Contest

Categories
- Website
- Motivational Item
- Poster
- Newsletter
- Training
- Video

Judges
- Not affiliated with any of the groups that submitted entries
- From various positions and industries
Website Entries (4)
Disaster Recovery & Contingency Planning (DRCP) Center of Excellence (CoE) Training Site

IHS has information technology (IT) plans in place so that they can respond to and manage adverse situations involving IT. These plans should be maintained in a state of readiness, which should entail training personnel to fulfill their roles and responsibilities within the plan, exercising plans to validate their content, and testing systems and components to ensure operability in the specified environment. These three types of events can be carried out efficiently and effectively through the development and implementation of a test, training, and exercise (TTE) program.

Test: Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment specified in an IT plan. For example, an organization could test if call tree cascades can be executed within prescribed time limits; another test would be removing power from a system or system component.

A test is conducted in as close to an operational environment as possible. If feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used. The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an IT plan. Tests often focus on recovery and backup operations; however, testing varies depending on the goal of the test and its relation to a specific IT plan.

Training: For the purposes of this publication, training refers only to informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities. Doing so prepares them for participation in exercises, tests, and actual emergency situations related to the IT plan.
Be Vigilant. Not a Victim.

USPS is committed to educating the public about today's cyber security risks and empowering everyone with ways to better protect themselves.

Scroll down to find the information most relevant to you.

Recent Threats
Stay informed of the latest threats. Learn more.

Recent Articles
- Cybersecurity Insurance: Does Your Business Need It?
- Jury Duty Scams and How to Avoid Them
- Job Posting Scams and How to Avoid Them

How Cyber Smart Are You?
Take the CyberSafe at USPS® evaluation and find out.

Explore Articles Tailored to You
Website Winner!
Evonne Thomas

Organization:
US Postal Service Corporate Information Security Office (USPS CISO)
Be Vigilant. Not a Victim.

USPS is committed to educating the public about today's cyber security risks and empowering everyone with ways to better protect themselves.

Scroll down to find the information most relevant to you.

Recent Threats
- Stay informed of the latest Ransomware attack. Click here for latest updates.

Multiple Days Ransomware Infestations Reported
- Learn more at Ransomware.gov

Ransomware Continues to Threaten Businesses
- Learn more at CyberSafe at USPS

Recent Articles
- Cybersecurity Insurance: Does Your Business Need It?
  - Learn about the types of cyber policies insurance companies offer and what to consider if you purchase one.
  - Learn More

- Jury Duty Scams and How to Avoid Them
  - Learn how scammers are targeting citizens with fraudulent jury duty fines and email scams.
  - Learn More

- Job Posting Scams and How to Avoid Them
  - Learn the many ways unscrupulous job scammers and how to best avoid their traps.
  - Learn More

How Cyber Smart Are You?
Take the CyberSafe at USPS evaluation and find out.

Explore Articles Tailored to You
Motivational Item Entries (5)
FRONT of T-Shirt

be aware.

diligence defeats social engineering
- be cyberwyze!

BACK of T-Shirt
PHISHING: DON'T TAKE THE BAIT

What is Phishing?
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and financial details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

PHISHING TARGETS
- Money
- Banking and Credit Card Info
- PII-Personally Identifiable Information
- Passwords

Be cautious about opening attachments or clicking on links in emails (even from your contacts).

Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear.

Dear User,
Check your account

Hover over links to verify the link's actual destination, even if it is from a trusted source.

Don't Click- it's a fake site!

Backup your files regularly to protect yourself against virus or ransomware attack.

STOP.THINK.CONNECT.

IDENTITY THEFT PROTECTION TIPS

DID YOU KNOW:
50% of American adults (110 million) had their personal information exposed by cybercriminals in 2016 alone.

Identity theft has been at the top of the Federal Trade Commission’s Top Consumer Complaints list for 15 years in a row.

2/3 of Americans (65 percent) who use the Internet received at least one online scam offer during 2013.

HOW TO PROTECT YOURSELF:
- Be careful on public wifi networks.
  - Do not use online banking, check work email, or access any other sensitive information while on public wifi.
  - Limit card use during travel. It’s best to limit card use when traveling outside of the US.

