying door prize and white elephant gifts for office people.

Happy Holidays!

Sunshine Crew

[EXTERNAL] Sending pictures of my new baby girl

TJ The Jones Family <howardjones36@hotmail.com>
To

I just wanted to share a [picture](#) with you of our daughter who was just born.

[EXTERNAL] Reminder: OneDrive retention policy

NR No Reply
To

This message was sent with High importance.

In order to be in compliance with our retention policy, we will be deleting all stored data older than three years. You can verify which documents in your OneDrive account are subject to deletion [here](#).

If a user was susceptible to the email, clicking on the link took them to the regular training, that also included this message:



The Impact of “Phish Your Colleagues”

The Phish your Colleagues program was an experiment to shift cyber security strategy by recognizing that our employees are not just targets but crucial allies in our defense against malicious actors. By involving employees in the process of crafting phishing, we are not only fostering a deeper understanding of cybersecurity threats, but also instilling a culture of vigilance and responsibility, particularly among those who interact directly with the public. These collaborative efforts help us better fortify our defenses and promote a stronger reporting culture.