FISSEA

Security Awareness, Training, and Education

Contest

Gretchen Morris, CISSP
FISSEA Working Group Member

March 2016

Contest

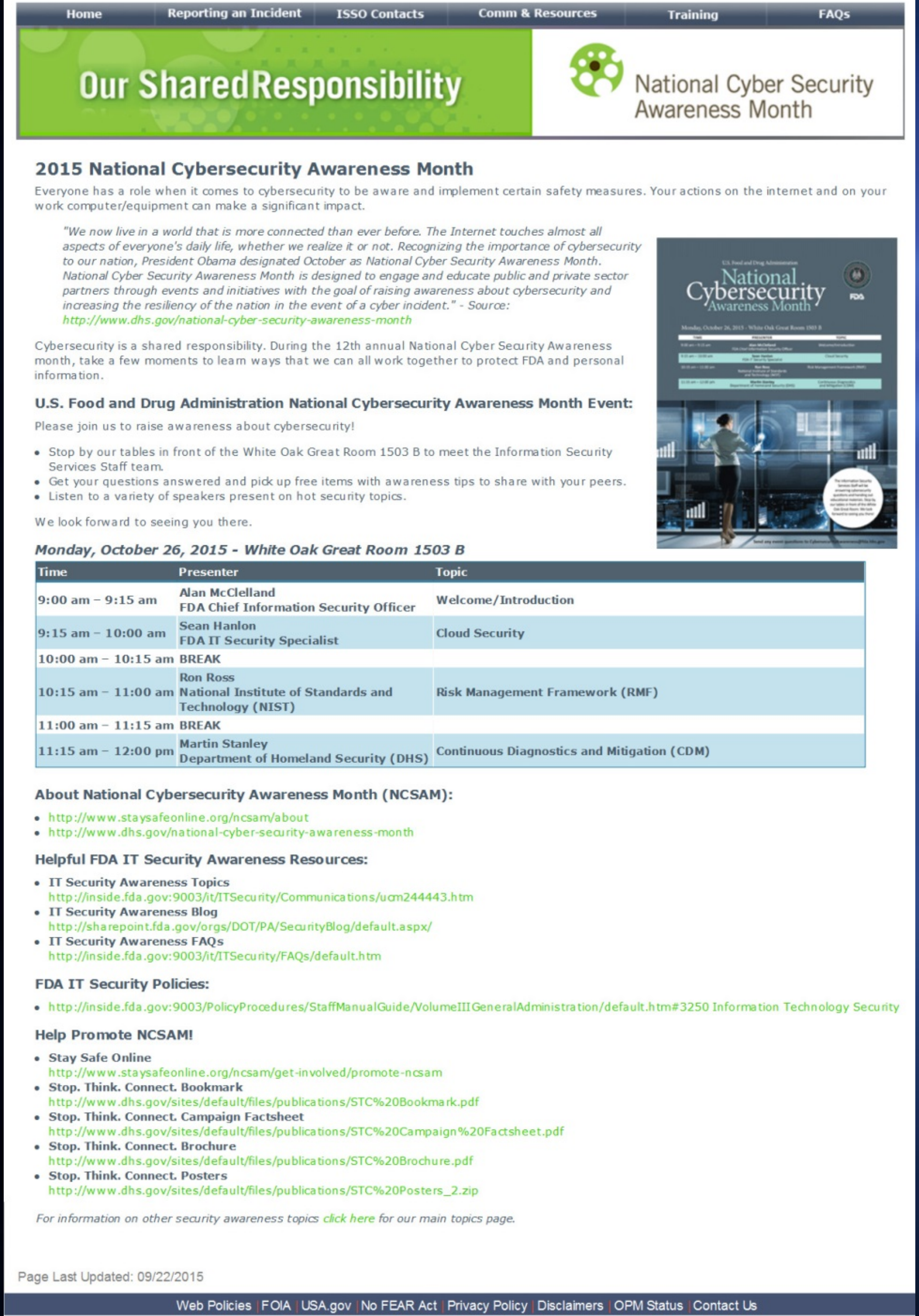
Categories

- 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

Everyone 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

Time	Presenter	Topic
9:00 am – 9:15 am	Alan McClelland FDA Chief Information Security Officer	Welcome/Introduction
9:15 am – 10:00 am	Sean Hanlon FDA IT Security Specialist	Cloud Security
10:00 am – 10:15 am	BREAK	
10:15 am – 11:00 am	Ron Ross National Institute of Standards and Technology (NIST)	Risk Management Framework (RMF)
11:00 am – 11:15 am	BREAK	
11:15 am – 12:00 pm	Martin Stanley Department of Homeland Security (DHS)	Continuous Diagnostics and Mitigation (CDM)

About National Cybersecurity Awareness Month (NCSAM):

- http://www.staysafeonline.org/ncsam/about
- http://www.dhs.gov/national-cyber-security-awareness-month

Helpful FDA IT Security Awareness Resources:

- IT Security Awareness Topics
  http://inside.fda.gov:9003/it/ITSecurity/Communications/ucm244443.htm
- IT Security Awareness Blog
  http://sharepoint.fda.gov/orgs/DOT/PA/SecurityBlog/default.aspx/
- IT Security Awareness FAQs
  http://inside.fda.gov:9003/it/ITSecurity/FAQs/default.htm

FDA IT Security Policies:

- http://inside.fda.gov:9003/PolicyProcedures/StaffManualGuide/VolumeIIIGeneralAdministration/default.htm#3250 Information Technology Security

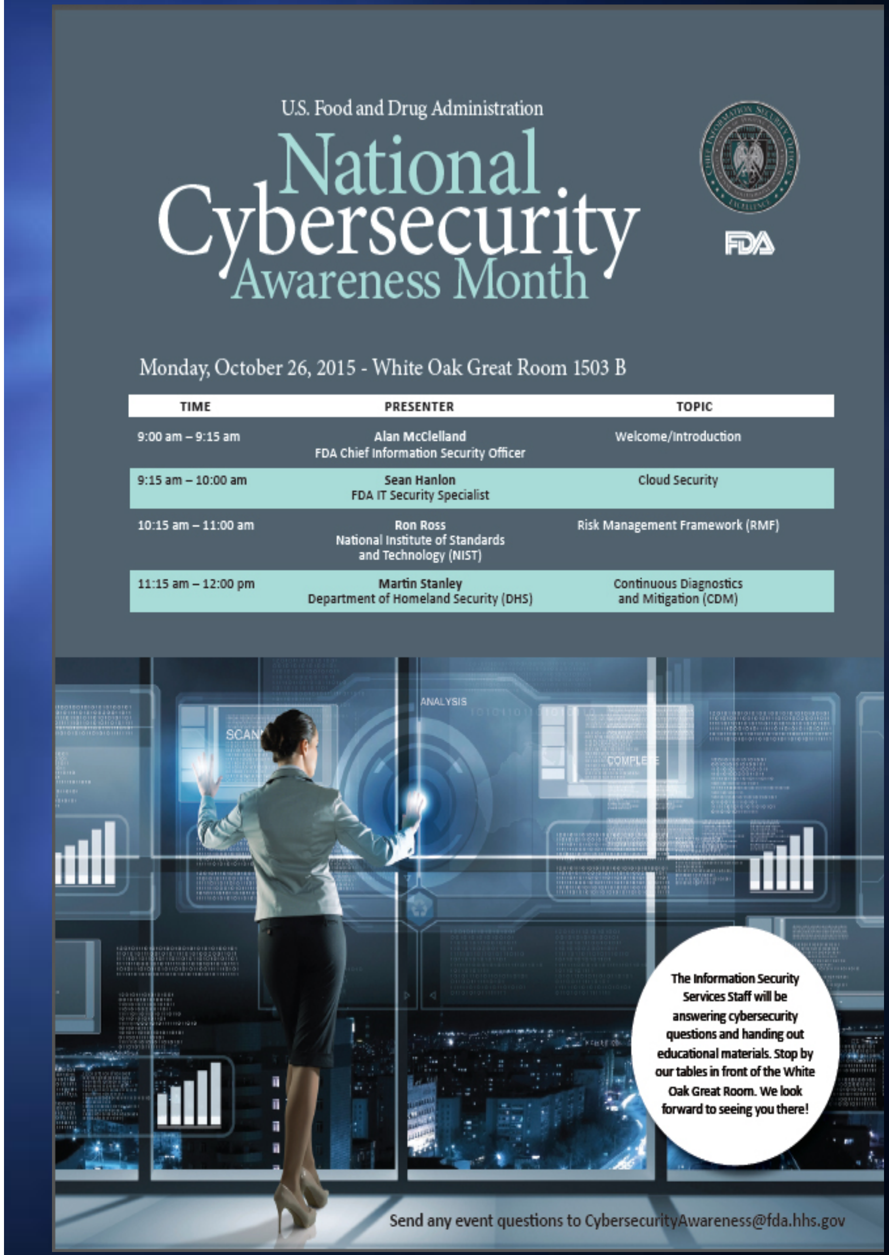
Help Promote NCSAM!

- Stay Safe Online
  http://www.staysafeonline.org/ncsam/get-involved/promote-ncsam
- Stop. Think. Connect. Bookmark
  http://www.dhs.gov/sites/default/files/publications/STC%20Bookmark.pdf
- Stop. Think. Connect. Campaign Factsheet
  http://www.dhs.gov/sites/default/files/publications/STC%20Campaign%20Factsheet.pdf
- Stop. Think. Connect. Brochure
  http://www.dhs.gov/sites/default/files/publications/STC%20Brochure.pdf
- Stop. Think. Connect. Posters
  http://www.dhs.gov/sites/default/files/publications/STC%20Posters_2.zip

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

Page Last Updated: 09/22/2015

Web Policies | FOIA | USA.gov | No FEAR Act | Privacy Policy | Disclaimers | OPM Status | Contact Us



U.S. Food and Drug Administration

National Cybersecurity Awareness Month

FDA

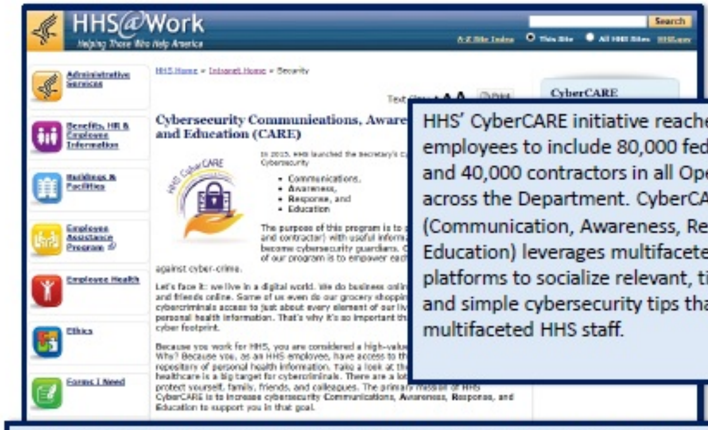
Monday, October 26, 2015 - White Oak Great Room 1503 B

TIME	PRESENTER	TOPIC
9:00 am – 9:15 am	Alan McClelland FDA Chief Information Security Officer	Welcome/Introduction
9:15 am – 10:00 am	Sean Hanlon FDA IT Security Specialist	Cloud Security
10:15 am – 11:00 am	Ron Ross National Institute of Standards and Technology (NIST)	Risk Management Framework (RMF)
11:15 am – 12:00 pm	Martin Stanley Department of Homeland Security (DHS)	Continuous Diagnostics and Mitigation (CDM)

The Information Security Services Staff will be answering cybersecurity questions and handing out educational materials. Stop by our tables in front of the White Oak Great Room. We look forward to seeing you there!

