FISSEA

Security Awareness, Training, and Education

Contest

Gretchen Morris

March 2015

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)

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

Search
Feedback

IT Security
Topics
Securing Information: Getting Started
Accessing and Storing
Transmitting
Transporting
Monitoring
Effective Security Habits
News and Alerts
Tools and Resources
DOs and DON'Ts
IT Security Dictionary
Learning
Frequently Asked Questions
Reporting IT Security Incidents
Video: Put a HALT to Phishing (MP4, 145 KB)
Key Links
Policies and Guidance
Contact Us
Branch Coordinators
IT Security Centre of Excellence
Regional Security Offices (RSO)
NHQ Security Contacts

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 departme
- 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, passwo
- Do you know how to securely store, transmit and dispose of e
- If you are a manager, have you ensured all your employees h check?
- As a Manager, do you know how to oversee and control acces information stored on the drive?

- Video (MP4, 144 MB)
- Transcript (DOCX, 29 KB)

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

Our home page features (in a rotating manner) current event items such as our video on phishing or Security Awareness Week.

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.

FDA Cloud Computing Web Site

The FDA Cloud Computing Website provides awareness on FDA cloud security related topics for employees.

Web pages include:

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

Website Winner!

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)

ACTUAL SIZE = 2” x 2”

January 2015

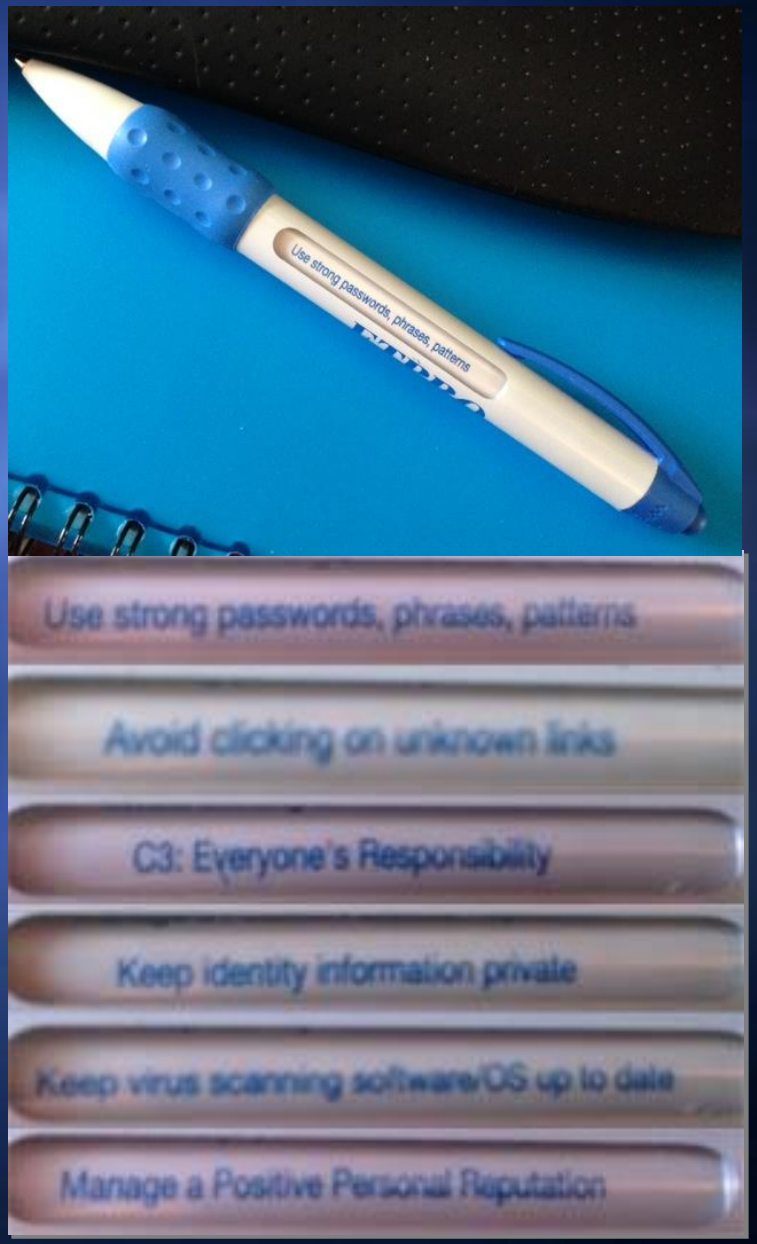
ISO Information Security Office

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

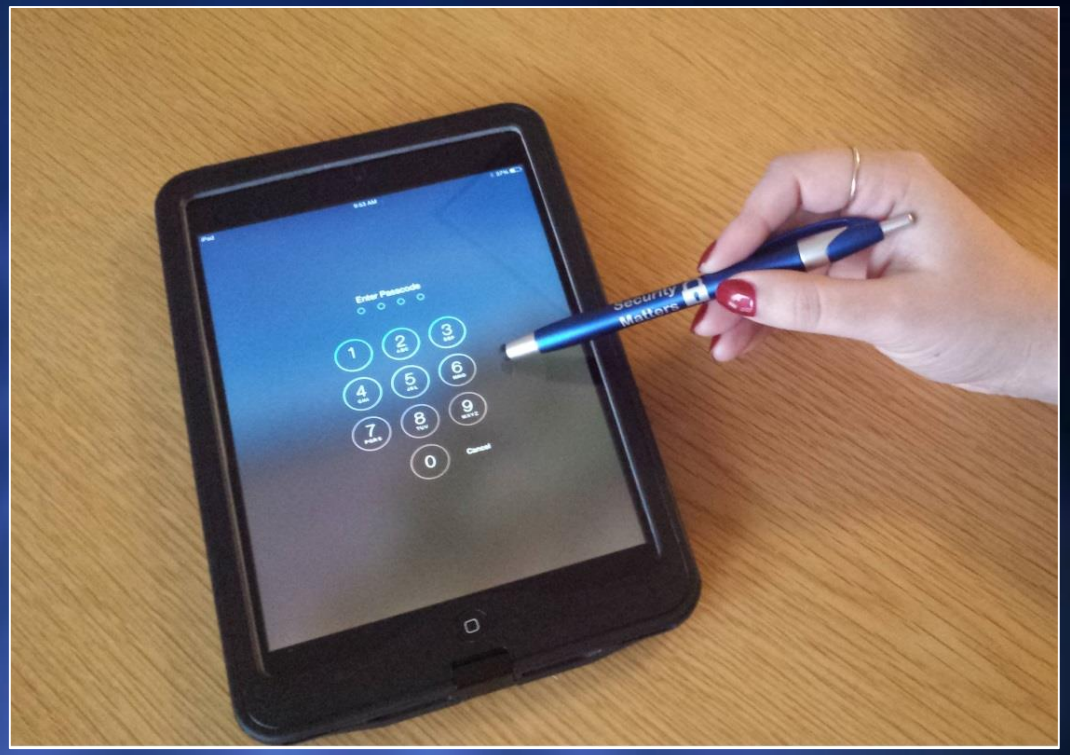



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
ISPG
Information Security
Privacy Group
certificate
encoded
authentication
system
protocol
password
shield
firewall
key
ssl
https
communications
spyware
encrypted
hackers
internet
key
virus
business
network
information
secure
access
privacy
browser
safety
guaranteed
2015 SECURITY AWARENESS & TRAINING CALENDAR
v1.3

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)

ACTUAL SIZE = 2” x 2”

Poster Entries (9)

CYBERSECURITY 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

How IHS Helps Prevent You From Getting Reeled In

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

It becomes a spearphishing attack when the crook targets you due to your affiliation with an organization. Sneaky spear phishers might even impersonate someone in your contacts list!

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

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

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

But IHS is prepared to battle the threat with automatic virus scans on all attachments and downloads.

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

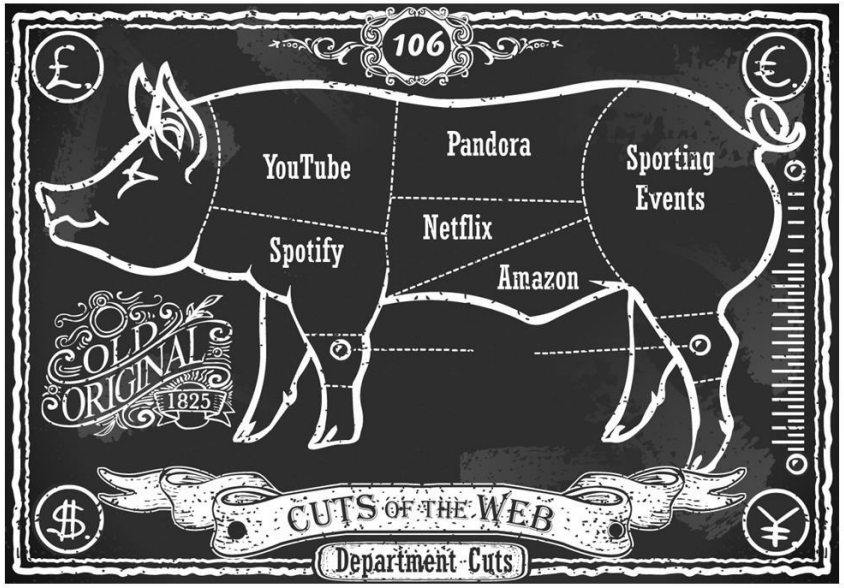
IHS works hard to protect its users and its patients from sensitive information breaches.

