FISSEA
Security Awareness, Training, and Education
Contest

Gretchen Morris, CISSP
FISSEA Working Group Member
March 2016
Contest

Categories

- Website
- Motivational Item
- Poster
- Newsletter
- Video *new!
- Training

Judges

- Not affiliated with any of the groups that submitted entries
- From various positions and industries
Website Entries (2)
2015 National Cybersecurity Awareness Month

Every one has a role when it comes to cybersecurity to be aware and implement certain safety measures. Your actions on the internet and on your work computer/equipment can make a significant impact.

“We now live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone’s daily life, whether we realize it or not. Recognizing the importance of cybersecurity to our nation, President Obama designated October as National Cyber Security Awareness Month. 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.” - Source: http://www.dhs.gov/national-cyber-security-awareness-month

Cybersecurity is a shared responsibility. During the 12th annual National Cyber Security Awareness Month, take a few moments to learn ways that we can all work together to protect FDA and personal information.

U.S. Food and Drug Administration National Cybersecurity Awareness Month Event:

Please join us to raise awareness about cybersecurity!

- Stop by our tables in front of the White Oak Great Room 1503 B to meet the Information Security Services Staff team.
- Get your questions answered and pick up free items with awareness tips to share with your peers.
- Listen to a variety of speakers present on hot security topics.

We look forward to seeing you there.

Monday, October 26, 2015 - White Oak Great Room 1503 B

<table>
<thead>
<tr>
<th>Time</th>
<th>Presenter</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 am - 9:15 am</td>
<td>Alan McClelland, FDA CISSP</td>
<td>Welcome/Introduction</td>
</tr>
<tr>
<td>9:15 am - 10:00 am</td>
<td>Sean Hardon, FDA IT Security Specialist</td>
<td>Cloud Security</td>
</tr>
<tr>
<td>10:00 am - 10:15 am</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>10:15 am - 11:00 am</td>
<td>Ruth Ross, National Institute of Standards and Technology (NIST)</td>
<td>Risk Management Framework (RMF)</td>
</tr>
<tr>
<td>11:00 am - 11:15 am</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>11:15 am - 12:00 pm</td>
<td>Martin Stanley, Department of Homeland Security (DHS)</td>
<td>Continuous Diagnostics and Mitigation (CDM)</td>
</tr>
</tbody>
</table>

About National Cybersecurity Awareness Month (NCSAM):

- http://www.staysafeonline.org/nCSAM/about

Helpful FDA IT Security Awareness Resources:

- IT Security Awareness Topics: http://inside.fda.gov/itsecurity/Communications/com244443.htm
- IT Security Awareness FAQs: http://inside.fda.gov/itsecurity/FAQs/default.htm

FDA IT Security Policies:


Help Promote NCSAM:

- Stay Safe Online: http://www.staysafeonline.org/nCSAM/get-involved/promote-nCSAM
- Stop, Think, Connect, Bookmark: http://www.fda.gov/aa/03/defaultfiles/publications/STC%20Brochure.pdf
- Stop, Think, Connect, Factsheet: http://www.fda.gov/aa/03/defaultfiles/publications/STC%20Factsheet.pdf
- Stop, Think, Connect, Start: http://www.fda.gov/aa/03/defaultfiles/publications/STC%20Start.pdf
- Stop, Think, Connect, Posters: http://www.fda.gov/aa/03/defaultfiles/publications/STC%20Poster.pdf
- Stop, Think, Connect, Brochure: http://www.fda.gov/aa/03/defaultfiles/publications/STC%20Brochure.pdf

For information on other security awareness topics click here for our main topics page.

Page Last Updated: 09/22/2015
HHS CyberCARE initiative reaches all HHS employees to include 80,000 federal employees and 40,000 contractors in all Operating Divisions across the Department. CyberCARE (Communication, Awareness, Response, and Education) leverages multifaceted communications platforms to socialize relevant, timely, memorable, and simple cybersecurity tips that resonate with a multifaceted HHS staff.

While we’re submitting our entry under the Website category, CyberCARE is so much more. We start with a theme each month ("Season's Teivings" in December, Cyber-Resolutions in January, Safer Internet Day in February, and Cyber Crime of Opportunity in March) and introduce it through a blast email to all staff. We post an attention-grabbing headline and graphic on a rotating banner and a voice of the customer (VOC) survey on the HHS intranet home page. All three of these communications lead our readers to interesting articles, stimulating Yammer social media conversations, and our Twitter account which socializes great tips for our internal and external customers.

Our monthly themes complement other cybersecurity awareness program initiatives including ethical phishing programs, printed media, National Cybersecurity Awareness Month (NCSAM), and ongoing cybersecurity awareness training. HHS CyberCARE builds upon and partners with other national-level efforts such as Stop.Think.Connect, CyberBullying, National Privacy Day, and Safer Internet Day.

One thing that sets CyberCARE apart from other initiatives is that, in addition to being relevant and topical, we strive to be conversational and write in a way so that we are talking to our readers, not at them. Our content is poignant, relevant, and often presented in humorous and even punny articles. We don’t want our readers to see the ‘same old stuff’, we want to engage them.

CyberCARE stands out because we’re not another droning, technical voice. We draw people in and get them interested and aware of the threats we face day in and day out. Check out some of our topics and posts on the following pages...

Each month the HHS intranet features a CyberCARE rotating banner that links to a cybersecurity topic. Each week CyberCARE posts a VOC survey pertaining to cybersecurity. It lets participants see how they compare with their colleagues while checking their cybersecurity knowledge. It also lets us know our readers a little better.
Website Winner!
Lisa Dorr, Sarah Moffat, Toney Rogers, and Jennifer Kimberly

Organization:
HHS, Office of Information Security (OIS), Governance, Risk Management, and Compliance (GRC) – Governance Division
HHS CyberCARE initiative reaches all HHS employees to include 80,000 federal employees and 40,000 contractors in all Operating Divisions across the Department. CyberCARE (Communication, Awareness, Response, and Education) leverages multifaceted communications platforms to socialize relevant, timely, memorable, and simple cybersecurity tips that resonate with a multifaceted HHS staff.