Send any event questions to CybersecurityAwareness@fda.hhs.gov

HHS CyberCARE



Cybersecurity Communications, Aware
and Education (CARE)

In 2015, HHS launched the Secretary's C
Cybersecurity

- Communications,
- Awareness,
- Response, and
- Education

The purpose of this program is to
and contractor) with useful informa
become cybersecurity guardians. C
of our program is to empower each
against cyber-crime.

Let's face it: we live in a digital world. We do business onli
and friends online. Some of us even do our grocery shoppin
cybercriminals access to just about every element of our liv
personal health information. That's why it's so important th
cyber footprint.

Because you work for HHS, you are considered a high-valu
Why? Because you, as an HHS employee, have access to th
repository of personal health information. Take a look at th
healthcare is a big target for cybercriminals. There are a lot
protect yourself, family, friends, and colleagues. The primary mission of HHS
CyberCARE is to increase cybersecurity Communications, Awareness, Response, and
Education to support you in that goal.

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.

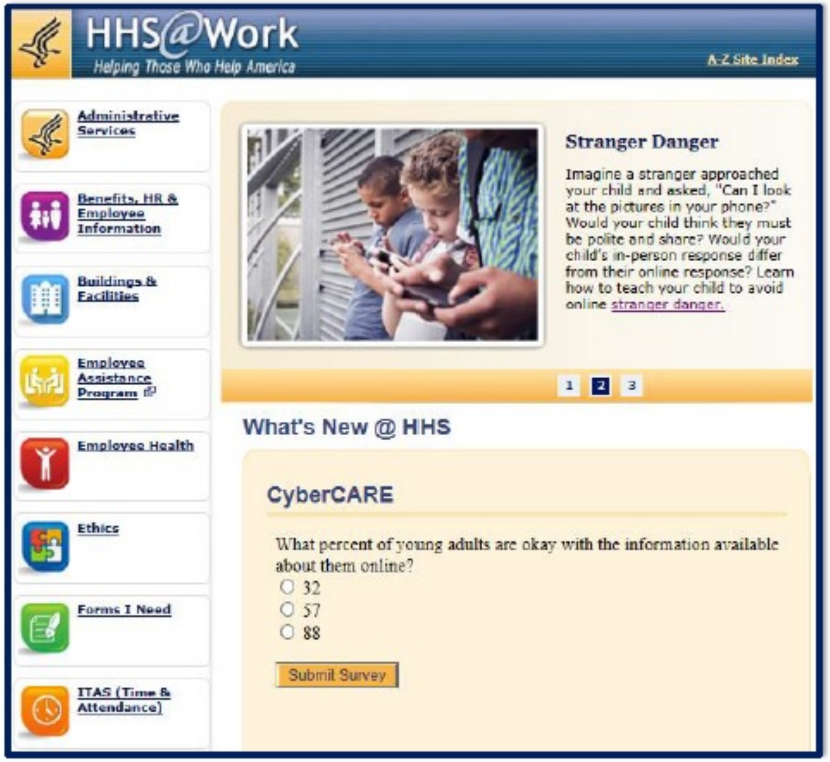
While we're submitting our entry under the Website category, CyberCARE is so much more. We start with a theme each month ("Season's Thievings" in December, Cyber-Resolutions in January, Safer Internet Day in February, and Cyber Crime of Opportunity in March) and introduce it through a blast email to 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…

HHS Intranet Home



Stranger Danger

Imagine a stranger approached your child and asked, "Can I look at the pictures in your phone?" Would your child think they must be polite and share? Would your child's in-person response differ from their online response? Learn how to teach your child to avoid online stranger danger.

What's New @ HHS

CyberCARE

What percent of young adults are okay with the information available about them online?

○ 32
○ 57
○ 88

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.

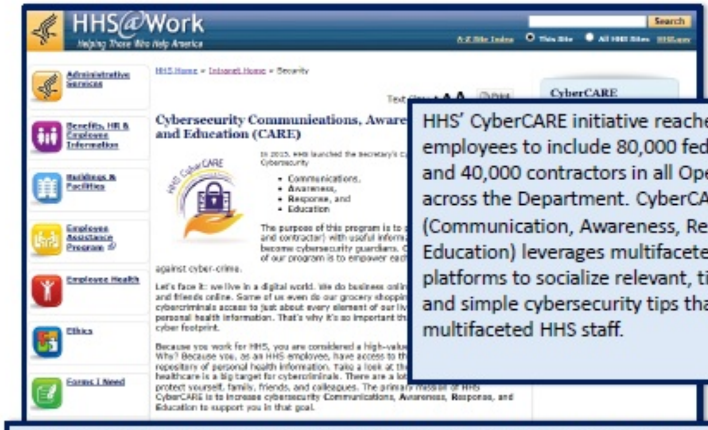
Website Winner!

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



Cybersecurity Communications, Aware
and Education (CARE)

In 2015, HHS launched the Secretary's c
Cybersecurity

- Communications,
- Awareness,
- Response, and
- Education

The purpose of this program is to
and contractor) with useful inform
become cybersecurity guardians.
of our program is to empower eac
against cyber-crime.

Let's face it: we live in a digital world. We do business onlin
and friends online. Some of us even do our grocery shoppin
cybercriminals access to just about every element of our liv
personal health information. That's why it's so important th
cyber footprint.

Because you work for HHS, you are considered a high-valu
Why? Because you, as an HHS employee, have access to th
repository of personal health information. Take a look at th
healthcare is a big target for cybercriminals. There are a lot
protect yourself, family, friends, and colleagues. The primary mission of HHS
CyberCARE is to increase cybersecurity Communications, Awareness, Response, and
Education to support you in that goal.

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.

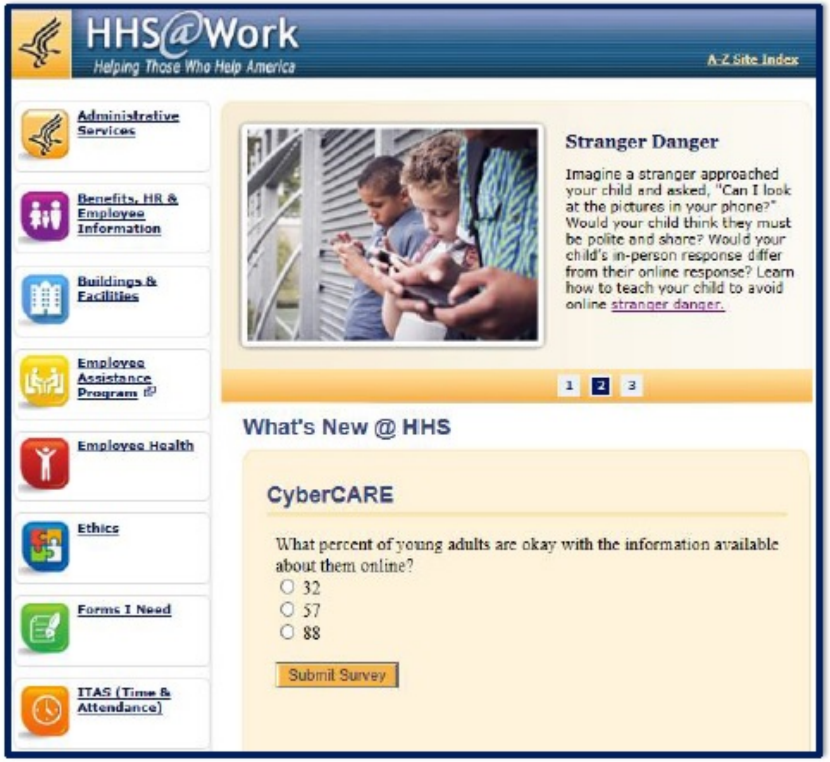
While we're submitting our entry under the Website category, CyberCARE is so much more. We start with a theme each month ("Season's Thievings" in December, Cyber-Resolutions in January, Safer Internet Day in February, and Cyber Crime of Opportunity in March) and introduce it through a blast email to 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…

HHS Intranet Home



Stranger Danger

Imagine a stranger approached your child and asked, "Can I look at the pictures in your phone?" Would your child think they must be polite and share? Would your child's in-person response differ from their online response? Learn how to teach your child to avoid online stranger danger.