But IHS employees must be vigilant against social engineering too.

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

Beware of anyone who asks you to disclose sensitive information!

Don't be a bandwidth hog...



Limit audio/video streaming on Department networks.

Email us: Awareness@state.gov
Visit us: https://intranet.ds.state.sbu/DS/SI/CS/Awareness1
Office of Cybersecurity (DS\SI\CS)

CYBER SECURITY AWARENESS

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

Protégez...
ne branchez pas!

Ne branchez jamais d'appareils PERSONNELS dans votre PC de travail.

(p. ex. lecteur MP3, téléphone intelligent, clé USB)

La sécurité est la responsabilité de tous!

http://iservice.prv

ISO Information Security Office

Linking security solutions with business needs.

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 570-271-8092 or the ISO right away.

During a security walkabout if you're spotted practicing good security habits we leave a slip for you to be entered in to 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.

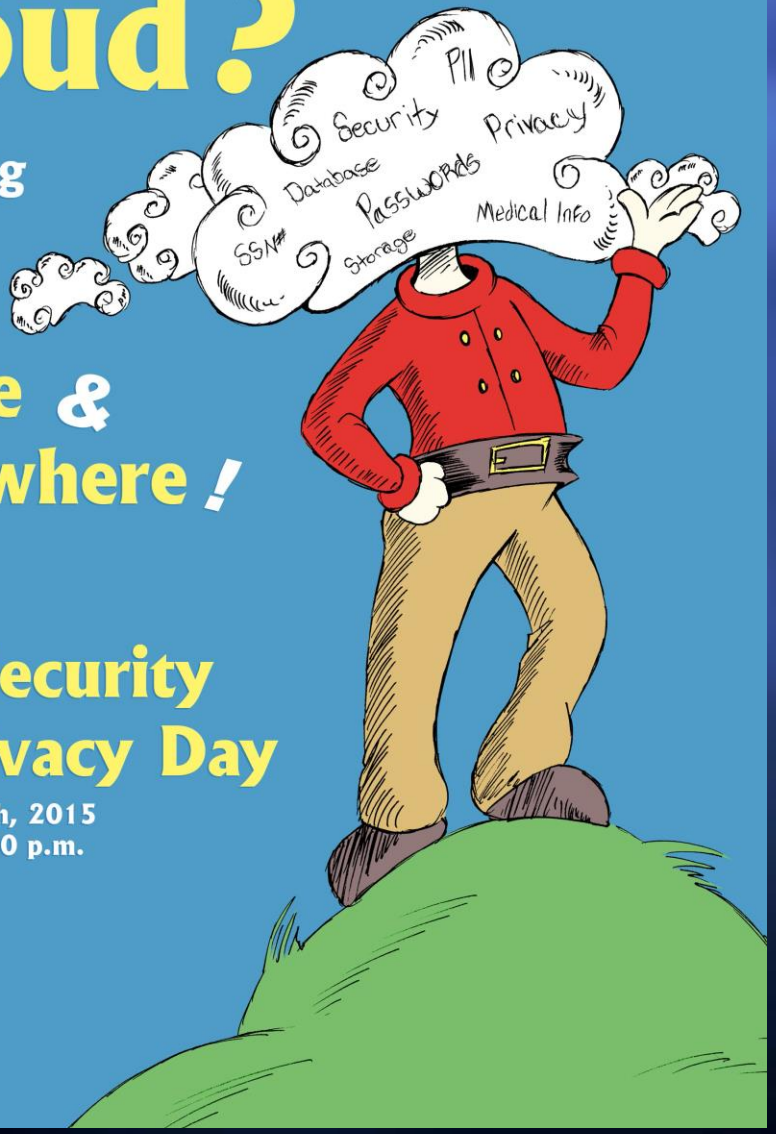
For more information please visit Geisinger's ISO Web site at http://infoweb.geisinger.edu/se_iso/index.html or contact us by e-mail: INFOSECURITY@geisinger.edu.

