fissea

Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review the rules before completing this entry form (pay attention to the due date). No late entries will be accepted. Be sure to fill this form out completely and email it with your entry to fissea-contest@nist.gov. Please submit an entry form with each entry.

Name of submitter: Mike Ginn

Name(s) to be printed on award certificate if your entry is selected as the winner:

Division of Information Security; Policy and Security Awareness Team

Organization:

Indian Health Service (IHS)

Please list how the organization should be listed under the name(s) on the award certificate if your entry is selected as the winner:

Office of Information Technology
Indian Health Service

Address:

Indian Health Service
5600 Fishers Lane
Rockville, MD 20857

Phone: 301-443-3733

Email Address: Mike.Ginn@ihs.gov

Type of Entry:

Please list the entry type below: it should be one of the 6 categories (poster, newsletter, website, motivational item, video, training scenario)

Training and Education Scenario/Exercise

Title of Entry: IHS Ethical Phishing Campaign

Description of Entry (use up to but no more than 500 words):

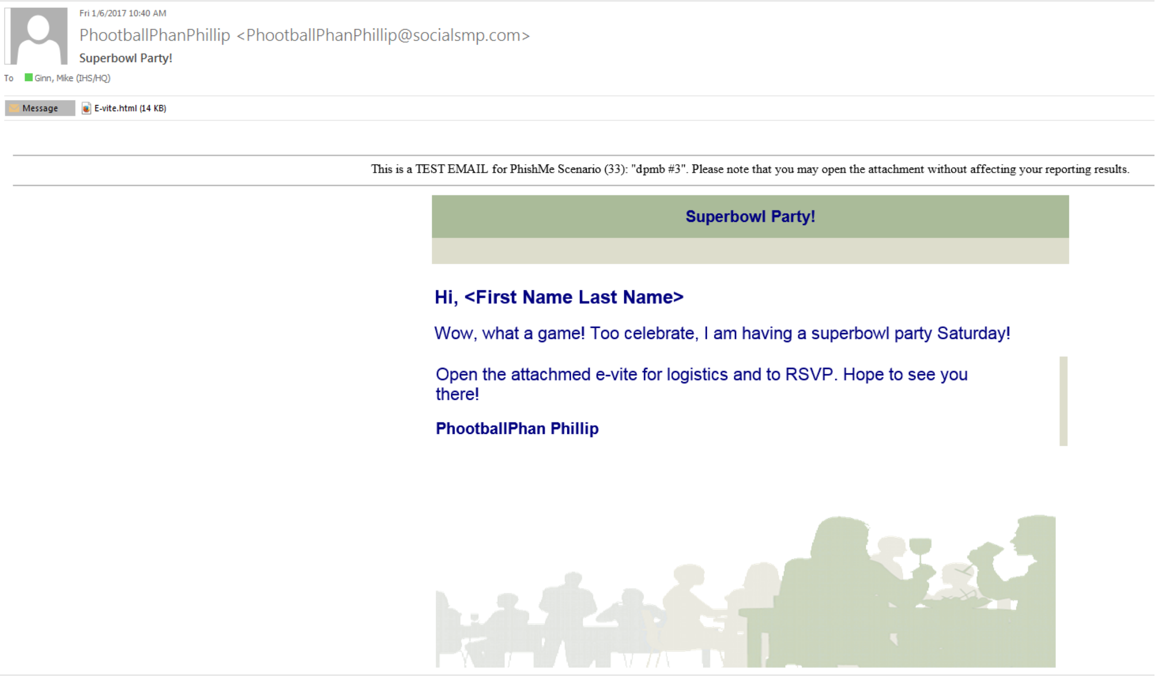
Ethical phishing is a method of heightening cybersecurity awareness and reducing susceptibility to email-based social engineering attacks. Recipients who engage in simulated phishing campaigns receive immediate, targeted education to help them better identify and respond to phishing schemes. IHS began implementing ethical phishing in early 2016. Our campaigns simulate real-world phishing attempts in a safe environment, typically employing an email that entices recipients to click a link, open an attachment, or launch or populate fields on a webpage.

