

Phishing...

Don't take the bait!

Complete this activity to check your phishing facts.

Phishers target people across IHS, from those in leadership positions to entry-level employees.

No matter what their role in IHS is, everyone will be targeted at some point.

Phishing can happen when you're not expecting it.

What can happen if you're phished? Click the tabs to see!

Identity Theft

Scammers can use your personal information to steal your money, your reputation, and your identity!

Identity thieves can open lines of credit in your name. Even if you aren't stuck paying the bill, your credit may still suffer.

PHI Theft

Protected Health Information (PHI) is more valuable to cyber criminals than credit card information. PHI includes the victim's personal information and oftentimes that of their family members as well.

PHI thieves can file fraudulent reimbursement claims, exceed the victim's insurance caps, change their medical history and diagnoses, or even steal their prescriptions.

Extortion

Ransomware is a type of malware that prevents you from accessing your system or files until a ransom is paid. Some ransomware encrypts certain file types and attempts to force victims to buy a decryption key.

As many as 93% of all phishing emails now contain ransomware, according to a new study by PhishMe.

Embarrassment

Phishers can attack you through cell phone texts, email, websites, and social media accounts. A phisher with your information can use it to target your friends and family. Using your hijacked email or social media account, criminals can pose as you to win the unwary trust of your contacts and steal their information and identities as well.

Why Me?

As a consumer, phishers target you for your finances and online accounts. As a computer user, phishers target you to gain control of your computer and/or your organizational network.

As an IHS employee, phishers target you for patient information and other IHS network resources.

Email is a
Common
Setting for
Phish Bait.

Email offers effective delivery methods--like corrupt attachments or malicious links. Vast numbers of victims can be emailed in very little time.

Email provides anonymity.

Email addresses aren't hard to obtain. As federal staff, it's especially easy for phishers to figure out your IHS email.

Hover over the blue boxes for details...

From: John Doe
To: IHS Wise Guy
Subject: WebMail Migration
Message: WebMail_Migration.pdf (909 KB)

Wise Guy,

This is to inform you that we are in the process of migrate our email infrastructure to the Windows 2015 platform, which includes eliminating certain email server mailboxes.

Attached is a document outlining the benefits of this new and improved email service we request you to your Windows password before 8 PM on Tuesday. Failure to do so will result in being locked out of your email account!

Please click here to update your password.

Thank you,

Joe Doe

When an attachment comes from someone you don't know or when you weren't expecting a file, make sure it's legitimate before opening it.

Spear phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.

Roll your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click!

Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.

Urgency

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.

Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.

Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

Note the email signature.

A signature block that is overly generic or doesn't follow agency protocol could indicate something is wrong.

Note the sender address.

If the address doesn't match the sender name, be suspicious of the entire email!

Note the email tone.

We know how our coworkers and friends talk, so if an email sounds strange, it's probably worth a second look.

Question 1 of 5

Multiple Choice

Which of the following should you do to foil the phisher? (Check all that apply.)

- A) Keep your security software and browsers up to date.
- B) Hover over links to identify obvious fakes.
- C) Take your time inspecting email; look for bad grammar or poor-quality graphics.
- D) Double check an email's fabulous offer by visiting the retailer's website directly by a known URL.

What are some types of bait phishers commonly use to trick their victim?
Any of These!

Dear Friend,

My car broke down in Dangertown, PA and I'm out of cash and food and the bad guys are after me! :(

Please send money to my paypal account here.

Your friend John

Don't just send money to your friend's Paypal account! Call him to see if he really is in trouble!

Dear Mr. So & So,

Bill Gates is giving a free iPad to everyone who participates in this survey!

Just click here to get yours tomorrow!

Thanks!

The Apple Customer Appreciation Rep

Bill Gates has no need to secure customer loyalty! Don't fall for these. They're almost ALWAYS a hoax.

Dear Bank of the Planet Customer,
We regret to inform you that your account has been compromised. Please reset your password at this link.
Without immediate action, your account could be locked.
Your Banking Team

This is a classic phishing ploy, but if you think it could be legitimate, call your bank by a KNOWN customer service number! Visit their website directly; don't follow the email link.

Their delivery might vary, but nearly all phishers ask you to take immediate action to prevent some disaster or to earn some prize. Hover over the samples above for tips on responding to these phishing attacks.

Question 2 of 5

True/False

Warning that "your account has been accessed!" is one tactic phishers might use to make you click on a link.

- A) True
- B) False

Phishers might try to scare you about some other hacker!

TRUE!

It's ironic but true! Phishers often try to scare you with warnings about some other dirty-rotten crook trying to take you and your accounts for a ride.

Always be suspicious of emails warning you to take immediate action to prevent something awful -- like a hack-attack -- from happening.

If you're asked to log in to your account to fix a problem, go directly to the organization's website or call them at a known number (not one provided in the email) before clicking that link.

Hover your mouse over the link to reveal the actual URL and examine it for legitimacy. Remember that the text directly in front of the .com indicates the web domain. www.paypal-bank.com is not the same as www. paypal.com. All manner of files can contain malicious code, even Word, Excel, and PowerPoint files! Besides, cyber-savvy criminals can disguise file extensions or hide them in zip files.