- Be careful shopping online.
  - Pay with an online wallet, i.e. PayPal to eliminate credit card fraud risks.
  - Guard your information online.
    - Set strong passwords and change them periodically.
    - Set up banking and fraud alerts. Use two factor authorization when available.

- Shred sensitive documents.
  - Do not throw out sensitive documents in the mail without shredding such as bank statements, documents with PII etc.

- Monitor your bank and credit card statements.

TOP METHODS OF STOLEN IDENTITY ARE:
- Stolen Wallet/Purse
- Stolen Social Security Number
- Stolen Mail
Motivational Item Winner!
K Rudolph, Niomi Rosenberg, Amira Armond, G. Mark Hardy, & Bryan Walthall

Organization:
Native Intelligence, Inc.
Poster Entries (15)
Backup Safely

Don't mix business and personal cloud storage.
VA CLOUD COMPUTING
IAM Services Impact Analysis

TEN STEPS TO ENSURE SUCCESS

1. Ensure effective governance, risk, and compliance processes exist.
2. Audit operational and business processes.
3. Manage people, roles, and identities.
4. Ensure proper protection of data and information.
5. Ensure privacy practices.
6. Assess the security provisions for cloud applications.
7. Ensure cloud network and connectivity protection.
8. Evaluate security controls on physical infrastructure and facilities.
9. Manage security issues in the cloud.
10. Understand the security requirements of the end process.

CLOUD SERVICE MODELS

SOFTWARE AS A SERVICE (SaaS)

PLATFORM AS A SERVICE (PaaS)

INFRASTRUCTURE AS A SERVICE (IaaS)

RISKS

- Cost increase
- Loss of control
- Loss of security
- Lack of interoperability
- Increased complexity
- Vendor lock-in
- Security risks
- Data management
- Legal and regulatory issues
- Performance and availability
- Compliance issues

BE PREPARED TO WEATHER ANY STORM WITH THE RECOMMENDATIONS OF SASA IAM

Verify security controls and key service contracts are in place. Identify the correct monitoring controls such as server scans. Consider the impact of any additional controls. Ensure effective governance, risk, and compliance processes exist. Audit operational and business processes. Manage people, roles, and identities. Ensure the security provisions for cloud applications. Ensure cloud network and connectivity protection. Evaluate security controls on physical infrastructure and facilities. Manage security issues in the cloud. Understand the security requirements of the end process.

*Based on VA Cloud Computing IAM Services Impact Analysis, VA HealthCare Center for more information.
National Cybersecurity Awareness Month

OCTOBER 2017

See Yourself Working in Cybersecurity

ORIGINAL LINEUP! REUNITED!

The Employed
Playing all the hits off their "Careers in Cybersecurity" album:
"Rockin' Security Engineer"
"ISSO, Is Do You"
"Hey There, Information Security Analyst"
"Security Architect of My Heart"
"CISO Strut"
"She Was a Crytographser"

CAPTAIN CYBERSECURITY SAYS...

I WANT YOU FOR CYBERSECURITY

HTTPS://WWW.CYBERCAREERS.GOV

Cybersecurity threats are on the rise, and we need passionate professionals to protect Indian Health Service (IHS) patient information!

Be a Cybersecurity IHS Super Hero and join our cause by staying cyberaware with security tips like the ones below.

TAKEN

[Various cybersecurity tips and tricks]

Don't Need Passwords
Don't need you to get in,
Just need your feedback.

Don't Let the Vultures
Have your data.

[More cybersecurity tips continued]
At IFDS, information security is everyone's responsibility. Don't get "Busted by Bogey".
In cybersecurity, there should be no ifs, ands, or butts!
Don’t Get Tricked!

Think Before You Click

Use these best practices to identify and avoid phishing attacks:

- Slow down and analyze your email messages.
- Be cautious when opening unsolicited email messages.
- Before clicking a link, hover over it on a desktop or hold it for several seconds on a mobile device to preview the true destination of a link.
- If you were not expecting an email with an attachment, don’t open it until you are certain that it is harmless.
- Never give out your password to anyone! ED Customer Service Desk staff, ED IT Systems Help Desk staff, and other legitimate personnel from your organization, will never ask you for your password.