What's New @ HHS

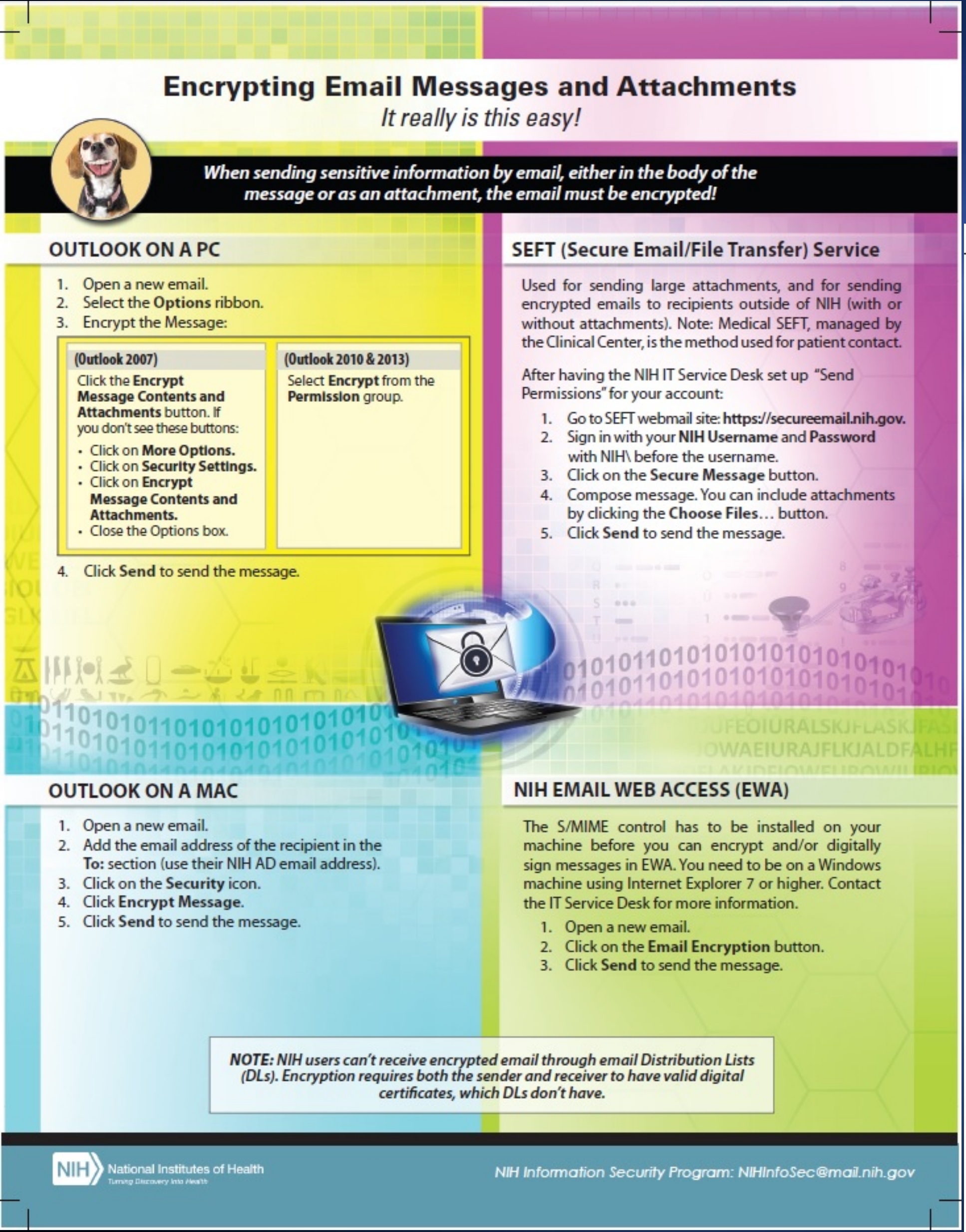
CyberCARE

What percent of young adults are okay with the information available about them online?

○ 32
○ 57
○ 88

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:

(Outlook 2007)	(Outlook 2010 & 2013)
Click the **Encrypt Message Contents and Attachments** button. If you don't see these buttons: • Click on **More Options.** • Click on **Security Settings.** • Click on **Encrypt Message Contents and Attachments.** • Close the Options box.	Select **Encrypt** from the **Permission** group.

4. Click **Send** to send 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:

1. Go to SEFT webmail site: **https://secureemail.nih.gov.**
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.

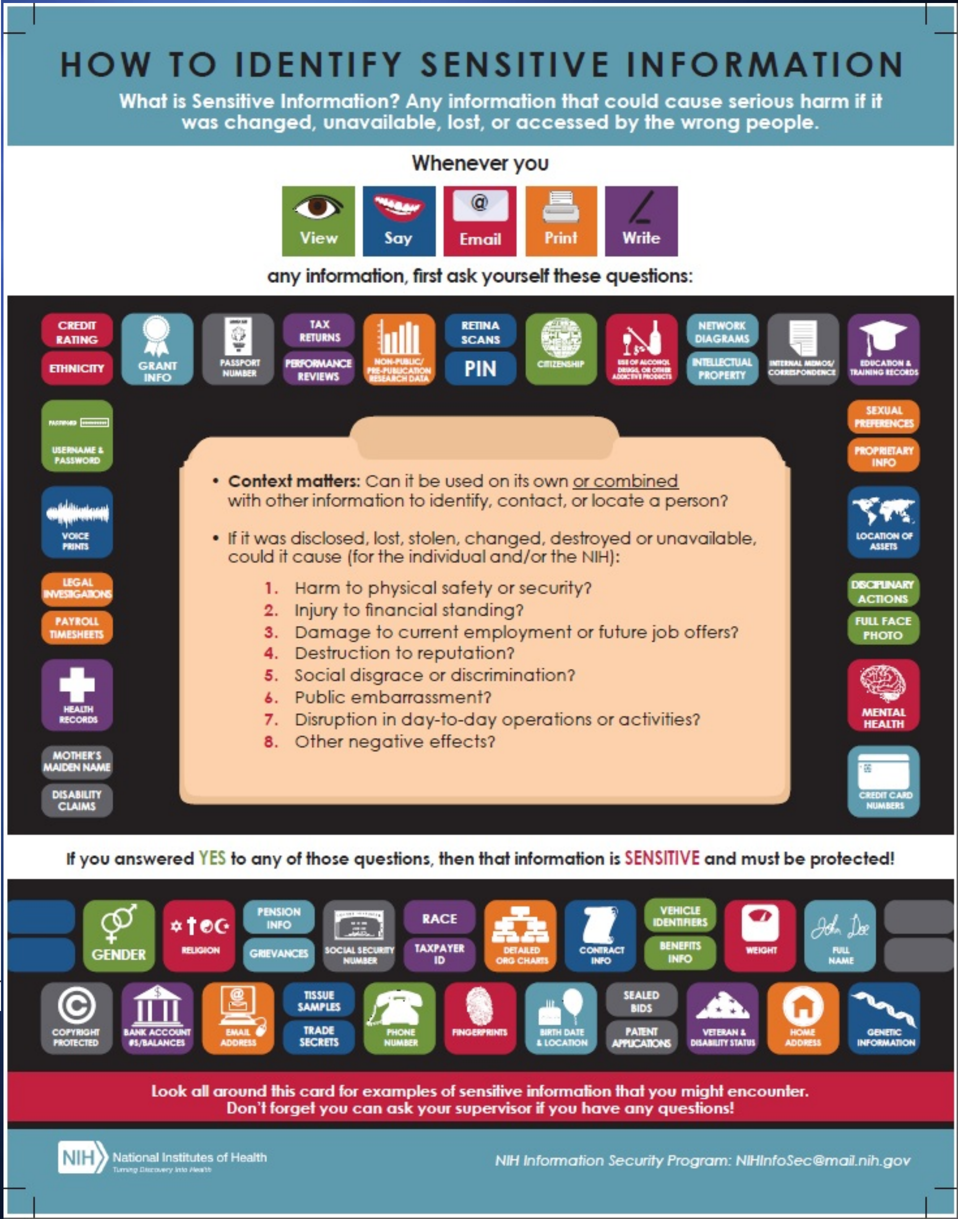
1. Open a new email.
2. Click on the **Email Encryption** button.
3. Click **Send** to send the message.

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.*

NIH National Institutes of Health
Turning Discovery Into Health

NIH Information Security Program: NIHInfoSec@mail.nih.gov

Reference Card



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 | Write

any information, first ask yourself these questions:

- **Context matters:** Can it be used on its own <u>or combined</u> with other information to identify, contact, or locate a person?
- If it was disclosed, lost, stolen, changed, destroyed or unavailable, could it cause (for 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!

CREDIT RATING · ETHNICITY · GRANT INFO · PASSPORT NUMBER · TAX RETURNS · PERFORMANCE REVIEWS · NON-PUBLIC/ PRE-PUBLICATION RESEARCH DATA · RETINA SCANS · PIN · CITIZENSHIP · USE OF ALCOHOL, DRUGS, OR OTHER ADDICTIVE PRODUCTS · NETWORK DIAGRAMS · INTELLECTUAL PROPERTY · INTERNAL MEMOS/ CORRESPONDENCE · EDUCATION & TRAINING RECORDS · USERNAME & PASSWORD · VOICE PRINTS · LEGAL INVESTIGATIONS · PAYROLL TIMESHEETS · HEALTH RECORDS · MOTHER'S MAIDEN NAME · DISABILITY CLAIMS · SEXUAL PREFERENCES · PROPRIETARY INFO · LOCATION OF ASSETS · DISCIPLINARY ACTIONS · FULL FACE PHOTO · MENTAL HEALTH · CREDIT CARD NUMBERS

GENDER · RELIGION · PENSION INFO · GRIEVANCES · SOCIAL SECURITY NUMBER · RACE · TAXPAYER ID · DETAILED ORG CHARTS · CONTRACT INFO · VEHICLE IDENTIFIERS · BENEFITS INFO · WEIGHT · FULL NAME · COPYRIGHT PROTECTED · BANK ACCOUNT #S/BALANCES · EMAIL ADDRESS · TISSUE SAMPLES · TRADE SECRETS · PHONE NUMBER · FINGERPRINTS · BIRTH DATE & LOCATION · SEALED BIDS · PATENT APPLICATIONS · VETERAN & DISABILITY STATUS · HOME ADDRESS · GENETIC INFORMATION

Look all around this card for examples of sensitive information that you might encounter. Don't forget you can ask your supervisor if you have any questions!

NIH National Institutes of Health
Turning Discovery Into Health

NIH Information Security Program: NIHInfoSec@mail.nih.gov

OU ARE THE BEST ANTI-VIRUS!
SECURITY COMES IN CANS NOT CAN'TS
SECURE
ARE THE BEST ANTI-VIRUS!

Motivational Item Winner!