While we’re submitting our entry under the Website category, CyberCARE is so much more. We start with a theme each month (“Season’s Thieves” in December, Cyber-Resolutions in January, Safer Internet Day in February, and Cyber Crime of Opportunity in March) and introduce it through a blast email to all staff. We post an attention-grabbing headline and graphic on a rotating banner and a voice of the customer (VOC) survey on the HHS intranet home page. All three of these communications lead our readers to interesting articles, stimulating Yammer social media conversations, and our Twitter account which socializes great tips for our internal and external customers.

Our monthly themes complement other cybersecurity awareness program initiatives including ethical phishing programs, printed media, National Cybersecurity Awareness Month (NCSAM), and ongoing cybersecurity awareness training. HHS CyberCARE builds upon and partners with other national-level efforts such as Stop.Think.Connect, CyberBullying, National Privacy Day, and Safer Internet Day.

One thing that sets CyberCARE apart from other initiatives is that, in addition to being relevant and topical, we strive to be conversational and write in a way so that we are talking to our readers, not at them. Our content is poignant, relevant, and often presented in humorous and even punny articles. We don’t want our readers to see the ‘same old stuff’, we want to engage them.

CyberCARE stands out because we’re not another droning, technical voice. We draw people in and get them interested and aware of the threats we face day in and day out. Check out some of our topics and posts on the following pages...

Each month the HHS intranet features a CyberCARE rotating banner that links to a cybersecurity topic. Each week CyberCARE posts a VOC survey pertaining to cybersecurity. It lets participants see how they compare with their colleagues while checking their cybersecurity knowledge. It also lets us know our readers a little better.
Motivational Item Entries (2)
Encrypting Email Messages and Attachments

It really is this easy!

When sending sensitive information by email, either in the body of the message or as an attachment, the email must be encrypted!

OUTLOOK ON A PC

1. Open a new email.
2. Select the Options ribbon.
3. Encrypt the Message.

SEFT (Secure Email/File Transfer) Service

Used for sending large attachments, and for sending encrypted emails to recipients outside of NIH (with or without attachments). Note: Medical SEFT, managed by the Clinical Center, is the method used for patient contact.

After having the NIH IT Service Desk set up "Send Permissions" for your account:

2. Sign in with your NIH Username and Password with NIH before the username.
3. Click on the Secure Message button.
4. Compose message. You can include attachments by clicking the Choose Files… button.
5. Click Send to send the message.

OUTLOOK ON A MAC

1. Open a new email.
2. Add the email address of the recipient in the To section (use their NIH AD email address).
3. Click on the Security icon.
4. Click Encrypt Message.
5. Click Send to send the message.

NIH EMAIL WEB ACCESS (EWA)

The S/MIME control has to be installed on your machine before you can encrypt and/or digitally sign messages in EWA. You need to be on a Windows machine using Internet Explorer 7 or higher. Contact the IT Service Desk for more information.

1. Open a new email.
2. Click on the Email Encryption button.
3. Click Send to send the message.

NOTE: NIH users can't receive encrypted email through email Distribution Lists (DLS). Encryption requires both the sender and receiver to have valid digital certificates, which DLS don't have.
Motivational Item Winner!
K Rudolph

Organization:
Native Intelligence, Inc.
YOU ARE THE BEST ANTI-VIRUS!

SECURITY COMES IN CANS NOT CAN'TS

YOU ARE THE BEST ANTI-VIRUS!
Poster Entries (11)
BE AWARE...
Connect with care.
**DON'T EMAIL YOUR WORK HOME**
A Decision Making Flowchart

**Start**
Should I Email My Work Home?

- **Do you have a lot of work?**
  - **No**
  - **Really?**
    - **What?**
      - Ok yeah, I'm so busy I can't think.
    - **Ok, then**
      - Congrats, you have work/life balance!
  - **Yes**
    - **Do you have to work at night?**
      - **Yes**
        - **Do you have a personal email?**
          - **Yes**
            - **Should you email your work home?**
              - **No**
                - **No**
                  - **No**
                    - **No!**
                      - **We're not kidding.**
        - **No**
          - **No**
            - **Should you email your work home?**
              - **No**
                - **No**
                  - **No**
                    - **Here's the right way.**

Why is it a risk to email work home?
- You could send the email to the wrong person by accident.
- Cybercriminals can intercept and read emails once they leave the Department’s firewall, or could compromise your personal email and read it there.
- Email providers store emails on their cloud servers worldwide, and backup their servers frequently. Even if you delete the email, the information could remain on their servers and under their control.

What should you do?
1) Get approval from your manager.
2) You will be provided with equipment to use:
   - Department-issued USB key: securely transport documents home and work on them using your personal computer.
   - Laptop: securely connect to the electronic network from home using VPN.

**Beware of Phishing**

**What is Phishing?**

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

**How Phishing works?**

1. Phishing email which appears genuine is sent to user from Hacker’s account.
2. By clicking on the link, the user is asked to share his personal information.
3. This information is transmitted to the Phisher.
4. Opening the webpage or an attachment in the email might also download malicious software (malware).
5. Malware may also send more phishing emails automatically or turn into a botnet.
6. Personal data obtained also allows the phishers to steal identities, money and corporate secrets.

