Contest

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

Judges
- Not affiliated with any of the groups that submitted entries
- From various positions and industries
Website Entries (3)
Our home page features (in a rotating manner) current event items such as our video on phishing or Security Awareness Week.

The side menu bar provides quick access to other sections of the site.

Information Technology (IT) Security

IT Security not only concerns the proper handling and protection of electronic information but also safeguarding IT assets from physical and digital security threats.

Knowing the best security habits:

- Do you always lock your computer screen when you step away?
- When working with sensitive information, do you adjust your computer screen or use a closed room?
- Have you got a lock code on your Blackberry or other departments?
- Do you know how to spot a suspicious e-mail?
- Do you understand the "Need-to-know principle"?
- Do you regularly review and update your user profile, passwords?
- Do you know how to securely store, transmit and dispose of electronic information?
- If you are a manager, have you ensured all your employees have access to the security check?
- As a Manager, do you know how to oversee and control access to electronic information stored on the drive?

Put a HALT to Phishing

A look at the implications of phishing, and what employees can do to be sure that they do not get "hooked".

- Video (MP4, 144 MB)
- Transcript (DOCX, 29 KB)
The IT Security Awareness and Training Center (ITSATC) website is a resource for employees to find information regarding information and computer security. The Home Page provides easy navigation on the left for users to find what they need, as well as a search feature in the upper right and a Site Map across the top menu bar.
The purpose of this website is to provide awareness on FDA cloud-related topics, particularly regarding cloud security. Some common questions include: What is Cloud Computing? How can I benefit from using the cloud at the FDA and what steps do I need to take to make sure I am utilizing this benefit securely?

Cloud computing is a model that allows universal, convenient, on-demand network access to a shared pool of IT resources (e.g., networks, servers, storage, applications, and services) that can be quickly disassembled with ease due to minimal management effort or assistance by the service provider. Cloud computing provides wide information technology (IT) capabilities that are offered as a service over the Internet to multiple users at one time. For the official NIST definition of cloud computing please click here: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Web pages include:

- FDA Cloud Computing Home
- FAQs
- FedRAMP
- Definitions
- FDA Cloud Security Authorization Process
- FDA CSP Authorization Status
Diane Blocksom

Organization:
NASA IT Security Awareness and Training Center
The IT Security Awareness and Training Center (ITSATC) website is a resource for employees to find information regarding information and computer security. The Home Page provides easy navigation on the left for users to find what they need, as well as a search feature in the upper right and a Site Map across the top menu bar.
Motivational Item Entries (5)
Dispositifs autorisés seulement.
Vérifiez la politique!

Only authorized devices.
Check the policy!

ACTUAL SIZE = 2” x 2”
When traveling, keep laptops and mobile devices not in use; in the trunk to avoid abuse!
Keep a laptop inventory of all devices by tag# and a name responsible for it.
Security Awareness
Message Pen

• Use Strong Passwords, Phrases, Patterns
• Avoid Clicking On Unknown Links
• C3: Everyone’s Responsibility
• Keep Identity Information Private
• Keep Virus Scanning Software/OS Up To Date
• Manage a Positive Personal Reputation
Title of Entry: Stylus Pen

Description of Entry:

During our Information Security Week event held during National Cyber Security Awareness Month in October 2014, we wanted to give out an awareness item to match the current theme of the event. The theme for 2014 was “Security: It’s in Your Hands,” emphasizing the important role that employees play in keeping information safe at work and at home. The stylus pen with the logo “Security Matters” was a fun way to remind employees to always be secure online.
Motivational Item Winner!
Jane Moser

Organization:
Employment and Social Development Canada (ESDC)
Dispositifs autorisés seulement. Vérifiez la politique!

Only authorized devices. Check the policy!

Employment and Social Development Canada

ACTUAL SIZE = 2” x 2”
Poster Entries (9)
How IHS Helps Prevent You From Getting Fooled In

Phishers use many tactics to trick you out of sensitive information. But IHS works behind the scenes to protect you and keep our information safe!

Email campaigns are a popular method of phishing attacks.

Lucky for us, IHS has automatic spam filters that block much of the unwanted email before it gets to your mailbox.

C'mon buddy! You can trust me!

STOP

Download these delicious treats!

Another popular method of phishy exploitation is to convince you to download malware like keystroke-loggers or spyware onto your computer.

Click this very important link!

Do Not Enter

Hopefully you never click on a culprit link, but if you do, WebSense blocks network traffic to many known trouble spots.