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

The strongest password you can make is a passphrase that's memorable to you - and nobody else!

Follow CyberCARE's tips to protect your sensitive information.

- Change your passwords often!
- Change the default password!
- Avoid the obvious!
- Don't set browsers to auto-fill usernames and passwords!
- Watch out! Shared computers can record your keystrokes... and passwords!
Are you the only one tracking your run?

When using fitness trackers, mobile devices, and other apps with geotagging, remember you may be broadcasting more than you realize.
WRITE YOUR BIGGEST REGRET

CLICKING THAT LINK.

Not being a better friend
Not trusting my gut
Working too much
Trading 10,000 bitcoins for pizza

Tattoo of her name
Not standing up to that bully
Not having kids

Burning bridges!!
Posting while angry
Not saying "I love you."

HAD SEPER. NOT HAVING KIDS
HAVING KIDS!
SLEPT WITH BEST FRIEND

Think Before You Click.
(and Be Kind)
CMS CYBERSECURITY IS LOOKIN’ NICE

Strengthening CYBERSECURITY with the NICE Framework

The NEW 2018 Cybersecurity and Privacy Training Catalog now includes training opportunities mapped to the NICE (National Initiative for Cybersecurity Education) Framework.

How does NICE help you?

NICE describes cybersecurity work roles. These are now mapped to the Training Catalog. This makes it easier to find role-based cybersecurity training and education programs.

What are NICE Categories?

There are seven categories within the framework comprised of specialty areas and work roles. Look for the categories in the Training Catalog and in future training opportunities at CMS.

Armed with the right knowledge, we’ll be better equipped to secure CMS.

February 2018 v.10C
You’re not familiar with the concept of attraction?

- Michael Crichton, Jurassic Park

Clever cyber criminals are. Think before you click.
CyberSafe at USPS

Separate for Security

NEVER

Never connect your personal or work devices to USPS computers, equipment or networks.

MOBILE PHONES - TABLETS - WEARABLE TECHNOLOGY - HEADPHONES - HOUSEHOLD EQUIPMENT - WMM ENABLED TOYS AND GADGETS

KEEP USPS NETWORKS SAFE
If you need to charge a device, use an outlet.

Stop and Think, before you Connect.

Report suspicious emails to CSOC immediately by selecting the email(s) and clicking the Report to CyberSafe button in the Outlook toolbar. For all other information security incidents, email cybersafe@usps.gov.
DO NOT open or download when emails say ✗

- you won lottery'
- fund for you'
- your legal heirs sent money'
- send me your account details'
- free for you to try'
- ransom requested'
- transferred money to your account'
- here is data you requested'
- mail from bank asking for personal info'
- mail from unknown entity asking personal info'

DO open or download emails only if ✓

- do not pose security risks/challenges'
- Pay attention to ‘from domain’ in email’
- you trust sender'
- you think relevant for you/your business'
- email does not sound creepy'
- do not click on link in email unless you are sure it is safe to do so'
- be careful opening large attachment'

Simple Rules to Keep your Systems & Network Safe

Security is always important, Say NO to Spam, Spoofing, Phishing, Junk, Ransomware, Data breaches or unsolicited emails
Phishful Thinking

Should I open this attachment?

DON'T
• Open email from unknown sources
• Enter personal information
• Enter system credentials

DO
• Examine the sender's email address
• Move mouse over links to determine validity
• Report emails to soc@nasa.gov immediately

IF A LINK LOOKS PHISHY, DON'T OPEN IT!
Phishing is a form of social engineering in which cyber criminals trick people into providing personal information by pretending to be someone they are not.

Learn more:
IT Security Awareness & Training Center
https://www.grc.nasa.gov/ITSA/itsecurity-threats/phishing

www.nasa.gov
Be Aware...
Understand Outlook Auto-Complete

CLICK WITH CARE

The Microsoft Outlook Auto-Complete feature provides you with a list of suggested recipients based on the first letter or two you enter into the To, CC, or BCC field in an email. Be aware; you may accidently choose the wrong recipient and send sensitive data to the wrong individual.

Outlook has features intended to reduce the risk of sending email to unwanted external recipients. Demonstrated in the email below are some of these features and indicators you should be aware of:

1. Warning indicator that the sender is external to the NRC
2. External recipient address in a different color (blue) than the internal address below it (black)
3. Ensure your attachment is correct.