**How to avoid a Phish?**

- Avoid strangers
- Don’t rush
- Notice the recipient list
- Beware of greetings
- Don’t be lured
- Keep sensitive data to yourself
- Do not click on suspicious links and attachments

**PhishPond Campaign**

PhishPond team sends an email, Subject reads: Your request for paid time off

**What do I do if I receive a suspicious email?**

- **Notification**
  - visit: phishpond.cisco.com
- **Mitigation**
  - Think before you click
PHISHING FOR PHI
THERE'S A REASON WHY HEALTHCARE LEADS ALL INDUSTRIES IN DATA BREACHES AND IT'S PROBABLY BECAUSE OUR PATIENTS' PHI IS ALL THAT PHISH AND A BAG OF CHIPS!

Valuable
- HIPAA Regulations
- Security Policies
- Access Controls
- Business Associates

Precious
- Medical Records
- Billing Information
- Insurance Information

Personal Information
- Name, Address, Phone
- Social Security Number
- Date of Birth

PHI
- Protected Health Information
- Optical and Physical Media
- Networked Computers

Cyberterrorism
- Denial of Service
- Malware
- Ransomware

Identity Theft
- Stolen credit cards
- Phony Social Security numbers

Customer Stolen
- Personal records
- Financial records

Insurance Fraud
- False claims
- Fraudulent submissions

HHS has one of the largest repositories of PHI in the country. You can do your part to safeguard the security of patient information by following some security best practices. Don't disclose PHI to anyone who doesn't have authorization to access it. Keep your account password secure. Don't use sensitive account to access sensitive accounts. Follow best practices when sharing PHI through the Internet, and be aware of phishing. If you suspect a breach has occurred, report it immediately.

Report security breaches, phishing attempts, and other security violations to the Incident Response Team at it@hhs.gov.
How to Identify Sensitive Information

What is Sensitive Information? Any information that could cause serious harm if it was changed, unavailable, lost, or accessed by the wrong people.

Whenever you view, say, email, print, or write any information, first ask yourself these questions:

- **Context matters**: Can it be used on its own or combined with other information to identify, contact, or locate a person?
- If it was disclosed, lost, stolen, changed, destroyed or unavailable, could it cause harm to the individual and/or the NIH?
  1. Harm to physical safety or security?
  2. Injury to financial standing?
  3. Damage to current employment or future job offers?
  4. Destruction to reputation?
  5. Social disgrace or discrimination?
  6. Public embarrassment?
  7. Disruption in day-to-day operations or activities?
  8. Other negative effects?

If you answered **YES** to any of those questions, then that information is **SENSITIVE** and must be protected!

Look all around this poster for examples of sensitive information that you might work with. Don’t forget you can ask your supervisor if you have any questions!
Your online presence is...

...as permanent as a tattoo.
You are the weakest link in the cybersecurity chain

Want to know more?
https://info.health.mil/hit/infosec/SitePages/KnowledgeBase.aspx
Or, search for "KnowledgeBase" from DHA HIT SharePoint

October is Cybersecurity Awareness Month
DON'T BE LOW HANGING FRUIT

- Encrypt data
- Click with caution
- Verify access requests
- Report incidents
- Use strong passwords
- Reduce browser plug-ins

Careless clicks
END-OF-LIFE SYSTEMS AND APPLICATIONS
CYBERSECURITY AWARENESS

Operating systems and applications are considered end-of-life when they are no longer supported by the vendor and do not receive product updates and security patches. Use of these products presents a significant risk to FDA IT infrastructure, information, and overall mission. The FDA must reduce risk and minimize the potential impact on the FDA’s computing resources, sensitive data, funds, productivity, and public health reputation.

Meet Jim

Jim works for the FDA and his operating systems and applications are malware free.
Jim’s system and applications are patched and up to date, avoiding risk and performance issues.
Be like Jim.

Meet Bob

Bob did not retire his unsupported applications, leaving his machine at risk for cyber attacks. His machine is performing strangely and exposing FDA data to cyber attacks.
Bob is running to help desk support, the Employee Resource & Information Center (ERIC).
Don’t be like Bob.

For more security tips and helpful information, search for “End-Of-Life” on inside.FDA.
See SMG 3251.9 Operating Systems and Applications End-of-Life Policy here:
INFORMATION SECURITY IS EVERYONE’S RESPONSIBILITY

If you are aware of a privacy or security incident, you must notify your Information System Security Officer (ISSO) as soon as possible. If you are unable to reach your ISSO, please send an email to EDCIRC@ed.gov, EDSOC@ed.gov and PrivacySafeguards@ed.gov. EDSOC may also be contacted by phone on 202-245-6350.
Be careful about how much information you post online.

Think about how the various pieces of information might be combined to make you vulnerable for use by a cyber criminal.
Poster Winner!
K Rudolph, John Ippolito, G. Mark Hardy, Andrew Ellis, & Charles A. Filius

Organization:
Native Intelligence, Inc. and Friends
DON'T BE LOW HANGING FRUIT

- Encrypt data
- Click with caution
- Verify access requests
- Report incidents
- Use strong passwords
- Reduce browser plug-ins
- Careless clicks
Find out... *What’s the Big Deal!*

<table>
<thead>
<tr>
<th>Safe Workplace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Access Cards</td>
</tr>
<tr>
<td>Building Evacuations</td>
</tr>
<tr>
<td>Personal Safety Threats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safe Saving, Storing, Sending &amp; Receiving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Signatures</td>
</tr>
<tr>
<td>Emailing “Protected B”</td>
</tr>
<tr>
<td>Emailing to Home or Personal Accounts</td>
</tr>
<tr>
<td>Email [Think First]</td>
</tr>
<tr>
<td>Phishing – Clicking on Links</td>
</tr>
<tr>
<td>Phishing – What to Consider</td>
</tr>
<tr>
<td>Phone Scams</td>
</tr>
<tr>
<td>Mailing Sensitive Documents</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safe Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing Computers (In the Office)</td>
</tr>
<tr>
<td>Securing Computers (Out of the Office)</td>
</tr>
<tr>
<td>Personal Device at Work</td>
</tr>
</tbody>
</table>

**What’s the big deal if...**

...I lend my ID/Access card to a colleague?