GEISINGER
REDEFINING BOUNDARIES

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
From: Mail Administrator <mail_admin@webaccess-email.com>
Subject: Your inbox is over the limit
Warning!
Your mailbox has exceeded the storage limit which is 20GB as set by your
Click here
to increase your mailbox size or you lose your account within 24 hours.
System Administrator Center
One click is all it takes to....
Silently execute malware
Compromise your computer
Snatch sensitive information
THINK BEFORE YOU CLICK

sTr(0)Ng P@sSw(_)rds

IT WORKFORCE DEVELOPMENT

More info? Visit vaww.itwd.va.gov.

create stronger security
for our Veterans

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

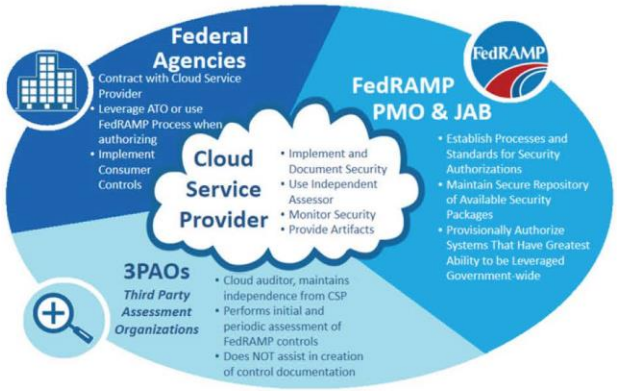
FDA Cloud Computing Website

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



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.

FDA OIMT
Office of Information Management and Technology

Poster Winner!

Kelly Wright

Organization:
VA IT Workforce Development

sTr(0)Ng P@sSw(_)rds

IT WORKFORCE DEVELOPMENT

More info? Visit vaww.itwd.va.gov.

create stronger security
for our Veterans

Newsletter Entries (5)

Cybersecurity 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

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!

Even non-security roles.

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.

ISSUE 2 | VOLUME 1 | October 2014

Security focus

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 11th 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:

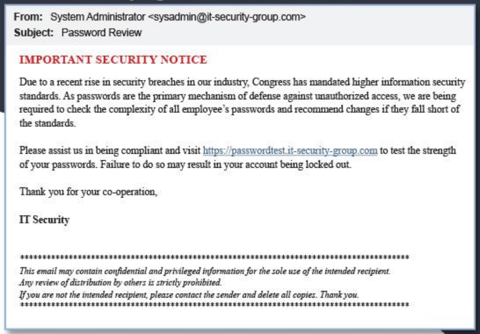
- Set strong passwords and don't share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates.
- Maintain an open dialogue with your family, friends, and community about Internet safety.
- Limit the amount of personal information you post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

Department of Education

Info Security News

Is this email a phishing scam?
See page 4 for the answer.



From: System Administrator <sysadmin@it-security-group.com>
Subject: Password Review

IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employee's passwords and recommend changes if they fall short of the standards.

Please assist us in being compliant and visit https://passwordtest.it-security-group.com to test the strength of your passwords. Failure to do so may result in your account being locked out.

Thank you for your co-operation,

IT Security

****

This email may contain confidential and privileged information for the sole use of the intended recipient. Any review of distribution by others is strictly prohibited. If you are not the intended recipient, please contact the sender and delete all copies. Thank you.

****

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 [illegible] and my Information System Security Officer (ISSO) as soon as possible

FRONTLINE

National Aeronautics and Space Administration

INFORMATION TECHNOLOGY SECURITY • OCIO • ITSD • ITSATC • WINTER 2014

QUARTERLY JOURNAL OF THE INFORMATION TECHNOLOGY SECURITY AWARENESS AND TRAINING CENTER

In this Issue

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 great priority in their lives.

Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the January 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Data Privacy Day is now a celebration for everyone, observed annually on January 28.

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 non-profit, public-private partnership dedicated to cyber security 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 Cigital, 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.

Cigital's software security curriculum provides valuable knowledge across many roles within software development, software security, and quality assurance. The Cigital 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.grc.nasa.gov/itsatc/training/cigital-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. NAPA IDENTIFIED GOVERNANCE, ACCESS CONTROL, AND IDENTITY *MANAGEMENT VULNERABILITIES*

Data provided by NASA's OCIO Security of Operations Center

May 2014 Issue 12

INFORMATION TECHNOLOGY DEFENDER

From the OIMT Information Security Program

Inside this issue:

Report an Incident

If you suspect lost, misplaced or stolen equipment, or a breach of Personally Identifiable Information (PII), notify your equipment manager **AND** contact the FDA Computer Security Incident Response Team (CSIRT) at:

- **Email: SecurityOperationsandResponse@fda.hhs.gov** or
- **Toll Free Number:** 855-5FDA-SOC (855-533-2762) (24x7)

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

Cybersecurity 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

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!