We are all accountable for managing sensitive information
CLICK WITH CARE
Poster Winner!
Office of Information Technology

Organization:
Indian Health Service
National Cybersecurity Awareness Month
OCTOBER 2017
See Yourself Working in Cybersecurity

ORIGIONAL LINEUP! REUNITED!

The Employed
Playing all the hits off their "Careers in Cybersecurity" album:
- "Rockin' Security Engineer"
- "ISSO, I Da Yo"
- "Hey There, Information Security Analyst"
- "Security Architect of My Heart"
- "CIO Strut"
- "She Was a Cryptographer"

CAPTAIN CYBERSECURITY SAYS...
I WANT YOU FOR CYBERSECURITY
HTTPS://WWW.CYBERCAREERS.GOV

Cybersecurity threats are on the rise, and we need passionate professionals to protect Indian Health Service (IHS) patient information!

Be a Cybersecurity IHS Super Hero and join our cause by staying cyberaware of security tips like the ones below.

TAKE ONE

- Report suspicious activity
- Lock your computer
- Avoid clicking on suspicious links
- Keep software up to date
- Use strong passwords
- Be cautious with financial information
- Keep your phone secure
- Be aware of phishing attempts
Phishing

Security Architecture Software Assurance (SASA) Identity and Access Management (IAM) provides information designed to help those on the frontline defend against malicious threats. One of the most prevalent forms of cyber attack is… Phishing.

Phishing attacks seek personal information from an individual or company by posing as a trustworthy organization or entity. Attackers often use email, sending messages to users that appear to be from an institution, or company with which the individual has familiarity.

Below is information on three different forms of phishing, and tips on how to reduce your vulnerabilities.

**Spear Phishing**
Spear phishing is when attackers utilize a more targeted and personalized approach to increase chances of tricking recipients. Attackers will gather publicly available information on targets such as their name, position, company, work phone number or other information to trick the recipient into believing that they have a connection with the sender.

Typically hackers will target individuals whose roles and responsibilities require important network and system access, simply put… those who may have the “keys to the kingdom.”

**Example:** An example of this is reaching out to Network and Security Operations Center (NSOC) personnel by posing as an organization of interest or close affiliation like NIST. Hackers can easily find government organization charts and the identities of key personnel through an online search.

**Whale Phishing**
Whaling, or whale phishing, is a type of phishing attack where hackers target “big fish,” typically executives and high profile users, using social-engineering tactics to trick them into divulging highly valuable or competitive information.

**Example:** An example of this would be emailing cabinet secretaries or members of congress using the presidential seal, or letterhead template, which can be easily found through a simple google search.

**Water Hole Phishing**
Water hole phishing is when an attacker targets a website typically frequented by the individuals they’re trying to exploit. By infecting the website, visitors can inadvertently get infected without even knowing it.

**Example:** Hackers might infect a site that they know government employees trust as reputable such as Health and Human Services (HHS) or Healthcare Information and Management Systems Society (HIMSS).

Help spread the word about the importance of phishing prevention by downloading and sharing our SASA IAM Anti-Phishing posters and infographic.
2017 IN REVIEW HEALTHCARE BREACHES

The healthcare sector has a lot of information that can be valuable to criminals and thus it is an attractive target. Healthcare organizations often have personal information that criminals can use for traditional financial fraud – things like names and Social Security numbers. Such organizations also have health insurance information, which can be more valuable because malicious actors can use it to commit medical fraud such as obtaining free medical care, purchasing medical equipment, or acquiring payment for fraudulent services.

Many breaches were in the news in 2017, which resulted from exposed websites, unencrypted storage drives, and users falling for phishing schemes.

This article highlights some of the largest healthcare breaches that occurred in 2017 and some key points that will help you do your part to make sure Indian Health Service (IHS) is safeguarding patients’ information so we don’t make the news for the wrong reasons!

RANSOMWARE. The Women’s Health Care Group of Pennsylvania notified 300,000 patients that a ransomware attack had put their personal health information at risk. The clinic discovered in May that a server and workstation located at one of its offices had been “infected by a virus designed to block access to system files.”