**Why it is a big deal**

- You will be held responsible (as the owner of the ID/Access card) if an incident occurs (e.g. loss of access card, access to areas without authorized approval).

**Scenario**

Bob has forgotten his ID/Access card at home. He is aware that you will be at an off-site meeting for two hours and asks if he can borrow your card while you are away. What do you do?

**Possible actions (vote on the best one)**

- Option 1: You refuse to lend your ID/Access card to Bob.
- Option 2: You give Bob your ID/Access card to use while you’re at the meeting.
- Option 3: You advise Bob to ask another colleague.

**Explanation**

- Option 1 is the correct option.
- By not lending your ID/Access card you are respecting the privileges and use of the card assigned to you.

**Key take-aways**

- You must never lend your personal departmental ID/Access card to anyone.
- If you forget your ID/Access card, tell your manager/team leader who will make temporary arrangements for you.
- You must wear your ID/Access card so it is visible – each day, all day long - while on departmental premises.
- If you lose your card or if it is stolen, immediately advise your manager/team leader, and complete the Security Incident Report.

**More information**

- [Departmental Security Practices](#)
Fry a Better Phish

Best Phish Bait on the Market
Phishing is an unsavory social engineering tactic that uses email, malicious websites, or phone calls from criminals posing as trustworthy organizations with the most wholesome of intentions. An attacker might send an email, carefully crafted to look like it’s coming from a reputable credit card company or financial institution, requesting personal account information. But take a closer look and these emails definitely smell phishy! They will often suggest that there’s a problem with your account to scare you into giving out the information they’ve requested. Don’t take a bite! Crooks can use the information to poach sizable morsels of your private accounts.

Hard-boiled cyber criminals have become super-savvy at reeling people in, luring them with sneaky links, tantalizing tricks, and seemingly harmless but corrupted attachments. Their emails can appear truly authentic - exactly like they would if they were coming from a real financial institution, government agency, or any other type of service or business. Be careful! Just because it looks gourmet, that doesn’t mean it’s tasteful!

A Tempting Dish
Phishing attacks usually urge you to act quickly. They might threaten to deactivate a particular account, or state that your account has somehow been compromised or frozen (and frozen phish is never tasty)! They even insist that an online order you’ve just made can’t be fulfilled until personal information or payment arrangements have been updated. Don’t get hooked! This is just another scare tactic used by foul Internet foes.

Regardless of any network defender’s best efforts, it’s impossible to prevent every unappetizing phishing campaign. While there is no magic solution for combating every possible ploy, there are a number of things YOU can do to in-the-know and on the lookout! By following these simple recipes, you can keep yourself safe from freeze-dried phishing shenanigans!

Recipe #1 - Discover With a Quick Hover
Type of Phish: An email urging you to click on a link, taking you to a website that asks for your password!
Ingredients: One email, a handful of savvy cyber criminals, a dash of social engineering, one fake link, and a pinch of malware.
Directions: Hover over the link BUT DON’T CLICK ON IT! Hovering will reveal the actual web address. If it looks suspicious, CALL your local IT staff or EMAIL irishna.gov!!

Recipe #2 - Social Media, Bait to Feed Ya
Type of Phish: Social engineers research your social media profiles to piece together your identity and interests! Then, they lure you into their net by pretending to be someone you know with content that interests you. Accepting the request or viewing the attachment launches their malware!
Ingredients: An array of social media flavors, one sneaky impersonator, malware added to taste.
Directions: Adjust your privacy settings so only friends see your profiles. Always examine senders’ email addresses to make sure they’re legitimate. Also examine website URLs. If it seems phishy, CLOSE THE PAGE!!

Recipe #3 - Think Twice With Your Mobile Device
Type of Phish: A text message on your mobile device directs you to a false website asking you for account information... especially the credit cards associated with the account!
Ingredients: One cell phone, a smidgeon of Smishing, and aheaping spoonful of unsuspecting texters.
Directions: Don’t respond to unfamiliar texters requesting personal information. Beware of messages from non-phone-numbers like “4325”! That’s a tactic scammers use to mask their identity by using email-to-text services that conceal their actual phone number. DON’T RESPOND!!

Recipe #4 - Don’t Stall with a Phony Phone Call
Type of Phish: Scammers obtain your name, job title, and contact information from public directories and call you up! Once on the line, they pretend to be tech support and try to confuse you with a healthy smattering of technical terms. Then they ask you to perform a series of tasks on your computer, claiming you’ve got a virus or software issue!
Ingredients: One telephone, a skosh of data mining, and a sprig of spear phishing.
Directions: Never give personal software information or passwords over the phone. If you get a call from some kind of “tech support,” call the company yourself using a phone number you know to be genuine. Hang up and GET OFF THAT LINE!!
Identifying and Protecting Sensitive Information

When you view, write, print, email, or discuss information, how do you know if it’s sensitive and needs protection? Sometimes, it’s obvious, like SSNs, but it can be tricky because the context, situation or circumstances may make some information sensitive.

One thing is clear—because of the nature of our work, NIH has a lot of sensitive information, and each of us needs to understand how to identify and protect it.

Learn more by clicking on this link to watch A Tale of Sensitive Information.

How to Protect Sensitive Information

- **What is it?** Non-public information that could cause serious harm if it was changed, lost, unavailable, or accessed by the wrong people. A “YES” to either of these questions means it’s sensitive:
  - Could it be used on its own or combined with other information to identify, contact, or locate a person?
  - If it was disclosed, changed, destroyed, or unavailable, could it cause harm and/or negative consequences for an individual or the NIH? [Think about physical safety, financial standing, employability, reputation, social stigma and discrimination, or disruption of day-to-day activities.]