Even non-security roles.

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...

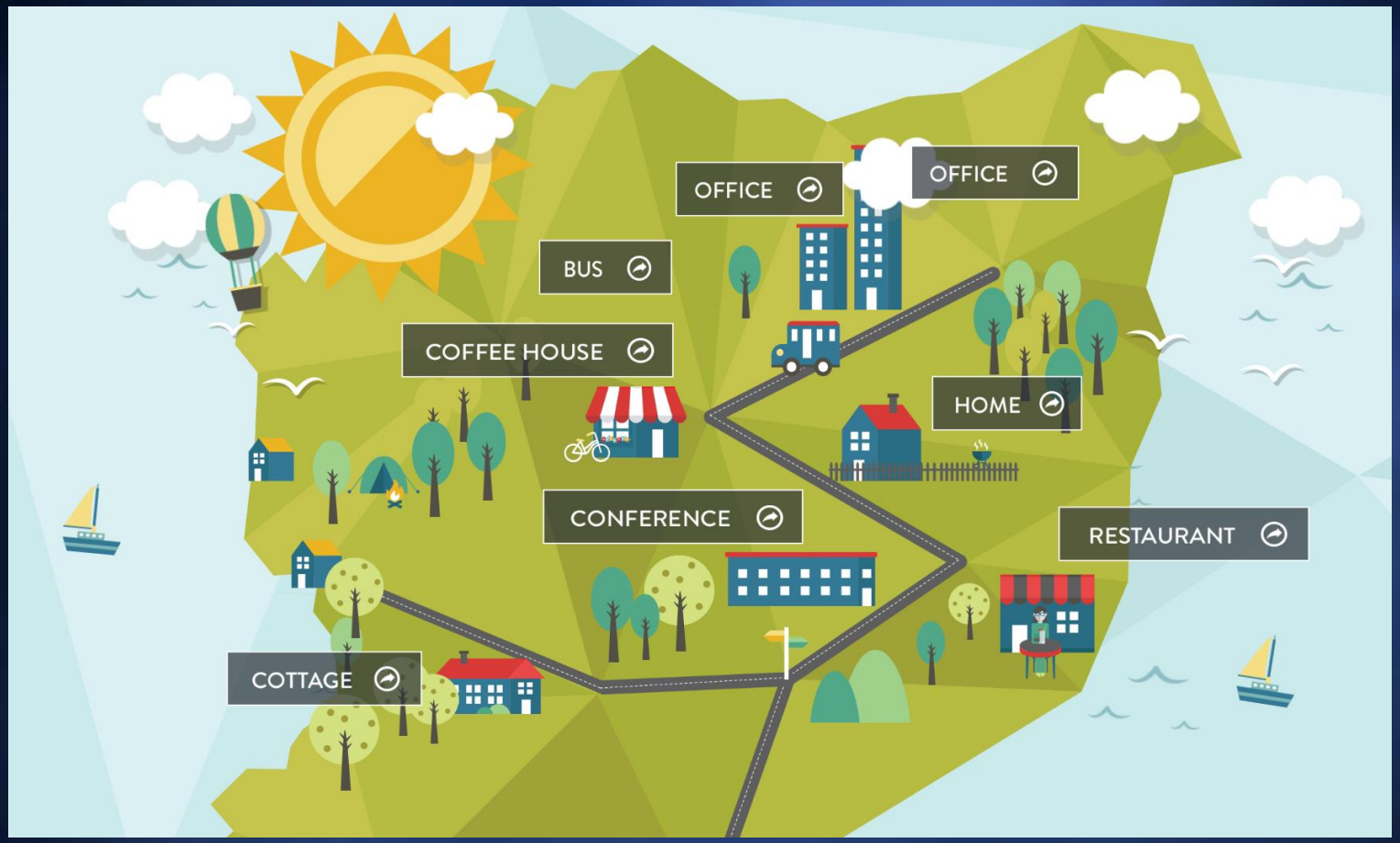
While Nurse Sally Friendly was in her office today, her sister Ramona stopped in. Ramona was on break and was in a hurry to get back to work at the security desk. Since her sister was already logged in, she sent some emails from Sally's account. That was convenient!

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)

Cyber Security Journey Map



- 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

Training Winner!

Jane Moser

Organization:
Employment and Social Development Canada (ESDC)

Put a HALT to Phishing Video

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!