For this award category, we are entering one of our campaigns that targeted a division in our organization. Users in this division received an email that appeared to be inviting them to a Super Bowl party. Deliberate hints were contained within the message to give clues to the recipient that it could be malicious:

- The email originated from the domain socialsmp.com, which is an unknown domain that does not appear to be consistent with IHS.
- Grammar and spelling errors were included.
- The Super Bowl is on Sunday, but the message referred to a Saturday party.

If the recipient opened the attachment they were immediately presented with an education page. IHS, graphics were utilized and IHS was identified as the facilitator. Education included information that will help the recipient recognize when an attachment might be malicious. The education as well as the phishing email is included in this submission.

Phishing Email Sent Out



Fri 1/6/2017 10:40 AM

PhootballPhanPhillip <PhootballPhanPhillip@socialsmp.com>

Superbowl Party!

To 🟩 Ginn, Mike (IHS/HQ)

E-vite.html (14 KB)

This is a TEST EMAIL for PhishMe Scenario (33): "dpmb #3". Please note that you may open the attachment without affecting your reporting results.

Superbowl Party!

Hi, <First Name Last Name>

Wow, what a game! Too celebrate, I am having a superbowl party Saturday!

Open the attachmed e-vite for logistics and to RSVP. Hope to see you there!

PhootballPhan Phillip

Landing Page (this was displayed if the recipient opened the attachment)

INDIAN HEALTH SERVICE · PHS · 1955

This was an authorized IHS phishing simulation.

If you receive an email at work that you suspect is a phishing attack, report it right away to the Cybersecurity Incident Response Team at csirt@ihs.gov. For any questions or feedback related to this exercise, email cybersecurity@ihs.gov.

Unhealthy Attachments

For years, spear phishers have used file attachments to spread malicious software (malware) through email messages.

Such attachments might contain spyware that allows them to steal your credentials, or viruses that cripple your machine and allow them access to your system or network.

Symptoms may not be obvious right away, but be assured these unhealthy attachments are infectious; your computer and your information are vulnerable as soon as you open one. You might be contagious too, spreading your virus to the rest of the network!

How Was I Supposed to Know?

Sometimes, identifying unhealthy attachments is tough, even for the experts. However, there are some clues that can help you recognize when an attachment might be carrying something malicious that can spread.

- **The attachment is out of context:** For instance, you receive a file named "Payroll," and you work in nursing.
- **You weren't expecting an attachment:** When someone you don’t know asks you to review an attachment, it could be a trick.
- **The type of file attached is not consistent with the function of the file you’re supposed to be opening:** If you are asked to review a document, for example, but the file extension is an executable file (.exe), don’t download.