- **Consider the context of the information.** The name “John” isn’t sensitive on its own. However, if you combine it with other information, such as “John Doe’s genetic profile”, you’ve got sensitive information.

- **Review examples.** The list isn’t exhaustive and may not relate to your duties. Ask your supervisor or security officer if the information you handle is sensitive:
  - Name (e.g. full name, maiden name, mother’s maiden name, alias, etc.)
  - Social Security Number, birth date, or place of birth
  - Home address, personal email address, telephone numbers
  - Personal characteristics (e.g. fingerprints, retina scans, full face photos, etc.)
  - Pre-award contract and grant application information
  - Employment records and disciplinary actions
  - Patient records that haven’t been de-identified, human genetic data
  - Police and criminal investigation information
  - Proprietary information provided to NIH by outside parties
  - Non-public invention reports or patent filings, pre-publication research findings

- **How should you protect it?** Regardless of whether the information is in electronic, physical, or verbal form, protection is your responsibility:
  - Encrypt - when emailing sensitive data, see instructions here.
  - Talking about it - not in public or around those without a need to know.
  - Faxing - verify it’s the correct fax number and that the recipient received it.
  - Passwords (preferably pass phrases) - make them strong and hard to guess.
  - Social engineering - watch out for phishing, phony calls, and impersonators.
  - Protect computer/mobile devices - from loss, theft, and damage.
  - Lock workstations and remove PIV cards - when leaving them unattended.
  - Check with your ISSO - if planning to bring/access government-owned equipment or information on foreign travel.
  - Sensitive physical documents - keep them out of view of unauthorized persons, locked up when not in use, and shred them when no longer needed.
  - Equipment sanitization - ask your ISSO before disposing of any government-issued devices or drives - they might contain sensitive data.
  - Access, collect, use, and disclose sensitive information - only when authorized for a legitimate job function that supports the NIH mission.

- **If you think sensitive information was inappropriately disclosed (via unencrypted email, loss/theft of device(s)/documents, verbal disclosure, etc.):** Notify the IT Service Desk within ONE HOUR (day or night). As soon as possible, inform your direct supervisor and ISSO.

NIH users are getting email attachments with malicious “macros”.

**Question:** A guy called saying he’s from Microsoft and that he needs to log into my computer to fix a vulnerability. Should I let him do this?

**Answer:** This is a form of “social engineering” (i.e., a caller claims to be from a help desk of other reputable source and requests users log in or access to their computers).

In this case, the caller is trying to manipulate you into giving up your network username and password. If you receive a call like this, don’t give out any information. Hang up and contact the Incident Response Team at IRT@mail.nih.gov.

NIH Information Security Program
Office of the Chief Information Officer

Email: NIHInfoSec@mail.nih.gov
HOW CRIMINALS USE ON-DEMAND APPS

Thanks to mobile apps, our culture is changing and many people are willing to let a stranger spend the night in their homes (using an app called Airbnb), get a ride with a stranger (Uber), or meet a potential date after just a few texts (Tinder).

Companies use background checks, user reviews, and systems of reward and punishment to encourage trust and good behavior. Most of the time, people get good, honest, and romantic encounters with no problems, but once in a while, there are problems.

People’s willingness to trust strangers from the internet has created new opportunities for crime. Why break into someone’s home to rob them when you can just book it for a night on Airbnb?

Here are some examples of how on-demand apps enabled crimes this year:

- **Last summer**, a woman who rented a home via Airbnb forced her way into a locked closet and made off with more than $35,000 in valuables. The homeowner gave police video of the theft, because he had home surveillance cameras. Airbnb said that incidents like this are rare.

- In 2014, there were multiple instances of kidnappers impersonating Uber drivers, including one where a Florida man drove a female student to a remote destination and demanded sexual favors.

- **Stay Safe When Using Apps**

- **When first meeting a stranger from the Internet in person, meet in public.**
- **Uber advises that you make sure your ride’s license plate matches the one in the app.**
- **Airbnb has advised users to be diligent when vetting emails that appear to come from the company.** Fake emails often have an urgent tone and threaten the loss of a reservation or a delayed payout if the guest doesn’t click the link and provide the information immediately.
- **Airbnb web pages begin with https://airbnb.com. If you click a link and the webpage doesn’t start with this, it’s a fraudulent page and you should close it and go to the Airbnb site by manually typing the web address.**

YOUR MONEY OR YOUR FILES

“Your files are encrypted,” the computer screen announced. “To get the key to decrypt files you have to pay 500 USD.”

The virus displays a countdown clock, and if the victim fails to pay within a week, the price goes up to $1,000. After that, the decryption key is destroyed along with any chance of accessing the files.

*NY Times* author Alina Simone learned about Cryptowall when her mother’s files were encrypted. Her mother chose to pay rather than lose her 5,726 files.

Cryptowall is a ransomware virus that gets into your computer when you click on a legitimate-looking attachment or visit an infected website. Once activated, it encrypts all your files.

But the Cryptowall hackers only accepted Bitcoins. By day 6, her mother had managed to make a direct deposit to the Bitcoin wallet provided by the hackers.

Unfortunately, since Bitcoin’s price is extremely volatile and payments can take six days to process, her payment was $25 short when it arrived.

The fastest way to send the extra $25 was to make a direct deposit at an ATM that handled Bitcoin transactions. But, by the time she had done this, the price had gone up to $15,000.