IHS Tips. Early warning signs of a potential malware infection include: emails, text messages, or other types of peer-to-peer messages indicating you won something or owe a payment; computers running slower than usual; and unusual or new types of pop-up windows showing up.

PHISHING ATTACK. UC Davis Health notified 15,000 patients of a security breach after an employee fell prey to an email phishing scam and disclosed login credentials. The cybercriminal used these credentials to send emails to other staff members and requested bank transfers for large sums of money.

IHS Tips. Think before you click! Hover over links that you are unsure of before clicking on them, and pay attention to the website’s URL. A malicious website may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net). Phishers like to use scare tactics and may threaten to disable an account or delay services until you update certain information.

(CONTINUED ON PAGE 2)
Partner Security

In 2017, hackers breached the Amazon accounts of several third-party vendors using stolen credentials to post fake deals and steal cash. Other examples of well-publicized breaches involving third-party attacks include:

Target, which was attacked through an HVAC contractor.

Medical Informatics Engineering, whose investigation showed NoMeraClipBoard, a subsidiary, was using a legacy system with inadequate network and application security, open to SQL injection.

Home Depot, where criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network, and then acquired elevated rights that allowed them to deploy unique, custom-built malware on its self-checkout systems in the US and Canada.

Boston Medical Center, which hired third-party vendor MDK Transcription after the company posted health records and demographic data of 15,000 patients to the vendor’s website with no password protection.

Mystery

Methodist Hospital in Henderson, Kentucky declared an “internal state of emergency,” shut down all hospital desktop computers, and reverted to paper-based procedures.

How did this happen?
Send your answer, with a suggestion for how to prevent such a breach to Security. Your answer enters you in a drawing for a fabulous prize.

3 Actions

If your job involves third-party vendors, you can help secure the data.

• Document who handles your data, how it's maintained, and where it travels throughout its lifecycle.

• Ask third party vendors how they are protecting your data. Use a business agreement with vendors that details the types of security measures the vendor must use when handling your data. Include an independent audit clause that verifies the vendor's compliance with specific security protocols.

• Engage your IT support early in the project to validate secure data connections and information storage.

Security Analogy

Robbery is illegal, but people still find it prudent to lock doors and close windows in their homes; so too must we lock up our information systems.

Never say anything on the phone that you wouldn't want your mother to hear at your trial.
— Sydney Biddle Barrows

We want to hear from you! security_contact@your.org
Spotlight: Practice Cybersafe Shopping this Holiday Season!

Online shopping is one very convenient way to find the perfect gift for everyone on your list this holiday season – but did you know that online shopping can put you at risk of a cyberattack? Make sure that you know the risks and are practicing your cybersafe shopping habits!

Cyberattackers target online shoppers in many ways, including fake website and email scams, hacking vulnerable computers, and intercepting financial information when a vendor’s webpage is not encrypted. Be sure that you are shopping safely online by sticking to the following tips:

1) **Only shop at reputable vendors:** When in doubt, do your research by checking the vendor’s reputation with the Better Business Bureau.

2) **Make sure that websites are encrypted:** Before you share any personal or financial information, check that the website’s URL begins with “https” rather than “http” to make sure a website is encrypted.

3) **Don’t respond to emails requesting personally identifiable information:** Legitimate businesses won’t request information this way.

4) **Use a credit card instead of a debit card:** Credit cards often offer additional protections against fraud in case you are the victim of a cyberattack.

5) **Avoid shopping on public computers:** Shop on your personal computer using a secure internet connection to avoid making your information vulnerable.

For more tips, check out additional guidance from CyberSafe at USPS.

Watch the “Report to CyberSafe” Video!

CIO Kristin Seever narrated a short video, available on Blue, on the Report to CyberSafe Outlook button. The animated video emphasizes the importance of protecting the Postal Service, its employees and customers by reporting suspicious emails using the new button. Be sure to watch the video to learn more!

Learn New Terms in the Cybersecurity Glossary

To further improve CISO’s cyber fluency, here are a few more cybersecurity terms that start with the letter I:

- **Inorganic growth** is growth in the operations of a business that arises from mergers or takeovers, rather than an increase in the company’s own business activity. Firms that choose to grow inorganically can gain access to new markets and fresh ideas that become available through successful mergers and acquisitions.