Often, phishing emails contain links to phony websites, and urgent messages to follow the link to resolve some problem.

Don't Take the Bait! Phishers Can be Foiled!

IHS works hard to protect its users and its patients from sensitive information breaches. But IHS employees must be vigilant against social engineering too.

Social engineers can call you too. They might even visit you in person!

Hi! This is your IT Department. Can I have your account password?

Beware of anyone who asks you to disclose sensitive information!

Indian Health Service
Division of Information Security
Don’t be a bandwidth hog...

Limit audio/video streaming on Department networks.
Protect... Don’t Connect!

Never connect PERSONAL devices to your work PC.
(eg. MP3 player, smartphone, USB key)

Security is everyone’s responsibility!

http://iservice.prv
Security Walkabouts

A walkabout is the practice of auditing physical security safeguards by performing a periodic unannounced walk-through (during or after hours) of Geisinger facilities and campuses by ISO staff. This program applies to all Geisinger-owned facilities, entities and/or wherever the presence of Geisinger workforce exists.

The following list represents examples of the security safeguards audited during a walkabout:

- Don’t leave personal items out in the open.
- Don’t allow viewing of sensitive documents to anyone without a business need to see (during or after hours).
- Log out of all applications and lock your PC when you are finished using it. (Ctrl+Alt+Delete then Lock) or (Window key & Lock).
- Secure expensive equipment (laptops, PDAs, etc.) in locked drawers, file cabinets and offices.
- Keep your name badge secure when not in use.
- Secure sensitive material, shred or recycle what you don’t need.
- Check that PC monitors are not visible to patients.
- Check printers, faxes & copiers in a timely manner.
- Don’t give out information without knowing who, what, why it is needed.
- Close/lock doors with keypads, card readers and locks.
- Encrypt mobile devices (Laptops, PDAs, etc.) and lock up when not in use.
- Report lost or stolen devices to the Help Desk 570-271-8082 or the ISO right away.

During a security walkabout, if you’ve spotted practicing good security habits we leave a clip for you to be entered into a drawing. If you are lacking good habits, we leave a pamphlet letting you know what to do better to be secure or policy compliant.

For more information, please visit Geisinger’s ISO Website at http://info.web.geisinger.edu/iso/index.html or contact us by e-mail: INFOSECURITY@geisinger.edu

570-271-8119
Is Your Head In the Cloud?
Protecting Data Here, There & Everywhere!

CISO Security and Privacy Day
Tuesday, April 7th, 2015
9:00 a.m. – 12:00 p.m.
Before You Take the Plunge...

Consider the risks of your Internet activity.
Invasion of the DATA SNATCHERS

CREEPING HORROR...FROM THE DEPTHS OF YOUR EMAIL INBOX

One click is all it takes to...
Silently execute malware
Compromise your computer
Snatch sensitive information

THINK BEFORE YOU CLICK
STRONG PASSWORDS create stronger security for our Veterans

Office of Information Management and Technology (OIMT) is pleased to announce the release of the new:

**FDA Cloud Computing Website**

Questions about cloud computing security or cloud-related topics? Find out more by searching FDA Cloud Computing on Inside.FDA.

**Benefits of Cloud Computing**

1. Scalability and elasticity
2. On-demand self-services
3. Energy efficiency
4. Cost savings and cost avoidance
5. Faster deployment
6. Mobile impact

**Cloud Security Stakeholders**

**Federal Agencies**
- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP Process when authorizing
- Implement Cloud Controls

**3PAOs**
- Third Party Assessment Organizations
- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

**FedRAMP PMO & JAB**
- Establish Processes and Standards for Security Authorization
- Maintain Secure Repository of Available Security Packages
- Provisionally Authorize Systems That Have Greatest Ability to be Leveraged Government-wide

**What is FedRAMP?**

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves cost, time, and staff required to conduct redundant agency security assessments.
Poster Winner!
sTr(o)Ng P@ssSw(_)_rds

create stronger security for our Veterans

Newsletter Entries (5)
Information Security is an important consideration for everyone these days—especially for people who work in the healthcare industry. Even if you think you have no place in the information security landscape, chances are, you do. Regardless of the vocational duties assigned, as IHS employees you are responsible for protecting patient and personal information.

**Cybersecurity! It’s For Everyone!**

There are vital functions in the IHS work force regarding patient care, and people filling these roles may not always handle sensitive information. However, protecting IHS information resources, including Protected Health Information (PHI) and Personally Identifiable Information (PII) is everyone’s responsibility.