So, she used the Cryptowall message interface provided by the hackers and explained the delay. She said that she really tried not to miss their deadline, and shortly after, her decryption key arrived. *NY Times*

TIPS

- Back up your files and disconnect the backup from your computer. Ransomware programs will encrypt any drive that is connected to your computer. An alternative is to use a cloud backup service such as Carbonite.
- Keep your software, apps, and operating system up to date, including your web browser and all plugins.
- Install anti-malware software and keep it up to date with a current subscription. New malware variants arise every day, so using old virus definitions is almost as bad as having no protection.
- Beware of attachments. Legitimate businesses will rarely send you an attachment.
- Disable Remote Desktop Protocol. Most ransomware tries to access target machines via Remote Desktop Protocol (RDP), a Windows utility that permits access to your desktop remotely. If you don’t use RDP, disable it to protect your computer.
Security at Vantiv

Did you realize that your VSS team (like many here at Vantiv) is quite accomplished and respected in the security field. For example, Kristy Westphal, who directs our Risk and Assurance function wrote an article published by the International Association of Privacy Professionals, and Kim Jones, our Chief Security Officer, was recently quoted in an article on sharing threat information.

Mark your calendar! The 4th quarter employee access review kicks off November 30. Just a reminder — on December 15, VSS will disable any accounts that haven’t been reviewed by EOD December 14.

Hot Attacks

Hackers stole $1.2 billion from 7,000 businesses in two years using a wire-fraud scam that starts with a simple phishing email. But one anti-phishing education company phished the phishers.

Nation states are widely regarded as the most dangerous cyber attackers. Why? Because they generally have unlimited resources — smart people, time, and lots of money. Here’s an interesting look at the current state of cyber warfare. And here in the U.S., cyber weaponry will be used in conjunction with physical weapons. On another front, the U.S. and China agreed not to hack each other for economic purposes.

Cybercrime / Hacking

Everyone talks so much about a migration to card-not-present fraud once EMV is in widespread use at the point of sale at U.S. merchants, but bad guys are developing methods to get around EMV. Read about card-tapping and skimming.

Be careful using unknown USB sticks. Here’s one that sends 220 volts through the signal lines of the USB interface, trying the hardware (with a somewhat unimpressive video). It’s not just malware (malicious software) we need to watch out for anymore.

We don’t talk about malware much anymore. It’s simply a fact of life. But here’s a statistic Snippets finds shocking: one AV vendor detected 230,000 new malware samples each day. Here’s a short, nice history of malware.

Home / Personal Issues

Do you use free AVG antivirus software on your home PC? If so, Snippets strongly recommends you re-read their updated privacy policy. They can now sell your web browsing and search history to third-party advertising companies. Don’t think it’s a big deal? Just check out the article showing why metadata matters.

With the release of the new iPhone 6s/6s and the launch of iOS 9, remember to secure your device and set your privacy.

Snippets finds this trev4ead. You may recognize these scams, but your parents may not. Check out the resources on AARP’s webpage and talk with your folks.

Politics / Legislation

The European Union has much stronger data protection laws than the U.S. So companies who want to do business with the EU must agree to protect EU citizens’ data — called the Safe Harbor agreement. Earlier this month, the Court of Justice of the European Union ruled that transatlantic data transfers made under the Safe Harbor agreement are illegal. While the U.S. Department of Commerce negotiates with the EU, U.S. companies are trying to figure out what to do. This is a pretty huge issue.

Here’s another biggie. The Obama administration won’t ask Congress for legislation requiring the tech sector to install backdoors into their products so the government can access encrypted data. Snippets was personally appalled by the idea of building backdoors into systems. Why? It weakens security (obviously).

In another move that indicates the importance of security, Standard and Poor’s has warned that it may downgrade the credit ratings of banks that have poor cybersecurity.

Privacy / ID Theft

In the first six months of 2015, there have been 858 data breaches with 248 million records compromised worldwide. Compared to the first half of 2014, data breaches increased by 10% while the number of compromised data records declined by 41%. Why the decline? We haven’t had those huge retail breaches like we did last year.

The Identity Theft Resource Center has a new mobile app to help victims of identity theft.

Best Practices

A DC power lawyer had a lot of feelings about the 2016 election and inadvertently decided to share them with the FBI in a tweet — which included two political reporters — as it zipped from D.C. to New York City. Key lesson: when you’re discussing work in public, be careful what you say. You never know who is listening.

Snippets loves cartoons, especially when they teach you how to protect your electronic device.
Malware is a term used to describe a variety of malicious software programs installed on a computer system without the user’s knowledge or consent. Malware comes in many forms, including spyware, viruses, worms, Trojan horses, and ransomware and can be used to compromise the end user’s computer system, gain access to sensitive information and systems, and launch attacks against other computer systems and networks. Malware can be difficult to detect and remove as it is typically installed in unexpected or hidden places or modifies the operating system. Therefore responding to and recovering from malware incidents can be time intensive and expensive. Malware is commonly spread through attachments and hyperlinks received in spam phishing email messages. If you receive an unsolicited email that makes you feel that immediate action is necessary, don’t open attachments or click links unless you’re certain they’re safe.

### Encrypting SPlI Using WinZip

Sensitive personally identifiable information (SPlI) sent via email must be encrypted using a password-protected WinZip archive.

To compress and encrypt files:

1. Browse to and select the files you want to encrypt.
2. Right-click on the files and select WinZip - Zip and E-mail Plus. A new window displays.
3. In the Zip file name section, select the radio button to accept the default zip file or select Use this name radio button and enter a name of your choice.
4. In the Compression type section, click the radio button next to .Zip: Legacy compression (maximum compatibility).
5. Click the Encrypt Zip File checkbox to select it.
6. Click the OK button. The Encrypt window displays.
7. In the Encrypt window, enter a password to protect your file. To comply with Department policy, enter a password containing at least one of the following: a lower case character (a-z), an upper case character (A-Z), and a symbol character (!, $, %, ^, &, *, etc.).
8. Re-enter the password to confirm it.
9. In the Encryption method section, select the 256-bit AES (stronger) radio button as the encryption method.
10. Click the OK button to create and email your new password protected, encrypted zip file.