- **Insider Threat** is a current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.

- **Internet Protocol Security (IPsec)** uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, and data confidentiality (encryption), and replay protection.

- **Intrusion** is an incident of unauthorized access to a network or device.

- **Intrusion detection** is a security management system for computers and networks that gathers and analyzes information to identify possible security breaches, which include both intrusions from outside the organization and misuse within the organization.

- **IT Security** is preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Stay tuned for “K” and “L” cybersecurity terms in the next edition!
**BLUETOOTH HACK AFFECTS 20 MILLION HOME DEVICES**

A series of recently disclosed critical Bluetooth flaws that affect billions of Android, iOS, Windows and Linux devices have now been discovered in millions of Artificial Intelligence (AI)-based voice-activated personal assistants, including Google Home and Amazon Echo. The name of this sophisticated attack is BlueBorne and it is exploiting a total of eight Bluetooth implementation vulnerabilities.

As estimated during the discovery of this devastating threat, several Internet of Things (IoT) and smart devices whose operating systems are often updated less frequently than smartphones and desktops are also vulnerable to BlueBorne. The IoT security firm who initially discovered this issue has now disclosed that an estimated 20 million Amazon Echo and Google Home devices are also vulnerable to attacks leveraging the BlueBorne vulnerabilities. Read more about this at: https://thehackernews.com/2017/11/amazon-alexa-hacking-bluetooth.html

**WHY PRIVACY OF INFORMATION IS SO IMPORTANT**

In today’s world, most people are digitally connected and must think about safety and security both on and offline. Personal devices make it easier to connect to the world around us, but these tools also store a substantial amount of personal information regarding users and their habits. Invariably, personal devices are targets for cybercriminals.

Human mistakes account for the vast majority of information security incidents and data breaches. Some of the biggest risks are people putting data where it doesn’t belong, not following policies, losing portable electronic devices containing data, and falling for phishing and social engineering schemes.

The success of NASA’s missions and objectives are contingent upon how effectively everyone does their part in securing information and information systems. It is important to follow NASA policies and guidelines and remain vigilant with your security habits both at work and at home.

Information Security Awareness
Phishing Attempts using Email

Be Aware - Don’t Open. Don’t Download. Don’t Forward.

Don’t compromise DHS information or its computer systems by falling for a phishing attack e.g., opening an email, clicking on a link, or downloading a file attachment from someone posing as a reputable source. Most phishing emails seem legitimate and appear to come from a known source by spoofing the header and email addresses however, you must stay vigilant and avoid these common pitfalls ...

Don’t Open.
Avoid opening emails or embedded email hyperlinks from known or unknown sources – they should be deleted immediately!

Can you identify the clues in this phishing email example?
From: ITSupport <alters@hq.dhs.gov>
Subject: Please verify your email address
Thank you for contacting the DHS help desk. In order to better serves you, we must verify your email address. For your protection, this email is being sent to you via secured email.

Instructions:
Click on the link below.
From the verification page, enter your contact information to confirm your identities.

Next, click the submit button which will send us the confirmation that your verification has been submitted.

Secured email access: Verify your account here

Don’t Download.
Avoid downloading unexpected email attachments embedded in suspicious emails – they should be deleted immediately!

Don’t Forward.
Avoid responding to & forwarding suspicious emails from known or unknown sources to others – when in doubt, contact the DHS HQ, CIRT team!

Report any suspicious activity or a potential incident to DHS HQ, IT:
☎ 1-800-250-7911
✉ ITSupport@hq.dhs.gov

To report phishing attempts notify:
✉ DHSspam@hq.dhs.gov

If you think you are a victim of a phishing attack, contact DHS HQ, CIRT:
✉ RMDISIncidentResponse@hq.dhs.gov

If you have additional questions regarding the “Be Aware” Program, contact:
✉ NPDITSecurityTraining@hq.dhs.gov

Answers to email example: mismatched names with an invalid email address, several mispellings, embedded email hyperlink is a caution!
Newsletter Winner!
Robert Cunningham

Organization:
Department of Veterans Affairs
Phishing

Phishing attacks seek personal information from an individual or company by posing as a trustworthy organization or entity. Attackers often use email, sending messages to users that appear to be from an institution, or company with which the individual has familiarity.