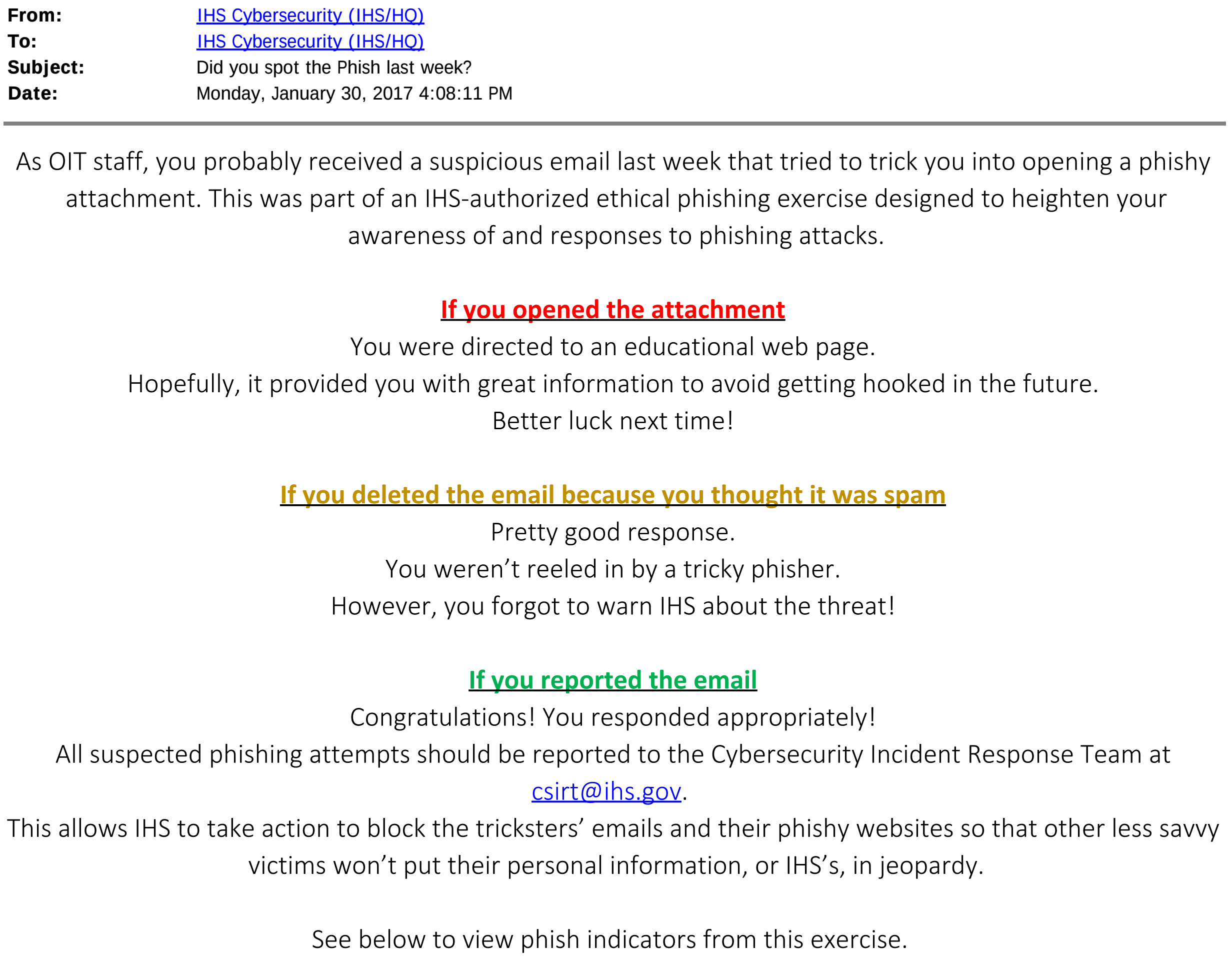
- **The file extension appears to contain two file types:** If you receive a file called "wiring_process.pdf.exe," for example, the sender is probably trying to make the file appear innocent upon first glance.

Spear-phishers can also place malicious attachments inside a compressed folder (.zip file) to make it appear more innocent. Plus, password-protected .zip files have a higher chance of making it past your spam filters and into your inbox.

It’s important to remember that all sorts of common file types can contain embedded code – that includes Word documents, .pdf files, and web coded files. Examine the context clues closely!

If you suspect that you have received a spear-phishing email at work, report it immediately to the IHS Cybersecurity Incident Response Team, by email at csirt@ihs.gov. For any questions please reach out to your Headquarters ISSO - Benjamin Koshy (benjamin.koshy@ihs.gov) or cybersecurity@ihs.gov.

Communication at the End of the Campaign



From: IHS Cybersecurity (IHS/HQ)
To: IHS Cybersecurity (IHS/HQ)
Subject: Did you spot the Phish last week?
Date: Monday, January 30, 2017 4:08:11 PM

As OIT staff, you probably received a suspicious email last week that tried to trick you into opening a phishy attachment. This was part of an IHS-authorized ethical phishing exercise designed to heighten your awareness of and responses to phishing attacks.

If you opened the attachment

You were directed to an educational web page.
Hopefully, it provided you with great information to avoid getting hooked in the future.
Better luck next time!