K Rudolph

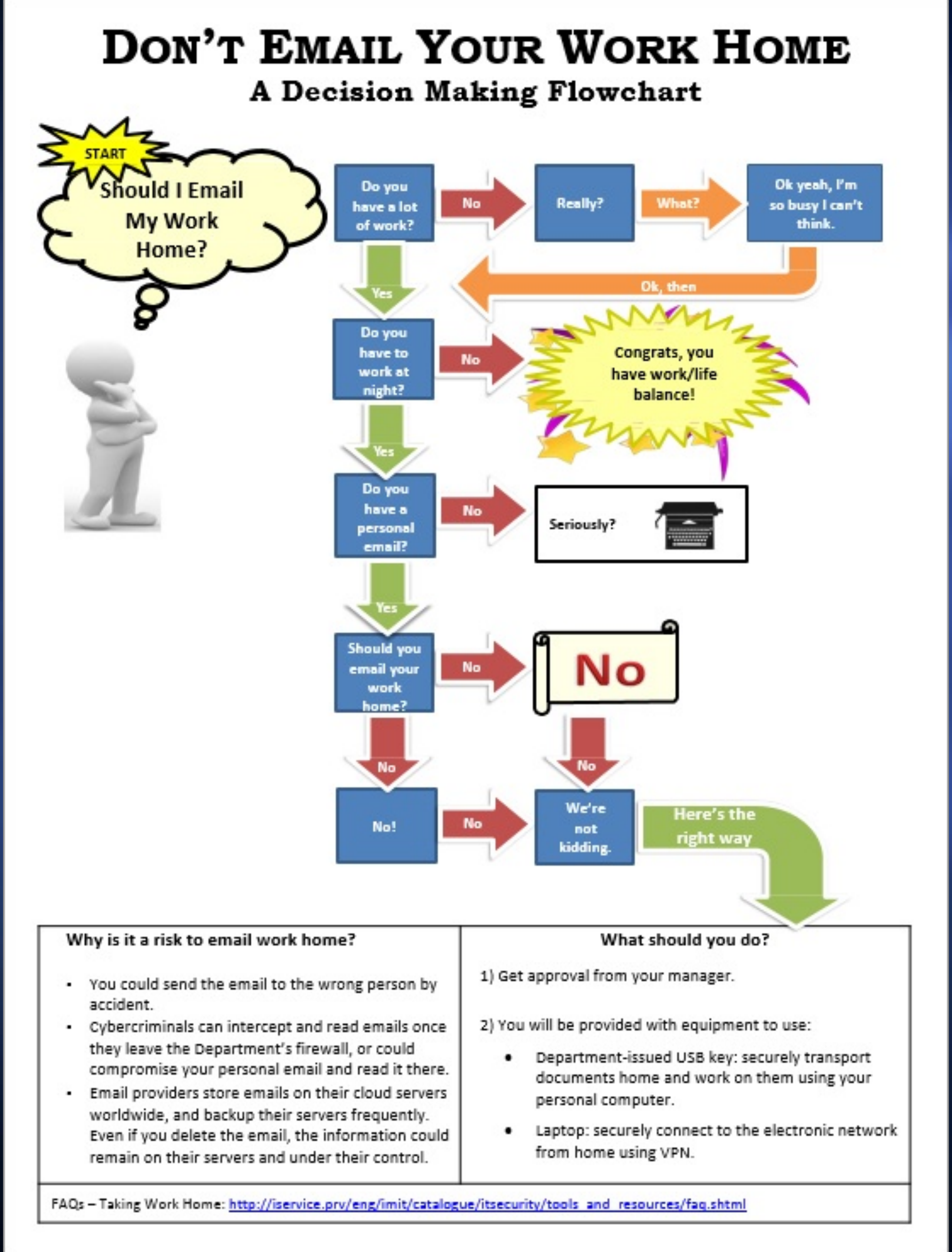
Organization:

Native Intelligence, Inc.

YOU ARE THE BEST ANTI-VIRUS!
SECURITY COMES IN CANS NOT CAN'TS
SECURE
YOU ARE THE BEST ANTI-VIRUS

Poster Entries (11)

BE AWARE...
Connect with care.
ITWD
IT WORKFORCE DEVELOPMENT



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

Yes

Do you have to work at night?

No → Congrats, you have work/life balance!

Yes

Do you have a personal email?

No → Seriously?

Yes

Should you email your work home?

No → No

No

No!

No → We're not kidding.

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.

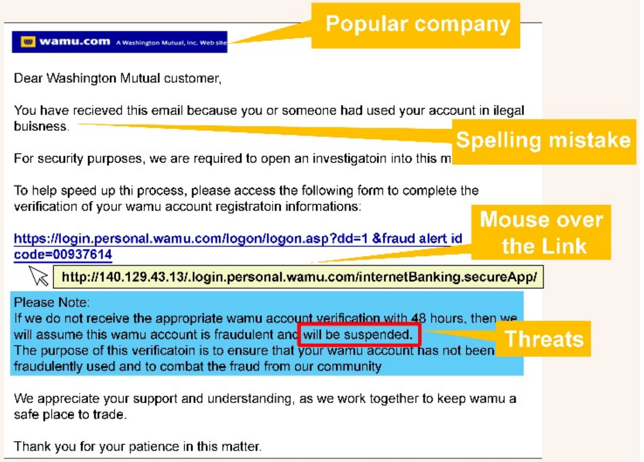
FAQs – Taking Work Home: http://iservice.prv/eng/imit/catalogue/itsecurity/tools_and_resources/faq.shtml

THINK
BEFORE YOU
CLICK

Beware of Phishing

What is Phishing ?

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



wamu.com A Washington Mutual, Inc. Web site

Dear Washington Mutual customer,

You have recieved this email because you or someone had used your account in ilegal buisness.

For security purposes, we are required to open an investigatoin into this m

To help speed up thi process, please access the following form to complete the verification of your wamu account registratoin informations:

https://login.personal.wamu.com/logon/logon.asp?dd=1 &fraud alert id code=00937614

http://140.129.43.13/.login.personal.wamu.com/internetBanking.secureApp/

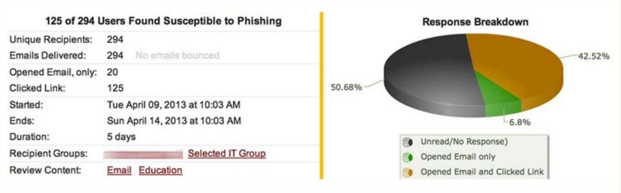
Please Note:
If we do not receive the appropriate wamu account verification with 48 hours, then we will assume this wamu account is fraudulent and will be suspended.
The purpose of this verificatoin is to ensure that your wamu account has not been fraudulently used and to combat the fraud from our community

We appreciate your support and understanding, as we work together to keep wamu a safe place to trade.

Thank you for your patience in this matter.

PhishPond Campaign

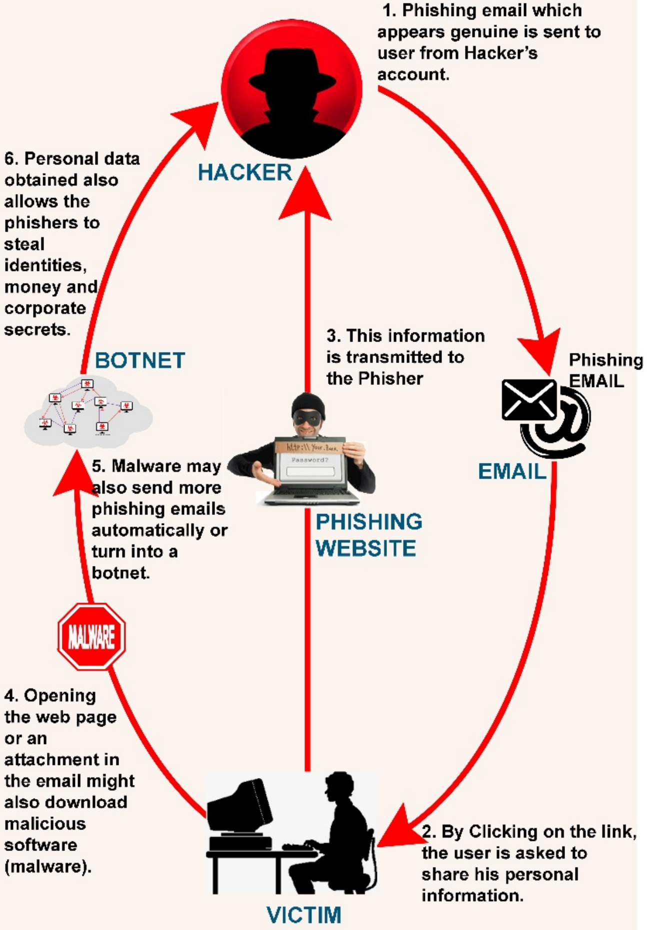
PhishPond team sends an email,
Subject reads : Your request for paid time off



125 of 294 Users Found Susceptible to Phishing

Unique Recipients:	294
Emails Delivered:	294 No emails bounced
Opened Email, only:	20
Clicked Link:	125
Started:	Tue April 09, 2013 at 10:03 AM
Ends:	Sun April 14, 2013 at 10:03 AM
Duration:	5 days
Recipient Groups:	[redacted] Selected IT Group
Review Content:	Email Education

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 web page 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*

What do I do if I receive a suspicious email?

Notification

visit : phishpond.cisco.com

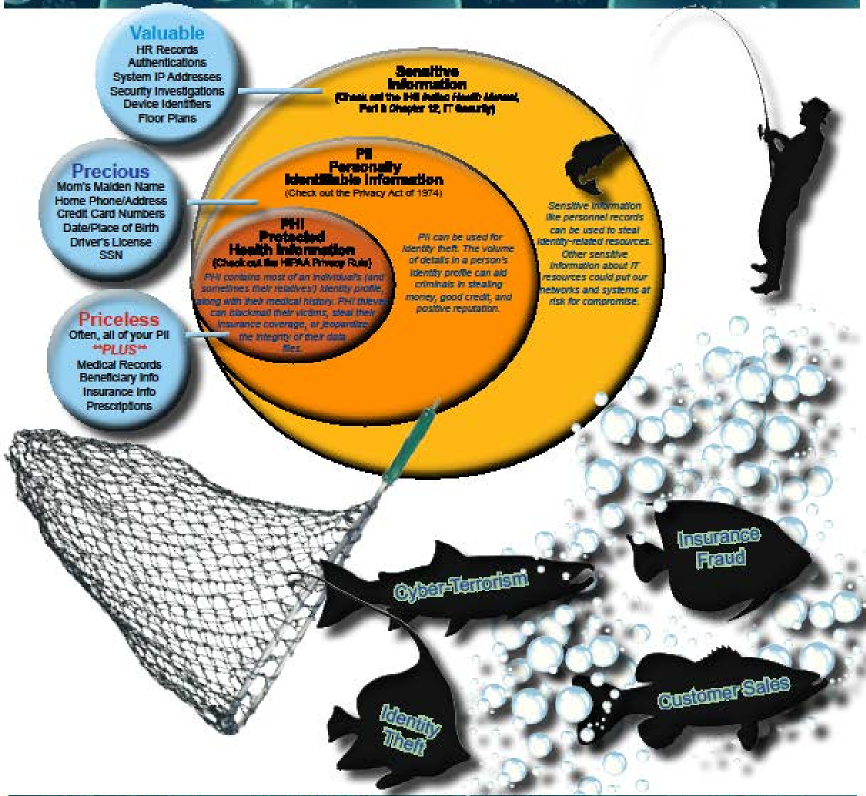
Mitigation

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
HR Records
Authentications
System IP Addresses
Security Investigations
Device Identifiers
Floor Plans

Precious
Mom's Maiden Name
Home Phone/Address
Credit Card Numbers
Date/Place of Birth
Driver's License
SSN

Priceless
Often, all of your PII
*****PLUS*****
Medical Records
Beneficiary Info
Insurance Info
Prescriptions

Sensitive Information
(Check out the IHS *Indian Health Manual*, Part 8 Chapter 12, IT Security)

PII
Personally Identifiable Information
(Check out the Privacy Act of 1974)

PHI
Protected Health Information
(Check out the HIPAA Privacy Rule)

PHI contains most of an individual's (and sometimes their relatives') identity profile, along with their medical history. PHI thieves can blackmail their victims, steal their insurance coverage, or jeopardize the integrity of their data files.

