FY22 Q3 Health Check: April 6th, 2022, Volume 2, Issue 3

Time to do some spring cleaning by completing another Cybersecurity Health Check. Review your cybersecurity practices and update them if necessary. Revisit SSA's Information Security Policy (ISP) Topics for Me, previous issues of the Cybersecurity Health Check, and other OIS training resources to ensure your cybersecurity measures stay current with updated SSA policies and guidance. Also, show off your good cybersecurity knowledge by completing a brief survey. Check out Survey Reflections where your feedback is addressed.

Protecting SSA data and assets is an agency-wide effort and every employee's responsibility. Get involved by completing the following health check:

☑ I am aware of the increased threat of Russian state-sponsored cyberattacks.

☑ I do not respond to emails soliciting credentials or other Personally Identifiable Information (PII).

☑ I am aware that the human element is the first line of cyber defense and my vigilance could help prevent a cyber incident from occurring at SSA.

☑ I follow the SSA's best practices to backup and store my data appropriately.

☑ I use encryption on files that contain passwords and on emails containing PII that are sent to external recipients not on the Secure Email Partners List.

☑ I have completed the mandatory "**FY 2022 Information Security and Privacy Awareness Training**" that is available in weLearn.

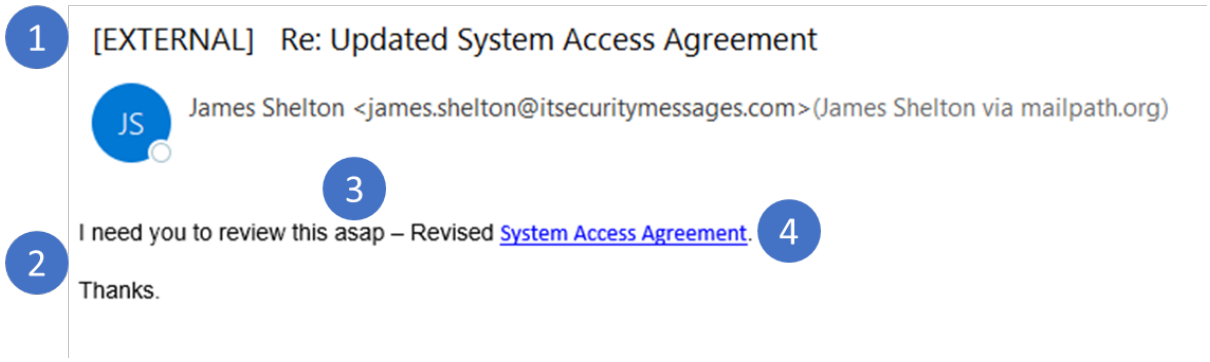
☑ I have reviewed available SSA resources to learn how to protect myself from Social Security scams at home.

☑ I report suspected phishing emails within 15 minutes of incident discovery by using the "SSA Reporter" button in the Outlook ribbon.

Phishing emails may look like they're from a trusted source but they can trick you into divulging sensitive information or performing actions that may compromise the security of SSA. Following SSA's best practices is the best way to avoid being a victim of phishing. Some best practices include: verifying the sender of the email and only selecting a link or opening an attachment after verifying its legitimacy.

Please review the following example of a phishing email and the clues that indicate the email is a phish.

Phishing Emails



Clues

1. The email was sent from an [EXTERNAL] email address that is not used by the SSA (non-ssa.gov domain).
2. The sender attempted to mimic a basic and familiar office message to lure the recipient in.
3. The sender attempted to use urgency to get the recipient to take an adverse action such as selecting a link.
4. The URL/Link in the email directs the recipient to an unfamiliar website outside of the SSA intranet.

*View additional types of incidents and reporting guidance in the agency's Information Security Policy (ISP) and Scam Awareness webpage.

We encourage you to complete your own cybersecurity health check. Review the agency's Information Security Policy and visit OIS' Cybersecurity Communication & Training Portal, SSA's one stop shop for cybersecurity communications, awareness, and training resources to help complete your health check.

Missed a previous Health Check? Stay current by reviewing previous issues on OIS' Cybersecurity Health Check's webpage. Should you have any questions, please email ^OIS Information Security Training.

Like the information in this health check? Let us know by selecting the smile face or frown face link.

Survey Reflections

Survey Reflections addresses the previous quarter's Cybersecurity Health Check. OIS would like to provide additional guidance based on comments and questions raised in the survey. Thank you for your participation!

Prior Reflections

Thank you to our survey respondents for your feedback. Your comments and suggestions are valuable to us. Popular topics in the survey included phishing, training, and systems upgrades. Based on the Cybersecurity Health Check survey responses, OIS recommends the following:

- We encourage users to refer to SSA's Social Engineering Resources page for guidance in handling phishing and vishing attacks.
- Stay informed about the cybersecurity trends and threats from around the world by subscribing to Cybersecurity Weekly. All links to external sites in the newsletter are safe and come from reliable sources on the Web, which should be accessible from your SSA-issued device. However, it is good cyber hygiene to always be vigilant when accessing external sites. You do this by

researching the company to see their review and verify that the URL begins with HTTPS (secure communication protocol) in the address bar.