Take for example the Friendly sisters, whose day-to-day activities don’t seem to involve cybersecurity, but who are nevertheless responsible for keeping IHS resources and data safe. The Friendly sisters have been working at the hospital for years. They’re always helpful and courteous, but they are also prime candidates for security incidents!

**Meet Ethel Friendly...**

She works in housekeeping, and in her duties she cleans all areas of the hospital... even secured areas. Today she held the door so her coworker didn’t have to rummage through her pockets and bags to find her ID badge. How polite! HOWEVER, piggybacking into secured areas on someone else’s badge violates IHS policy.

Badged access ensures that IHS can track whoever enters secured areas. That way, incidents can be traced back to the appropriate party, rather than to the nice person who loaned their access badge to someone else.

**Meet Sally Friendly...**

While Nurse Sally Friendly was in her office today, her sister Ramona stopped in. Ramona was on break and was in a hurry to get back to work at the security desk. Since her sister was already logged in, she sent some emails from Sally’s account. That was convenient!

HOWEVER, accessing network resources with someone else’s login credentials violates IHS policy. Just like badges are used to monitor physical traffic in secured areas, login credentials are used to monitor virtual traffic in IT resources.

Never lend your credentials to anyone, even if you’re there in the same room. That way, incidents that may occur can be traced to the appropriate party.
October is National Cyber Security Awareness Month

The Internet is part of everyone’s life, every day. We use the Internet at work, home, for enjoyment, and to connect with those close to us.

However, being constantly connected brings increased risk of theft, fraud, and abuse. No country, industry, community, or individual is immune to cyber risks. As a nation, we face constant cyber threats against our critical infrastructure and economy. As individuals, cybersecurity risks can threaten our finances, identity, and privacy. Since our way of life depends on critical infrastructure and the digital technology that operates it, cybersecurity is one of our country’s most important national security priorities, and we each have a role to play—cybersecurity is a shared responsibility.

National Cyber Security Awareness Month is designed to engage and educate public and private sector partners through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident. October 2014 marks the 4th Annual National Cyber Security Awareness Month sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center.

Year-Round Tips and Resources to secure a Cybersecurity Knockout

You can follow simple steps to keep CMS yourself and your families assets, and personal information safe online. Here are a few tips all Internet users can leverage to practice cybersecurity during National Cyber Security Awareness Month and throughout the year:

- Set strong passwords and don’t share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates.
- Maintain an open dialogue with your family, friends, and community about Internet safety.
- Limit the amount of personal information you post online and use privacy settings to avoid sharing information widely.

Remember, be cautious about what you receive or read online—if it sounds too good to be true, it probably is.
Make Cybersecurity One of Your New Year’s Resolutions

For many, January marks the opportunity to start fresh and improve on the previous year by setting goals—“resolutions”—and striving to achieve them. Lose weight. Exercise more. Quit smoking. Wait, something is missing! No list of New Year’s resolutions is complete without “Remember Cybersecurity.” As an ED-Defender, protect yourself and the Department from cybercrime by resolving to:

1. Be cautious when opening unsolicited email messages
2. Not open attachments received in unsolicited email messages until I am certain the attachment is harmless
3. Not click on links received in unsolicited email messages or pop-up boxes
4. Not provide sensitive personal or Department information in response to email or phone requests
5. Use strong and unique passwords on my work and personal web accounts
6. Protect sensitive personally identifiable information (SPII) in email communications using encrypted, password-protected WinZip archives
7. Practice good situational awareness and protect sensitive information
8. Complete the Department’s Mandatory Cyber Security and Privacy Awareness Training ahead of the deadline
9. Understand my responsibilities for protecting privacy and ensuring information security and comply with the Department’s Rules of Behavior
10. Report known or suspected security incidents to and my Information System Security Officer (ISSO) as soon as possible
January 28
Data Privacy Day

Data Privacy Day is an international effort to empower and educate people to protect their privacy, control their digital footprint, and make the protection of privacy and data a priority in their lives.


Data flows freely in today's online world. All online participants, from home computer users to multinational corporations, need to be aware of the personal data others have entrusted to them and remain vigilant about protecting it. Good online citizenship means practicing conscientious data stewardship.

The National Cyber Security Alliance (NCSA), who assumed leadership of Data Privacy Day in August 2011, is a nonprofit, public-private partnership dedicated to cybersecurity education and awareness that is advised by a distinguished advisory committee of privacy professionals.