PII can be used for identity theft. The volume of details in a person's identity profile can aid criminals in stealing money, good credit, and positive reputation.

Sensitive information like personnel records can be used to steal identity-related resources. Other sensitive information about IT resources could put our networks and systems at risk for compromise.

Cyber-Terrorism

Cyber-terrorism is a growing threat facing United States organizations. Foreign and state-sponsored agents seek to undermine the faith in American organizations by publicizing their weaknesses.
Domestic terrorists, too, may simply want to cause embarassament or psychological trauma to their victims.

Identity Theft

There is no question about the lucrative benefits for identity theft criminals. Healthcare systems are notorious for being less secure, and the PII within health records allows criminals to access another person's financial resources and open lines of credit. Fraudulent activities can cause the victim endless grief and bad credit.

Customer Sales

Without a doubt, to cyber criminals, the most valuable asset of a healthcare database is the sheer volume of patient information that can be obtained.
Not only are there hundreds or thousands of records in a database worth ten times that of a credit card number, there are also hundreds or thousands of contacts to sell to marketers and other spammers.

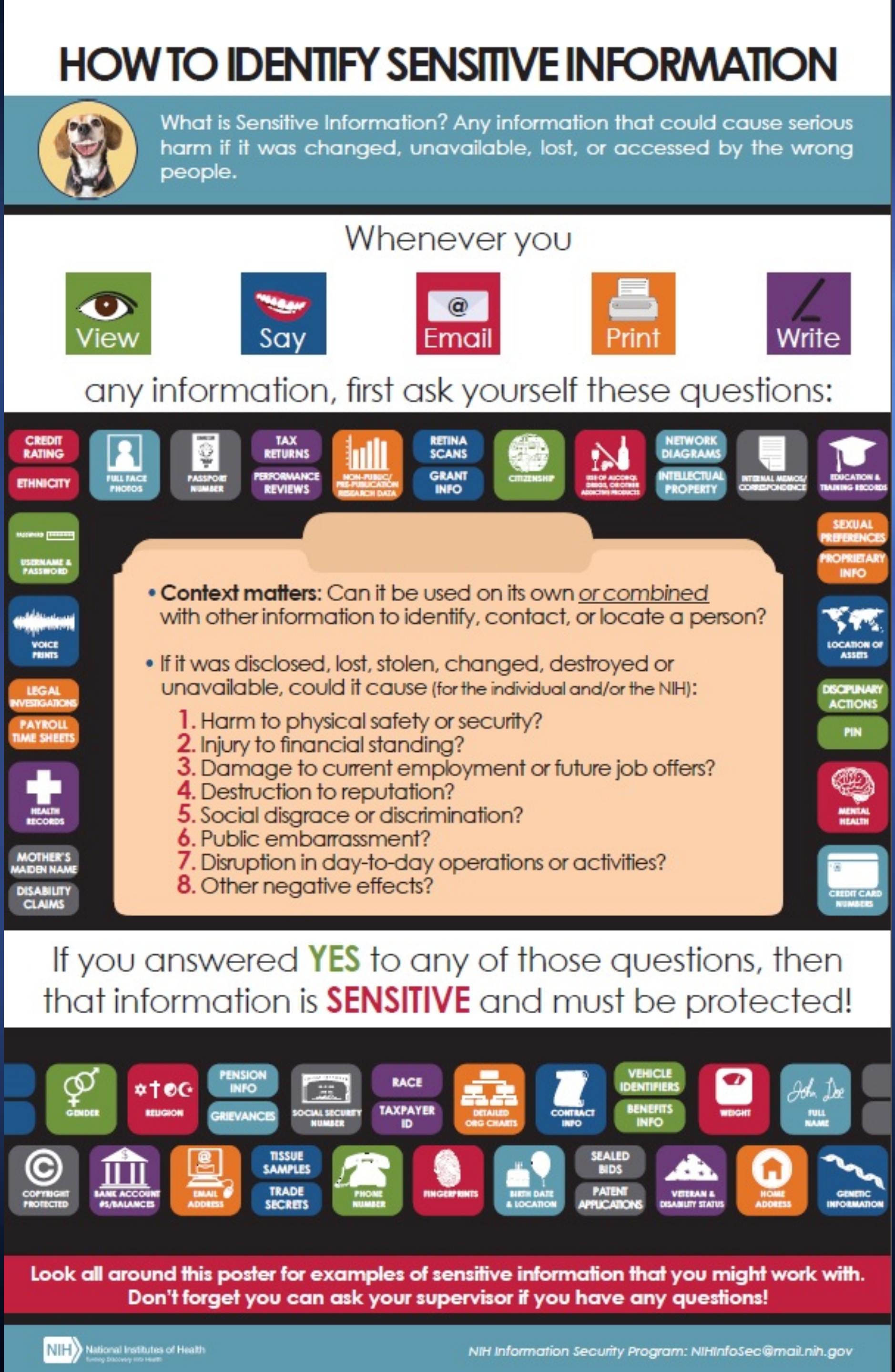
Insurance Fraud

Thieves who steal our patients' health insurance information can use it to file reimbursement claims, to access narcotics, and to qualify for government services.
Fraudlent claims can lead to exceeded coverage caps or loss of coverage. They can also lead to dangerously mishandled medical care when the victim's diagnosis and treatment history have been altered by a fraud.

"Healthcare data are valuable because medical records can be used to commit several types of fraudulent activities or identity theft. Their value in the hacking underground is greater than stolen credit card data." - InfoSec Institute

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 passwords a secret. Don't allow anyone to use your account to access IHS systems. Exercise caution when emailing and browsing the Internet, and don't be reeled in by phishers. If you suspect a breach may have occured, report it immediately!

Report security breaches, phishing attempts, and other security violations to the Incident Response Team at irt@ihs.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

Write

any information, first ask yourself these questions:

CREDIT RATING

ETHNICITY

FULL FACE PHOTOS

PASSPORT NUMBER

TAX RETURNS

PERFORMANCE REVIEWS

NON-PUBLIC/ PRE-PUBLICATION RESEARCH DATA

RETINA SCANS

GRANT INFO

CITIZENSHIP

USE OF ALCOHOL, DRUGS, OR OTHER ADDICTIVE PRODUCTS

NETWORK DIAGRAMS

INTELLECTUAL PROPERTY

INTERNAL MEMOS/ CORRESPONDENCE

EDUCATION & TRAINING RECORDS

PASSWORD

USERNAME & PASSWORD

VOICE PRINTS

LEGAL INVESTIGATIONS

PAYROLL TIME SHEETS

HEALTH RECORDS

MOTHER'S MAIDEN NAME

DISABILITY CLAIMS

SEXUAL PREFERENCES

PROPRIETARY INFO

LOCATION OF ASSETS

DISCIPLINARY ACTIONS

PIN

MENTAL HEALTH

CREDIT CARD NUMBERS

- **Context matters:** Can it be used on its own <u>or combined</u> with other information to identify, contact, or locate a person?
- If it was disclosed, lost, stolen, changed, destroyed or unavailable, could it cause (for 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!

GENDER

RELIGION

PENSION INFO

GRIEVANCES

SOCIAL SECURITY NUMBER

RACE

TAXPAYER ID

DETAILED ORG CHARTS

CONTRACT INFO

VEHICLE IDENTIFIERS

BENEFITS INFO

WEIGHT

John Doe

FULL NAME

COPYRIGHT PROTECTED

BANK ACCOUNT #S/BALANCES

EMAIL ADDRESS

TISSUE SAMPLES

TRADE SECRETS

PHONE NUMBER

FINGERPRINTS

BIRTH DATE & LOCATION

SEALED BIDS

PATENT APPLICATIONS

VETERAN & DISABILITY STATUS

HOME ADDRESS

GENETIC INFORMATION

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!