Below is information on three different forms of phishing, and tips on how to reduce your vulnerabilities.

Spear Phishing

Spear phishing is when attackers utilize a more targeted and personalized approach to increase chances of fooling recipients. Attackers will gather publicly available information on targets such as their name, position, company, work phone number or other information to trick the recipient into believing that they have a connection with the sender. Typically, hackers target individuals whose roles and responsibilities require important network and system access, simply put, those who may have the “keys to the kingdom.”

Example: An example of this is reaching out to Network and Security Operations Center (NSOC) personnel by posing as an organization of interest or close affiliation like NIST. Hackers can easily find government organization charts and the identities of key personnel through an online search.

Whale Phishing

Whaling, or whale phishing, is a kind of phishing attack where hackers target “big fish” typically executives and high profile end users, using social-engineering tactics to trick them into divulging highly valuable or confidential information.

Example: An example of this would be emailing cabinet secretaries or members of congress using the presidential seal, or letterhead template, which can be easily found through a simple google search.

Water Hole Phishing

Water hole phishing is when an attacker targets a website typically frequented by the individuals they’re trying to exploit. By infecting the website, visitors can inadvertently get infected without even knowing it.

Example: Hackers might infect a site they know government employees visit such as “Health and Human Services” or “Healthcare Information and Management Systems Society (HIMSS).”

Help spread the word about the importance of phishing prevention by downloading and sharing our SASTA IAM Anti-Phishing posters and infographics.

Prevention “How to spot a phish”

Phishing is most often initiated through email, but can come in other forms of communication. Regardless of the method, there are ways to distinguish suspicious items from those that are legitimate. Telling employees on how to recognize these malicious attempts is one of the most fundamental steps to data protection. The following may be indicators that an email or website is a phishing attempt rather than a legitimate form of communication.

1. First consider the obvious, if the email is part of a thread there is a low risk that it’s malicious
2. Look at the sender address, you can usually double click to check if the address looks correct
3. Check for any misspellings or grammatical errors
4. Hover over mouse over linked items to check their link address
5. Do not open attachments but right click them and save in a “safe” folder, then right click and look at the “properties” for inconsistencies, or after right clicking “View in a text editor” like notepad

DON’T TAKE THE BAIT!

Prevent a phishing attack by using caution when opening suspicious emails.
Training Entries (6)
Cybersecurity Awareness Interactive Module

IHS wants to involve all personnel in the conversation about IT security, so we designed the interactive module with effective delivery of content in mind, and a goal of making security lessons meaningful to everyone. This module gives trainees the opportunity to stop sitting there watching, and start participating.

Trainees are prompted to use their mouse to roll over images or click on screen elements to get answers and further explore content.

Recurring quizzes throughout the presentation keep them engaged by periodically compelling them to think about what they’re viewing and make practical sense of it.

*Take Away:* By prompting trainees to take action to learn more, we engage their minds through hands-on exploration.
Exercise Phishing Email

Training is most effective when presented in a real world context. Therefore as part of each authorized exercise, a simulated spear phishing email is delivered without prior notification (i.e., blind exercise) to assess the ability of Department personnel to distinguish legitimate email from spear phishing messages.

**eCard Delivery**

Someone you know has sent you warm wishes for this Autumn season!

**To:** employee@iestemail.com

---

Someone you know has sent you warm wishes for this Autumn season!

You've received a very special Autumn eCard from someone you know. Click the link below to reveal your eCard, and to send an eCard of your own!

See your eCard

---

Having trouble viewing your eCard? We're here to help. Click here to contact customer support.

---

Email automatically generated for the account associated with email address. Please do not reply to this email. If you received this email in error or would prefer to stop receiving these emails, please click here to update your email preferences.

---

Privacy - Terms of Use - Customer Support - Email Preferences
Healthy Technology Lunch n’ Learn
Phishing at Sea
Recognizing and Reporting Phishing Attempts
You have been selected to be a member of the Department of State’s elite Cyber Task Force. Recently, Embassy Botchester was under a massive cyber attack. Your mission as a cyber special agent is to solve the details of the cyber attack — including the perpetrator, his/her city of origin, date of the crime, how the attack was carried out (methodology/tactic), and the perpetrator’s motivation. You must also list the 3 countermeasures or steps to teach people so this does not happen again.