### Malvertising

With the explosive growth of online advertising, cybercriminals are using mainstream websites to infect end-user computers with advertisement-based malware, or “malvertising.” Malvertising occurs when malicious code is embedded into legitimate advertisements on trusted, mainstream websites. Users can fall victim to malvertising by opening a malicious advertisement or by simply visiting a website that contains malicious advertising. These attacks are particularly hard to detect because most advertising comes from a variety of ad networks and not from the mainstream website itself. A single online advertisement for an individual consumer routinely goes through five or six companies before finally reaching the end user’s computer—providing cyber criminals with many entry points along the way to infect malware.

To defend against malvertising, be sure to keep your anti-virus up to date. Also, don’t click on links within pop-up windows as this may cause malicious software to install on your system. Always close pop-up windows by clicking the “X” icon in the title bar instead of any “close” link within the pop-up window.

### Emails Attack!

Did you know that many large, widely publicized data breaches began with a spear phishing email? These malicious emails closely resemble legitimate messages that you may receive on a regular basis and may appear to be from a co-worker, known business contact, a well-known retailer, bank, or other service provider. The messages often urge you to take action by referring to important and usually time-sensitive information such as shipping delivery services, invoices, purchase orders, or an issue with the user’s computer or email account. By tricking you into clicking the link or opening an attachment, an attacker can install various forms of malware which can compromise your computer and snatch sensitive data.
The Danger of Reusing Passwords

Cyber criminals compromise websites every day and post lists of usernames, email addresses, and passwords online. While this can be embarrassing, it also leaves users open to potential attacks due to passwords reuse. Passwords make it easy for attorneys to access the passwords of multiple websites of accounts. This is a vulnerability when the password is chosen in such a way that it is common to the attacker. If the password is used elsewhere, attackers can use the password to gain access to the accounts.

Cyber criminals can take advantage of reused passwords by:

1. Searching for other accounts you use – like Facebook, Twitter, or banking websites and trying to log in with the same password. If they can identify those accounts, they can use your password to log in.
2. Searching for websites that divulge legitimate websites that require you to enter an email address, password, and potentially other information to gain access. Once you provide the login information, they know who you are and who you can search for on your other accounts with the same password.

Avoiding Password Reuse:

Avoiding passwords can be challenging, but there are a few ways to do both avoid it and ensure that the password you create meets recommended password complexity requirements.

Make your passwords complex:

- Use a mix of uppercase and lowercase letters, numbers, and special characters (e.g., @ # $ %).
- Don't use words from the dictionary – these are the first things hackers will try (e.g., applepie, password, abc123).
- Don't use names of your sports teams, friends, pets, celebrities, etc.

Choose a memorable pattern for your passwords that contains something unique to the website or account, and then change the first letter of each word of your password. For example, the sentence “When the Empire strikes back, it will be with a vengeance” becomes “WhenTheEmpireStrikesBackItWillBeWithAVengeance.”

Regardless of the technique you use to create a complex password, it is important that every password is unique. More advice on choosing a strong, complex password can be found at www.WiFiSecurityAlerts.com.

Same day credit on deposits made by 9pm

Remote Deposit Express

Don't you love it when someone makes life easy?

For more information, please contact us toll free at 1-800-731-0213

Scareware:

The blight of small businesses

Cybercriminals are getting more creative by using your techniques to worm their way into the computers (and websites) of unsuspecting victims. One of the most prevalent methods currently used by cybercriminals is scareware, a digital threat that preys upon users to drive traffic to websites which ultimately ends in one of the following:

- Pop-up ads that you cannot close.
- Downloads that you cannot delete.
- Malware that is difficult to remove.

Recommendations for our customers:

- Change your passwords for online accounts:
  - Secure your remote deposit applications.
  - Ensure that your website is secure.
- Take steps to ensure your website is secure:
  - Use SSL encryption on your website.
  - Use a firewall to protect your website.
- Take steps to ensure your remote deposit applications are secure:
  - Use strong passwords for your remote deposit applications.
- Take steps to ensure your remote deposit applications are secure:
  - Use strong passwords for your remote deposit applications.
- Take steps to ensure your remote deposit applications are secure:
  - Use strong passwords for your remote deposit applications.
- Take steps to ensure your remote deposit applications are secure:
  - Use strong passwords for your remote deposit applications.

ACH Alert

Next Generation Account Protection

Stay up with your account activity and fraud prevention on your ACH. Take advantage of the new ACH Account Protection stalls.

- Check on your account activity when you are using an online application.
- Check on your account activity when you are using an online application.
- Check on your account activity when you are using an online application.
- Check on your account activity when you are using an online application.
- Check on your account activity when you are using an online application.

Protect your business against Credit Card fraud

- Remove personal account number storage
- Use tokenization encryption tool to store card data
- Prepare for EMV chip technology

Be ahead of new threats, like the Linux/mirai toilet malware, these steps can help you stay ahead:

- Back up your websites files
- Create strong passwords
- Update your website's contact information
Newsletter Winner!
IHS Division of Information Security

Organization:
Indian Health Service, Office of Information Technology, Division of Information Security
Fry a Better Phish

Best Phish Bait on the Market
Phishing is an unsavory social engineering tactic that uses email, malicious websites, or phone calls from criminals posing as trustworthy organizations with the most wholesome of intentions. An attacker might send an email, carefully crafted to look like it’s coming from a reputable credit card company or financial institution, requesting personal account information. But take a closer look and these emails definitely smell phishy! They will often suggest that there’s a problem with your account to scare you into giving them the information they’ve requested. Don’t take a bite! Crooks can use the information to poach sizable morsels of your private accounts.