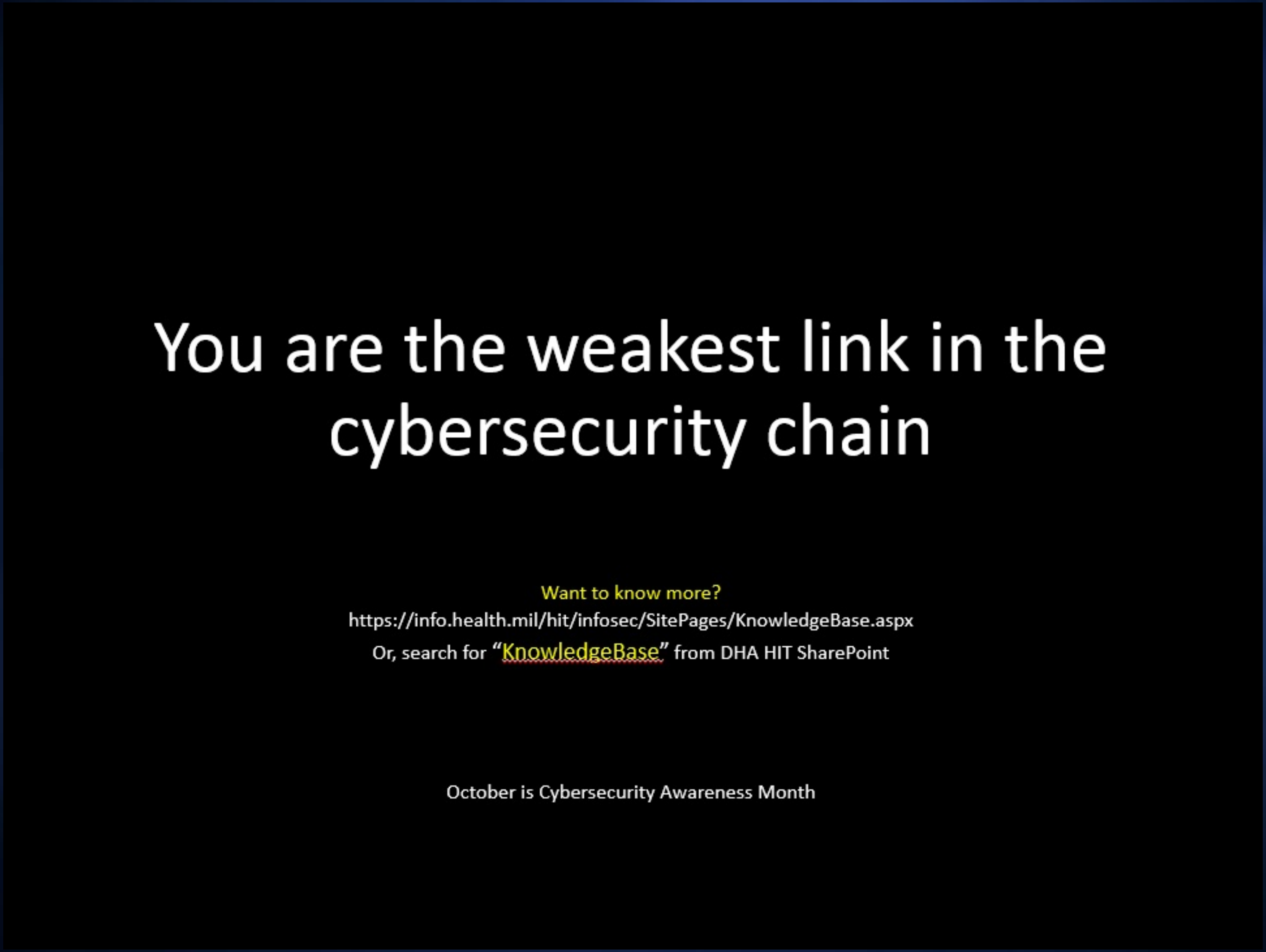
NIH National Institutes of Health
Turning Discovery Into Health

NIH Information Security Program: NIHInfoSec@mail.nih.gov

Your online presence is...

...as permanent as a tattoo.

Bureau of Diplomatic Security | Office of Cybersecurity



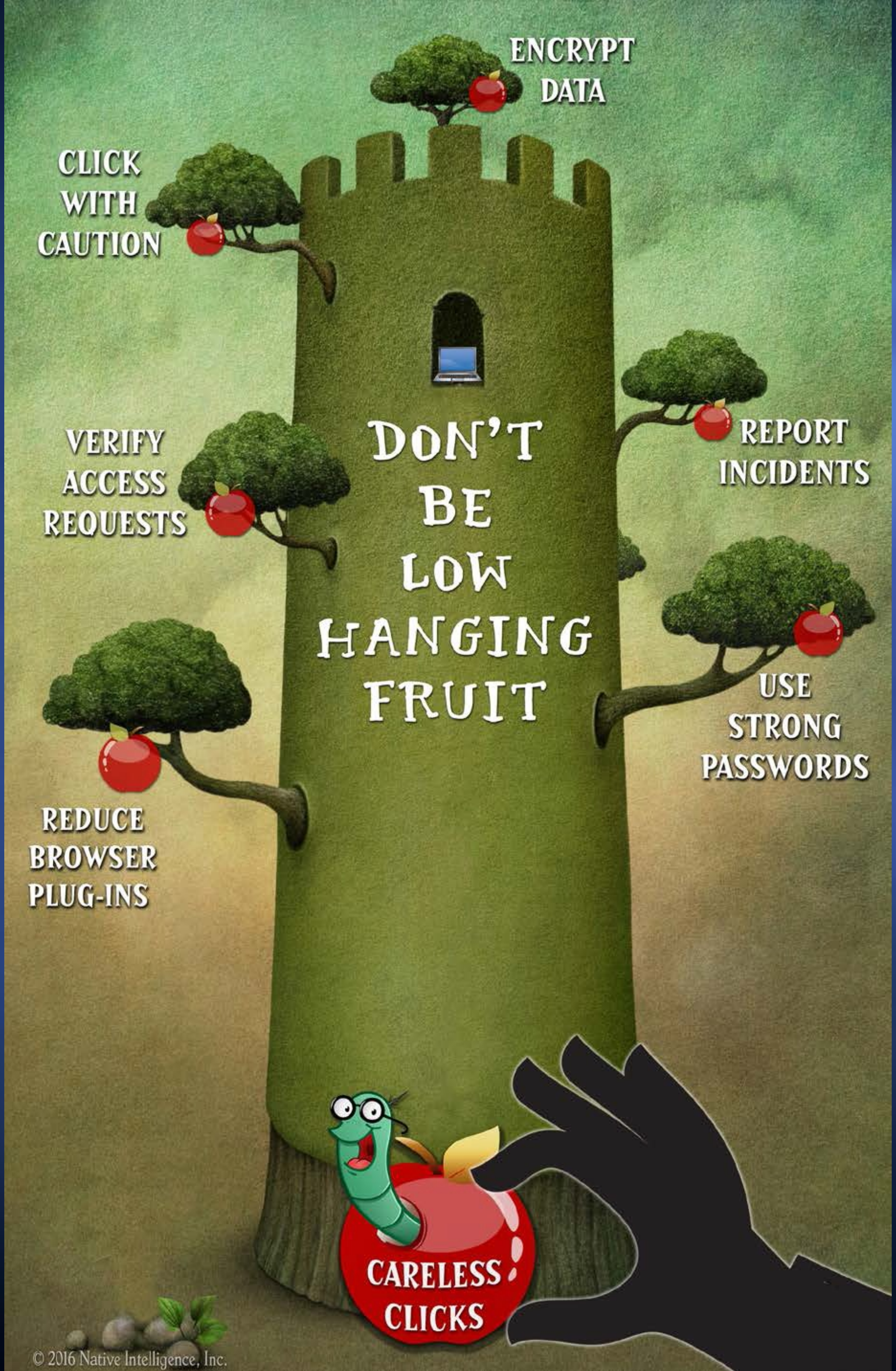
You are the weakest link in the cybersecurity chain

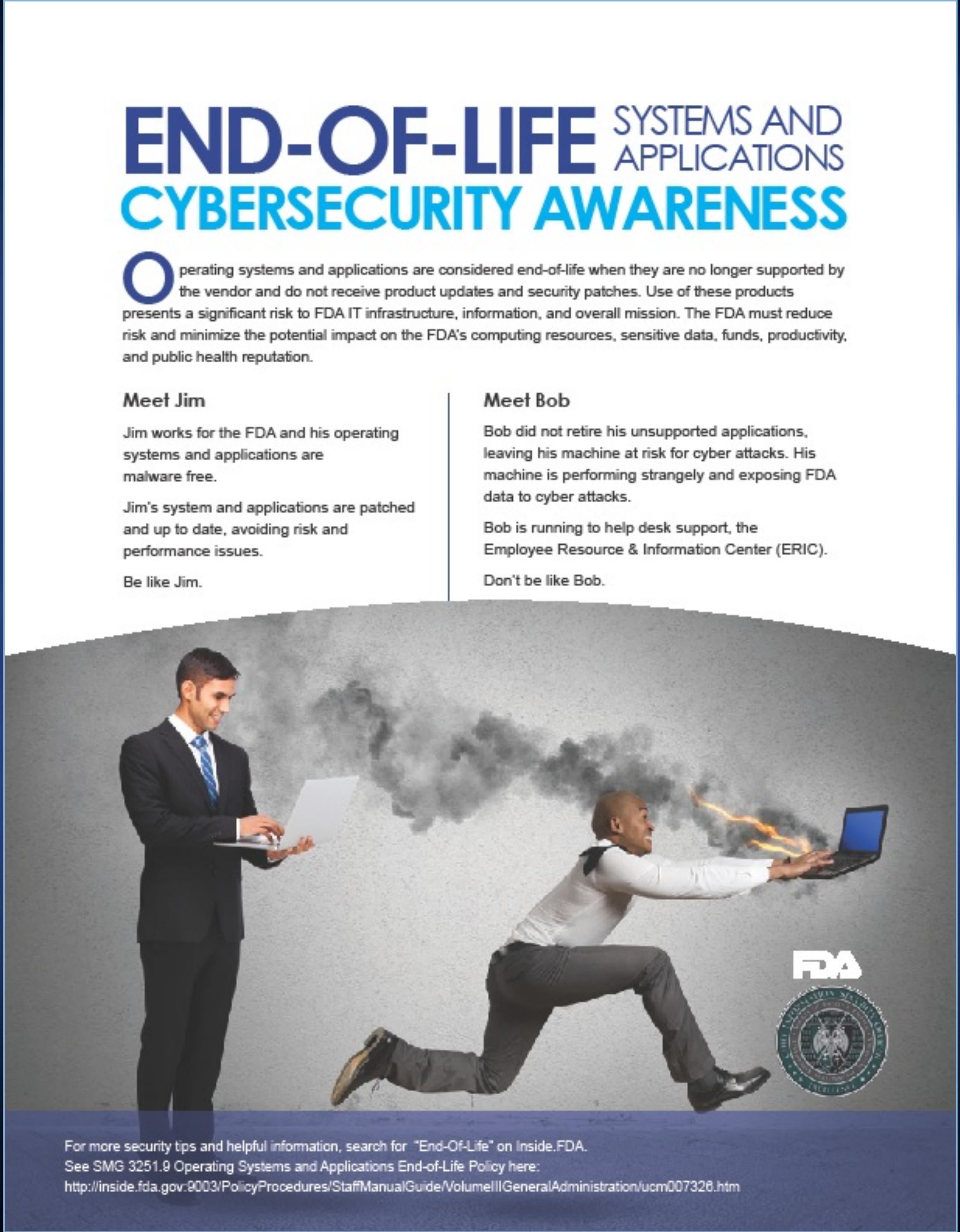
Want to know more?

https://info.health.mil/hit/infosec/SitePages/KnowledgeBase.aspx

Or, search for "KnowledgeBase" from DHA HIT SharePoint

October is Cybersecurity Awareness Month


ENCRYPT DATA
CLICK WITH CAUTION
DON'T BE LOW HANGING FRUIT
REPORT INCIDENTS
VERIFY ACCESS REQUESTS
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.