Click the pyramid blocks for simple rules

Is the attachment out of context or the file type out of place? Take these as clues and follow the rules below.

- 1) Stranger Danger! Never trust an attachment from someone you don't know!
- 2) Friend or Foe? Don't assume every attachment from a familiar source is ok! Emails can be hacked or spoofed. Malware can also be spread unwittingly by someone who just wants to share something interesting!
- 3) Better Safe than Sorry. before you open any attachment, scan it using a trusted malware scanner.

Also, Exercise

Caution

When

Visiting

Websites.

Some phony websites look real. Examine the URL closely, and make sure it's https.

Legitimate websites can also be infiltrated.

Internet ads can be detours to malware sites.

Emails, text messages, and legitimate websites can lure victims to phony websites. Be especially cautious with login forms. Just because it looks authentic, that doesn't mean it is.

Question 3 of 5

Multiple Choice

What can happen if you're lured to a phony website? (Check all that apply.)

- A) Invisible content can automatically launch malware.
- B) Login prompts can provide crooks with access to many of your accounts.
- C) Clicking on an item can initiate configuration changes to your system.
- D) Invisible threats can run amok on your system and monitor your actions.

The answer is all of these!

What can happen if I get lured to a phony website?

Any of These!

Website-hosted malware is sneaky!

Clicking on an item on a website or even just visiting a compromised site can initiate download and launch spyware, adware, or viruses on your computer.

It can download ransomware, you say??

Ransomware is an increasingly popular and particularly insidious malicious software.

Ransomware hackers might encrypt your files, move your operating system data, or delete key system data, rendering your files or your entire system inaccessible.

They do this by convincing you to launch their malicious code.

How do they convince you to do such a thing? Typically, by exploiting your fears through phishing emails or compromised websites.

You may know someone whose home PC was taken hostage by ransomware.

They may have received a message saying their computer was locked down due to some criminal activity and that they must pay a "fine" to regain access. Or perhaps the crooks made no such pretense, simply stating:

"Your files are encrypted. Pay up!"

Question 4 of 5

Fill-In-The-Blank

Ransomware hackers are so successful because they exploit your fears. Fill in the blanks below to identify the fears successful ransomware is based on.

- 1) Fear of (hackers) taking control of your accounts compels you to immediately follow their directions to prevent it.
- 2) Fear of (malware) on your computer convinces you to download their own "PC Cleaning" ransomware.
- 3) Fear of losing (important files) convinces you to pay their demanded ransom.

Exploiting my f-f-f-fears!

Exploiting your fear that a crook might access your online shopping or banking accounts is a great way to prompt you to take hasty actions to prevent loss. In reality, you may be exposing yourself to their nefarious schemes!

Ransomers might try to make you think some other bad guy's malware is the threat, and if you allow them to, they'll remove it for a minimal fee. But allowing them access to your system might give them the opportunity to do even worse things!

When a ransomer does take control of your system, they can take control of your life! The idea of losing precious pictures, legal documents, or other personal files can compel you to pay any price.

Most
Importantly!
Know What
to Do if you
Get Phished!

Don't ignore them! Report all phishing attempts to local IT staff!
Change your passwords, especially any you saved to your browser!
Don't use an infected computer to report the incident or to update passwords!

Whether you fall for them or not, phishing attempts should always be reported. This will help ensure culprit sites are blocked and other users won't be victimized.

Question 5 of 5

Matching

Match the following unexpected email messages with the person you should contact for questions.

CSIRT or your ISSO

Your Coworker

Your local IT staff or system administrator.

- A) An email from an ihs.net address asking you to review an attachment.
- B) An email from an ihs.gov address asking you to change your expiring password at this link.
- C) An email from a coworker asking you to sign up for the office potluck on the attached spreadsheet. An email from a coworker asking you to sign up for the office potluck on the attached spreadsheet.

Who should I contact when I receive an unexpected or suspicious email?

An email from a sender with a questionable email address should always be a red flag. If you receive an email about IHS or organizational business, be immediately suspicious if it doesn't come from the ihs.gov or related organizational domain. Contact your ISSO or CSIRT@ihs.gov to report it, because it could be a phishing attack that someone less savvy might fall for!

An email from your coworker is generally safe. However, email addresses can be spoofed or hacked by cyber-crooks! If you receive an email from a coworker that seems out of place or uncharacteristic, contact them directly to confirm the message came from them.

We all receive messages at times about expiring passwords. If the message comes from a recognized ihs.gov email address, it's usually legitimate. However, be cautious with any link you receive in an email, and hover over it with your mouse before you click, to see where it's actually going to take you.

What if my IHS machine is compromised?
Follow These Steps!

If you take the bait in a phishing attack or notice that your machine appears to be compromised, do not log off or power down your computer. Lock your computer with the screen saver lock.

Don't think twice about reporting it. Better to report a non-incident than to not report a real one. Immediately notify your local ISSO or the Incident Response Team.

After you've taken the mitigating steps, do some research and consider the implications. Make sure you take appropriate precautions, like changing all your passwords.

Congratulations!

You've completed the ISSA Phishing Activity.

Click the "Complete Don't Take the Bait Training Module" button below to continue.