Contribute to the success of Data Privacy Day by taking a proactive approach to your online privacy and security, by following these steps from the National STOP. THINK. CONNECT.

Software Security Training Opportunity

NASA has procured training through Capital Inc., a consulting firm specializing in software security, and is offering computer-based training for Web Programming Techniques for Security Vulnerabilities for both civil servant and contractor employees. The purpose of this training is to reduce the number of web-related programming incidents and to strengthen NASA’s IT security posture.

Capital’s software security curriculum provides valuable knowledge across many roles within software development, software security, and quality assurance. The Capital training catalog contains over 20 courses that focus on the most common security defects found in web applications taken from the Open Web Application Security Project (OWASP) Top 10 list.

A complete list of available courses may be found on the IT Security Awareness and Training Center (ITSATC) website located at https://www.arc.nasa.gov/itsatc/training/cyber-training/course-listings.

Top Cybersecurity Risks
1. Social Engineering & Phishing
2. Compromise of NASA Information and Assets
3. Web Security
4. Compromise of User Accounts/Lost Devices
5. NASA-Identified Governance, Access Control, and Identity Management Vulnerabilities

Data provided by NASA’s 2016 Security of Operations Center
Is There Such a Thing as Privacy on the Internet?

Have you ever Googled yourself?

If you have, you might find a lot more than you bargained for. It is increasingly difficult to remain anonymous on the Internet. A lot of the information you’ll find on yourself online is already considered public information. For instance, when you buy a house, details of the transaction are recorded in the local courthouse, to include the purchase price and the names of the buyers and sellers.

It has become much easier to collect information about an individual by collecting public information and personal data you publish on social media sites (Facebook, Twitter, etc.). While there are certain things that will always be part of the public record (such as home sales), there are some things you can do to reduce your “digital footprint.”

Helpful Tips to Reduce Your Digital Footprint:
- If you are a Facebook user, make...
Newsletter Winner!
Wendy Andrews

Organization:
Indian Health Service
Information Security is an important consideration for everyone these days—especially for people who work in the healthcare industry. Even if you think you have no place in the information security landscape, chances are, you do. Regardless of the vocational duties assigned, as IHS employees you are responsible for protecting patient and personal information.

**Cybersecurity! It's For Everyone!**

There are vital functions in the IHS work force regarding patient care, and people filling these roles may not always handle sensitive information. However, protecting IHS information resources, including Protected Health Information (PHI) and Personally Identifiable Information (PII) is everyone's responsibility.

Take for example the Friendly sisters, whose day-to-day activities don't seem to involve cybersecurity, but who are nevertheless responsible for keeping IHS resources and data safe. The Friendly sisters have been working at the hospital for years. They're always helpful and courteous, but they are also prime candidates for security incidents!

### Meet Ethel Friendly...

She works in housekeeping, and in her duties she cleans all areas of the hospital... even secured areas. Today she held the door so her coworker didn't have to rummage through her pockets and bags to find her ID badge. How polite! HOWEVER, piggybacking into secured areas on someone else's badge violates IHS policy.

*Badged access ensures that IHS can track whoever enters secured areas. That way, incidents can be traced back to the appropriate party, rather than to the nice person who loaned their access badge to someone else.*

### Meet Sally Friendly...

While Nurse Sally Friendly was in her office today, her sister Ramona stopped in. Ramona was on break and was in a hurry to get back to work at the security desk. Since her sister was already logged in, she sent some emails from Sally's account. That was convenient!

HOWEVER, accessing network resources with someone else's login credentials violates IHS policy. Just like badges are used to monitor physical traffic in secured areas, login credentials are used to monitor virtual traffic in IT resources.

*Never lend your credentials to anyone, even if you're there in the same room. That way, incidents that may occur can be traced to the appropriate party.*
Training Entries (2)
This is the main screen of the application, that allows users to choose to learn more about 8 different IT security risk scenarios pertinent to the Government of Canada. The scenarios range from what to do with an unverified USB, how to spot a spear phishing e-mail, to what to do if your co-worker starts talking about sensitive work information in a public place.
Put a HALT to Phishing Video

Lorne Sundby
DG, Strategy, Planning, Architecture and Management
Training Winner!
Jane Moser

Organization:
Employment and Social Development Canada (ESDC)
Put a HALT to Phishing Video

Lorne Sundby
DG, Strategy, Planning, Architecture and Management
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!