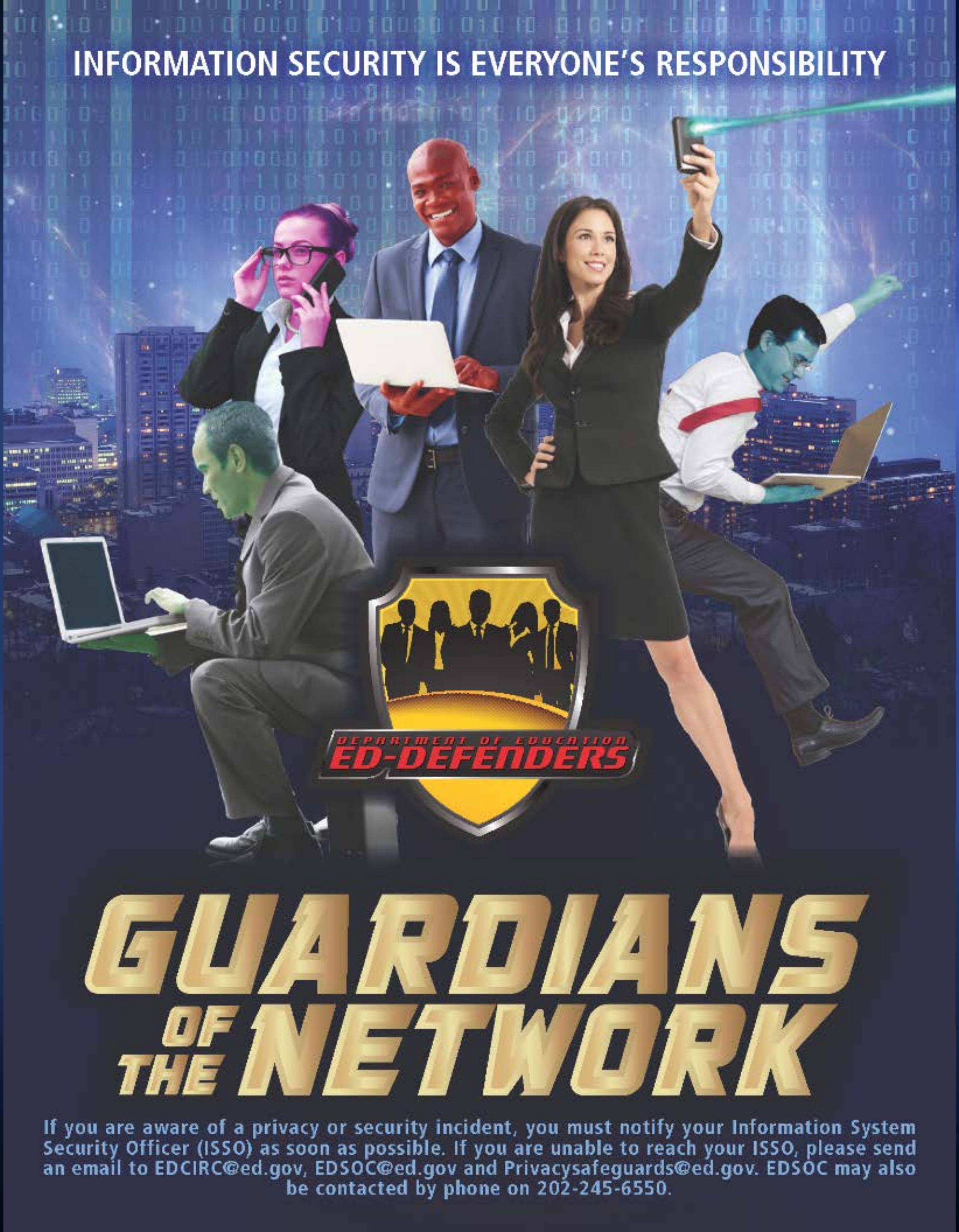
Meet Bob

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.

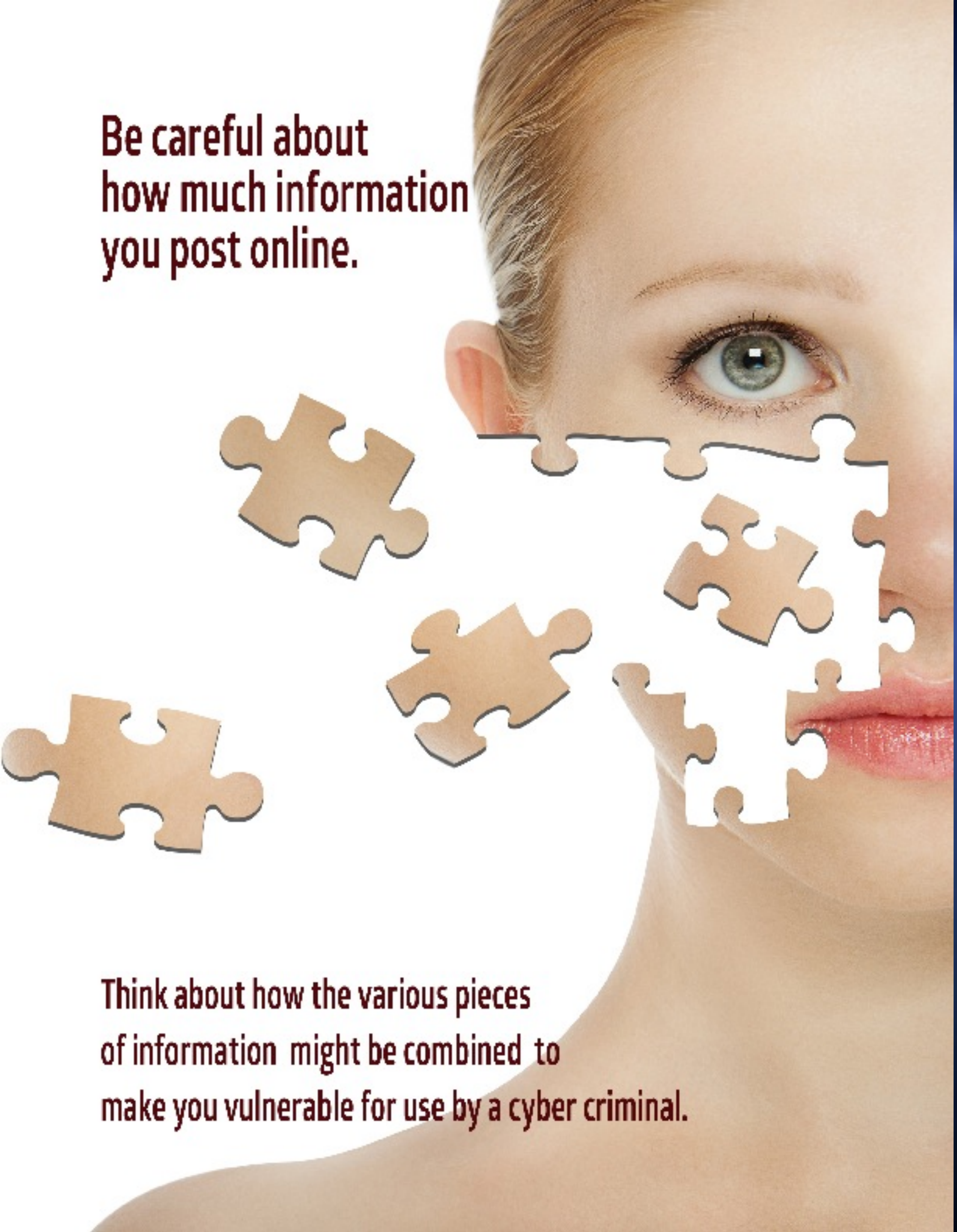
Bob is running to help desk support, the Employee Resource & Information Center (ERIC).

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:
http://inside.fda.gov:9003/PolicyProcedures/StaffManualGuide/VolumeIIIGeneralAdministration/ucm007326.htm



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 202-245-6550.



Be careful about
how much information
you post online.

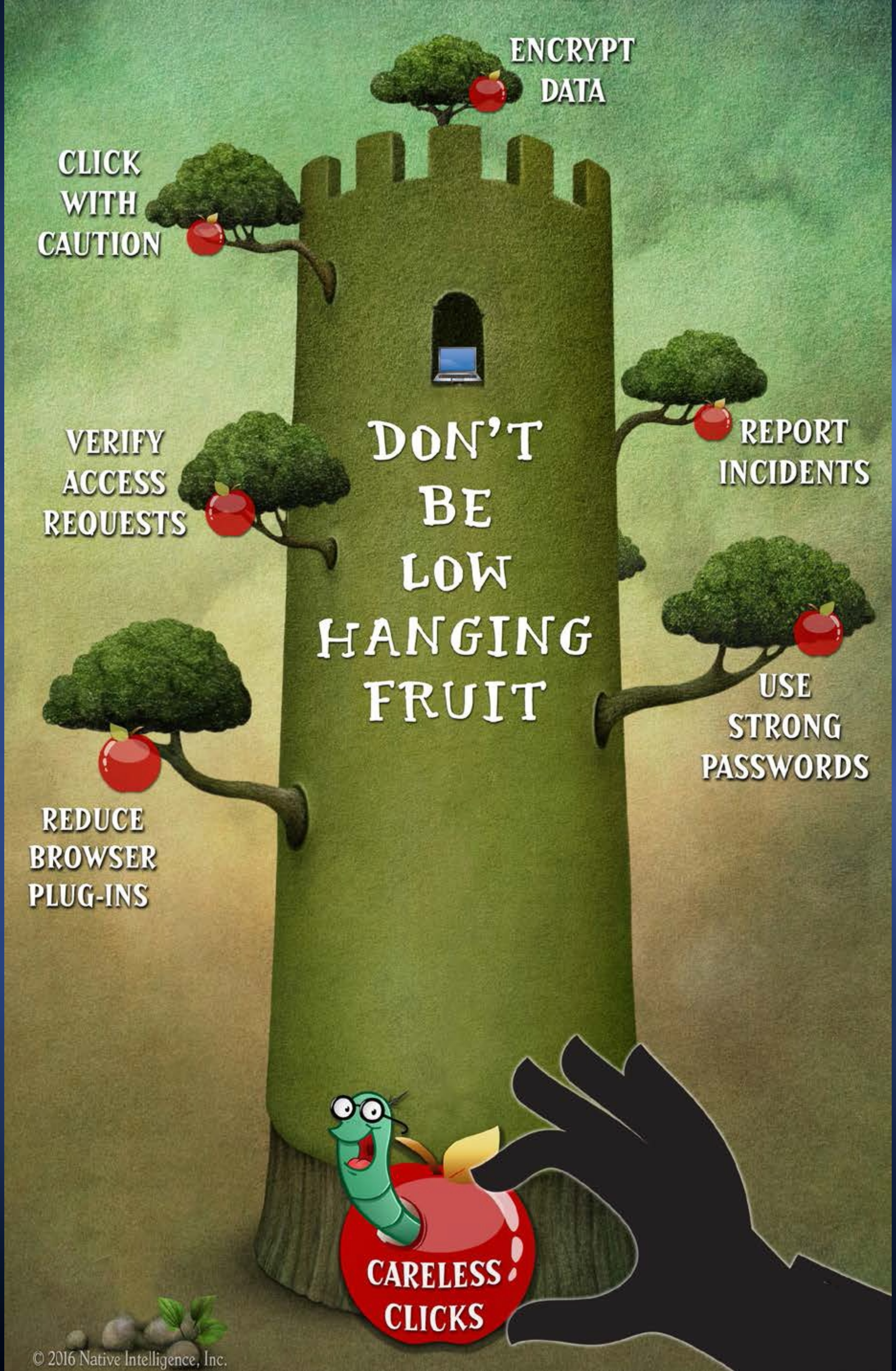
Think about how the various pieces
of information might be combined to
make you vulnerable for use by a cyber criminal.