Hard-boiled cyber criminals have become super-savvy at reeling people in, luring them with sneaky links, tantalizing tricks, and seemingly harmless but corrupted attachments. Their emails can appear truly authentic—exactly like they would if they were coming from a real financial institution, government agency, or any other type of service or business. Be careful! Just because it looks gourmet, that doesn’t mean it’s tasteful!

A Tempting Dish
Phishing attacks usually urge you to act quickly. They might threaten to deactivate a particular account, or state that your account has somehow been compromised or frozen (and frozen phish is never tasty!). They may even insist that an online order you’ve just made can’t be fulfilled until personal information or payment arrangements have been updated. Don’t get hooked! This is just another scare tactic used by foul Internet foes.

Regardless of any network defender’s best efforts, it’s impossible to prevent every unsavory phishing campaign. While there is no magic solution for combating every possible ploy, there are a number of things YOU can do to be in-the-know and on the lookout! By following these simple recipes, you can keep yourself safe from freeze-dried phishing shenanigans!

Recipe #1 - Discover With a Quick Hover
Type of Phish: An email urging you to click on a link, taking you to a website that asks for your password!
Ingredients: One email, a handful of savvy cyber criminals, a dash of social engineering, one fake link, and a pinch of malware.
Directions: Hover over the link BUT DON’T CLICK ON IT! Hovering will reveal the actual web address. If it looks suspicious, CALL your local IT staff or EMAIL irish.a.gov!!

Recipe #2 - Social Media, Bait to Feed Ya
Type of Phish: Social engineers research your social media profiles to piece together your identity and interests! Then, they lure you into their net by pretending to be someone you know with content that interests you. Accepting the request or viewing the attachment launches their malware!
Ingredients: An array of social media flavors, one sneaky impersonator, malware added to taste.
Directions: Adjust your privacy settings so only friends see your profiles. Always examine senders’ email addresses to make sure they’re legitimate. Also examine website URLs. It seems phishy? CLOSE THE PAGE!!

Recipe #3 - Think Twice With Your Mobile Device
Type of Phish: A text message on your mobile device directs you to a fake website asking for account information—especially the credit cards associated with the account!
Ingredients: One cell phone, a smidgeon of SMiShing, and a heaping spoonful of unsuspecting texters.
Directions: Don’t respond to unfamiliar texters requesting personal information. Beware of messages from non-phone-numbers like “4325.” That’s a tactic scammers use to mask their identity by using email-to-text services that conceal their actual phone number. DON’T RESPOND!

Recipe #4 - Don’t Fall for a Phony Phone Call
Type of Phish: Scammers obtain your name, job title, and contact information from public directories and call you up! Once on the line, they pretend to be tech support and try to confuse you with a healthy smattering of technical terms. Then they ask you to perform a series of tasks on your computer, claiming you’ve got a virus or software issue!
Ingredients: One telephone, a splash of data mining, and a sprig of spear phishing.
Directions: Never give personal software information or passwords over the phone. If you get a call from some kind of “tech support,” call the company yourself using a phone number you know to be genuine. Hang up and GET OFF THAT LINE!!

Indian Health Service
Video Entries (6)
Video 1: https://www.youtube.com/watch?v=CpmdhQEanzc

Video 2: https://youtu.be/lPyrGvkDdek

Video 3: 
https://www.youtube.com/watch?feature=player_embedded&v=xfEf8jzTILk

Video 4: https://youtu.be/3hHnT1szO7c

Video 5: https://www.youtube.com/watch?v=Regfcjtqqa08

Video 6: 
https://vimeo.com/infosightinc/review/71762956/3a70dcbbc50
Video Winner!
Cheryl Seaman & Stephanie Erickson

Organization:
The National Institutes of Health
Training Entries (3)
Don't Take the Bait Interactive Activity

What can happen if you're phishing? Click the tabs to see...

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

Email Phishing

Emotions:

Curiosity: People are usually curious about the promised free product or prize.

Fear: Scammers use tactics that make the victim feel vulnerable or exposed to a situation that could cause harm.

Urgency: Scammers create a sense of urgency or immediate need to act.

Sender Address:

- Overly generic or doesn't follow agency's protocol could indicate something is wrong.
- Name be suspicious of

Email Tone:

- A real service provider's email tone is likely to be polite and professional.
- Scammers may use aggressive or threatening language.

Subject Line:

- Real service providers are likely to have clear and straightforward subject lines.
- Scammers may use misleading or urgent subject lines.

Body:

- Real service providers often provide detailed information and instructions.
- Scammers may include links or attachments that can infect your device.

Footer:

- Real service providers often include clear contact information.
- Scammers may use fake contact information or ask for personal information.

Note:

Hover over the blue boxes for hints...
Information security is all about managing risks, making balanced decisions about performing your work with the appropriate level of security to ensure the confidentiality, integrity and availability of our data and information systems.

The moment you leave your office with sensitive information and government-issued devices, you take the responsibility for their protection. Gone are the security guards, key card controlled access, agency firewalls, secure wired connections to the NIH network and many other safeguards found in the workplace. This is when you need to heighten your situational awareness—knowing what is going on around you—from both an electronic and physical perspective.

While you may think that some precautions are excessive, NIH information/data and computing resources are high value assets. Scientific and biomedical intellectual property, medical records, personally identifiable information (PII), email and other system accounts are subject to targeted attacks.

It's your responsibility to take necessary precautions and to follow the best practices contained in this course.
Training Winner!
The ESDC Security Training and Awareness Program Team

Organization:
Employment and Social Development Canada (ESDC)
ARE YOU CYBER SAVVY?

PLAY

INFO SHIELD

TO FIND OUT!

PLAY NOW!

Already registered? Log in here
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 alongside 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!