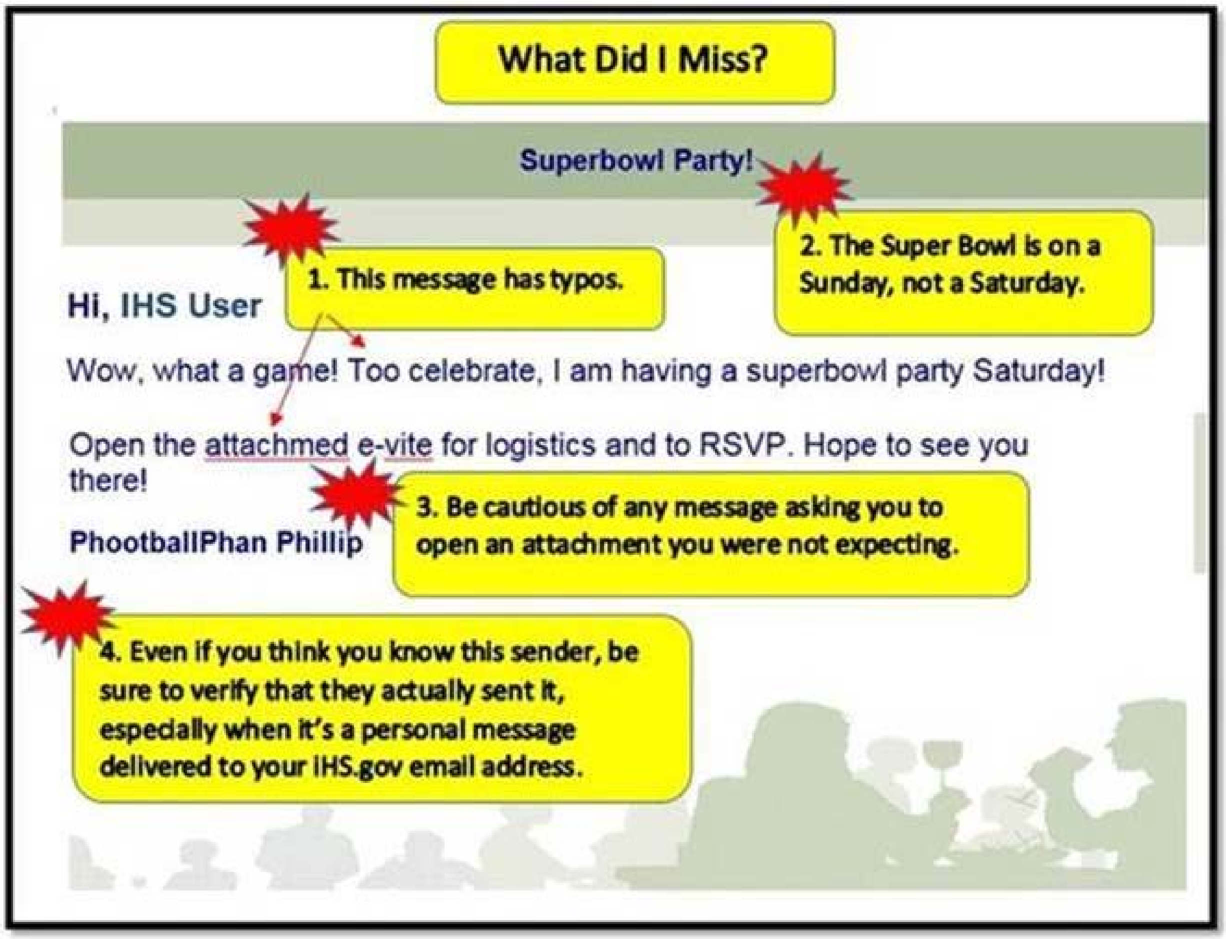
If you deleted the email because you thought it was spam

Pretty good response.
You weren't reeled in by a tricky phisher.
However, you forgot to warn IHS about the threat!

If you reported the email

Congratulations! You responded appropriately!
All suspected phishing attempts should be reported to the Cybersecurity Incident Response Team at csirt@ihs.gov.
This allows IHS to take action to block the tricksters' emails and their phishy websites so that other less savvy victims won't put their personal information, or IHS's, in jeopardy.

See below to view phish indicators from this exercise.



What Did I Miss?

Superbowl Party!

Hi, IHS User

Wow, what a game! Too celebrate, I am having a superbowl party Saturday!

Open the attachmed e-vite for logistics and to RSVP. Hope to see you there!

PhootballPhan Phillip

1. This message has typos.

2. The Super Bowl is on a Sunday, not a Saturday.

3. Be cautious of any message asking you to open an attachment you were not expecting.

4. Even if you think you know this sender, be sure to verify that they actually sent it, especially when it's a personal message delivered to your IHS.gov email address.

Indian Health Service
Office of Information Technology

Division of Information Security

cybersecurity@ihs.gov