Use the box of clues and this dossier to crack the codes and solve the puzzles. Fill out the Crime Report and submit it to your captain to escape the room and save Embassy Botchester!

SPECIAL NOTE: If you need help, your captain has provided 3 sealed envelopes with hints. However, each hint will add 5 minutes to your final completion time.

Good luck!
USPS CISO
OWASP Top 10

02/12/2018
Contingency Scenarios – Group Activity

Instructions

For this exercise, each group will be assigned one of the contingency scenarios listed below. Working together, each group should review their scenario and consider the following:

1. How would your organization be impacted by this contingency event?
2. How long could your organization continue its mission/operations?
3. How would you respond to this scenario?
4. What procedures/mechanisms would you like to be in place to assist in resolving the contingency event?
5. Depending on the nature of your system, what characteristics might affect your recovery strategy?

Be prepared to discuss your contingency scenario with the class.

Contingency Scenarios

Contingency Scenario A - Server Hard Drive Crash

The database server hosting your application has failed, resulting in the loss of all application data. This is a mission critical system that cannot remain offline for a long period of time without impacting your organization’s mission.

Contingency Scenario B - Physical Access Control System Failure

The Physical Access Control System that controls all the badge readers and access points in your building has failed and will be down for an indeterminate amount of time.

Contingency Scenario C - Fire in the Data Center

Your building has suffered a major fire over the weekend. The liquid based fire suppression system originally installed in the building was not removed when the data center was built. Therefore, your data center has suffered catastrophic water and electrical damage, resulting in an electrical fire in the data center.

Contingency Scenario D - Corrupt Database

After several help desk calls from system users, your database administrator investigates and discovers that many of your database files have been corrupted.

Contingency Scenario E - Power Outage

Due to age and recent weather conditions, the power relay station that supplies grid power to your building has suffered a catastrophic failure of the transformers used to distribute incoming power to the local grid. The utility company has located one replacement transformer that can be transported and installed in approximately two weeks, however this will only replace 25% of the required power. Complete restoration is expected to take six weeks.
Training Winner!
Exercise Phishing Email

Training is most effective when presented in a real world context. Therefore as part of each authorized exercise, a simulated spear phishing email is delivered without prior notification (i.e., blind exercise) to assess the ability of Department personnel to distinguish legitimate email from spear phishing messages.

**eCard Delivery**

Someone you know has sent you warm wishes for this Autumn season!

To: employee@testemail.com

---

**Someone you know has sent you warm wishes for this Autumn season!**

You've received a very special Autumn eCard from someone you know. Click the link below to reveal your eCard, and to send an eCard of your own!

[See your eCard]

---

Having trouble viewing your eCard? We're here to help. Click here to contact customer support.

---

Email automatically generated for the account associated with email address. Please do not reply to this email. If you received this email in error or would prefer to stop receiving these emails, please click here to update your email preferences.

---

Privacy - Terms of Use - Customer Support - Email Preferences
Video Entries (6)
https://youtu.be/OSwr4jyLPtA
Are you a Cyber Target?

https://www.powtoon.com/online-presentation/duetTaiU0pW/cyber-threats/?mode=movie
https://www.uspsecybersafe.com/articles/individuals/best-practices-for-staying-cybersafe-every-day/
https://youtu.be/UIOYRXXE35k
Video Winner!
Evonne Thomas

Organization:
US Postal Service Corporate
Information Security Office
(USPS CISO)
https://www.uspscybersafe.com/articles/individuals/best-practices-for-staying-cybersafe-every-day/
Peer’s Choice Awards

• Part of the Government Best Practice Session today
  • Stop by and see the full entries and descriptions up close
  • Vote for your favorites (1 from each category)
  • Winners will be announced during the closing session Wednesday
  • Peer’s Choice Award Winners will be listed along side the official Contest winners on the FISSEA Website

• No official award certificate... just bragging rights 😊
Thanks to all who submitted entries!

A special thanks to our judges!