Poster Winner!

**K Rudolph, John Ippolito,
G. Mark Hardy, Andrew Ellis,
& Charles A. Filius**

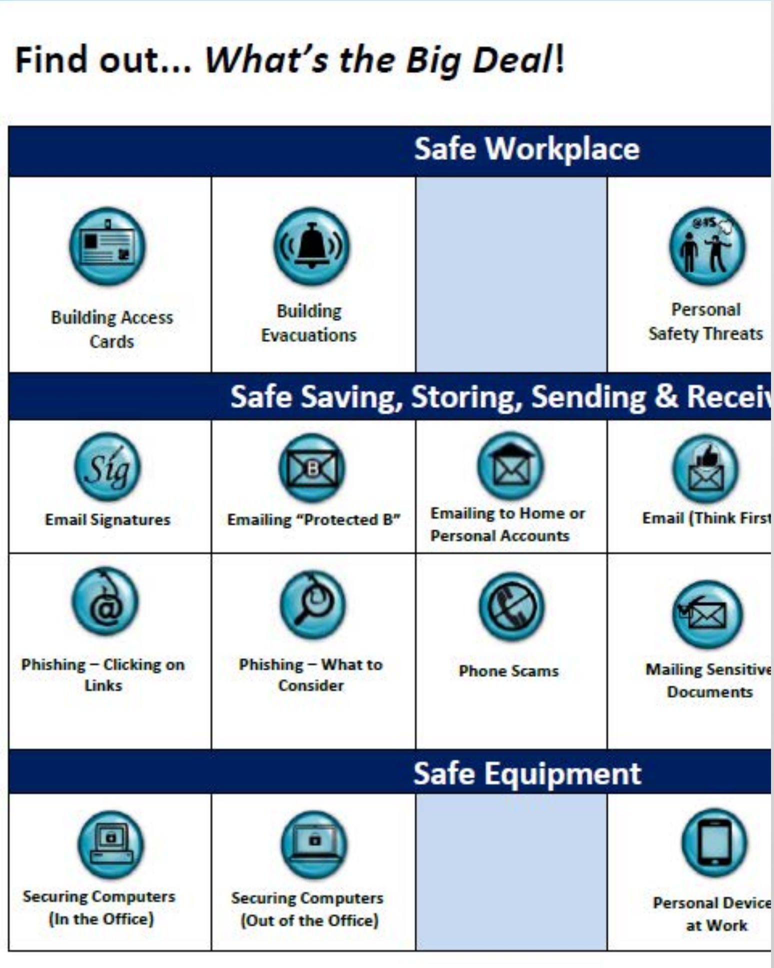
Organization:

Native Intelligence, Inc. and Friends


ENCRYPT DATA
CLICK WITH CAUTION
DON'T BE LOW HANGING FRUIT
REPORT INCIDENTS
VERIFY ACCESS REQUESTS
USE STRONG PASSWORDS
REDUCE BROWSER PLUG-INS
CARELESS CLICKS

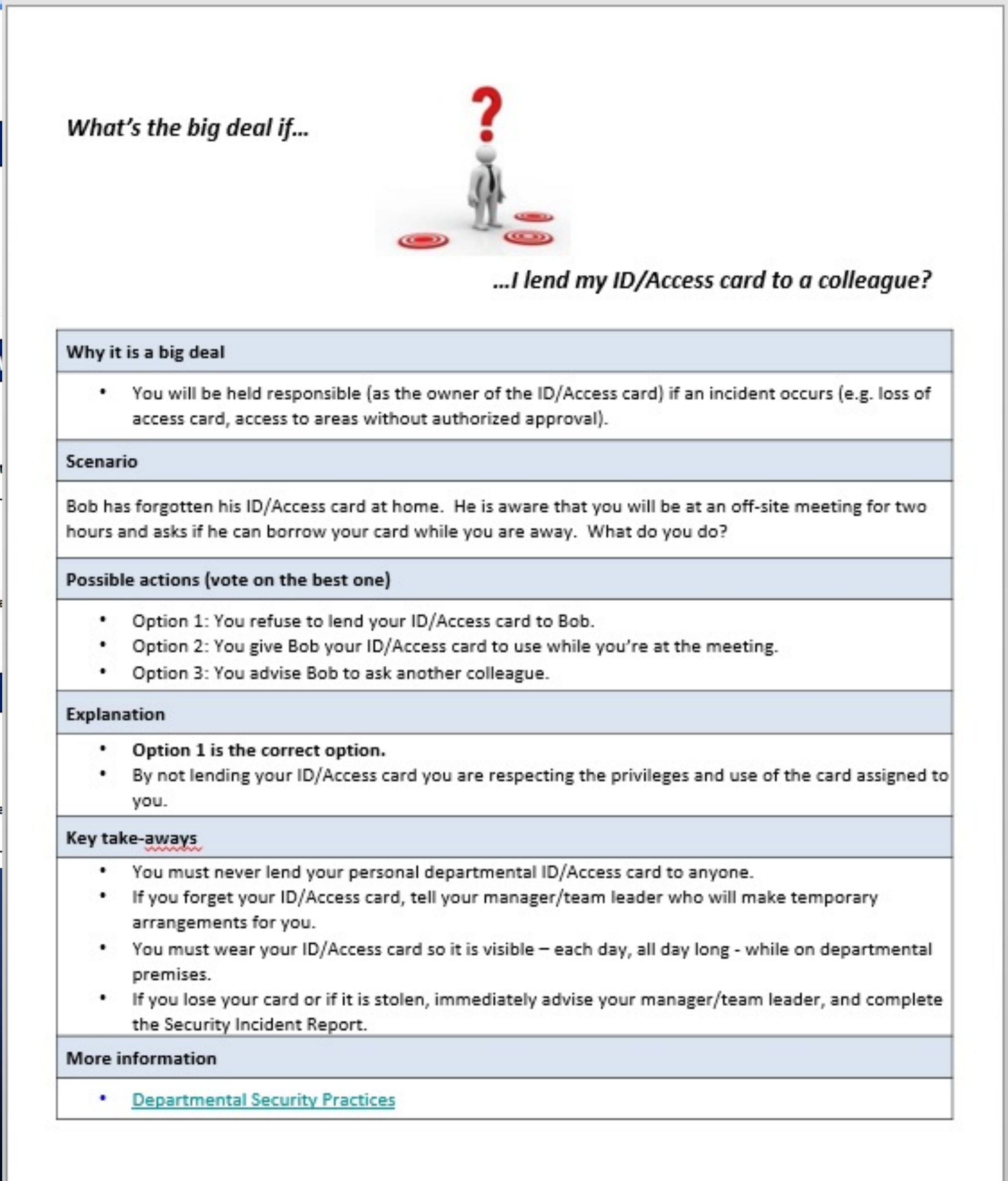
Newsletter Entries (7)

Easy Action Toolkit for Employees and Managers



Find out… *What's the Big Deal*!

Safe Workplace			
Building Access Cards	Building Evacuations		Personal Safety Threats
Safe Saving, Storing, Sending & Recei			
Email Signatures	Emailing "Protected B"	Emailing to Home or Personal Accounts	Email (Think First
Phishing – Clicking on Links	Phishing – What to Consider	Phone Scams	Mailing Sensitive Documents
Safe Equipment			
Securing Computers (In the Office)	Securing Computers (Out of the Office)		Personal Device at Work



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

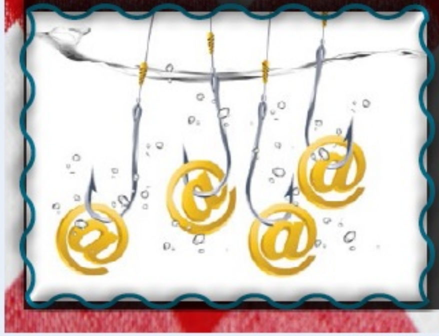
Best Phish Bait on the Market

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 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 unappetizing phishing campaign. While there is no magic solution for combatting 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!

National Cyber Security Awareness Month
October 2015
OUR SHARED RESPONSIBILITY

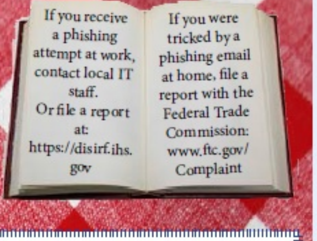
Fry a Better Phish

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 irt@ihs.gov!!



If you receive a phishing attempt at work, contact local IT staff.
Or file a report at: https://disirf.ihs.gov

If you were tricked by a phishing email at home, file a report with the Federal Trade Commission: www.ftc.gov/Complaint

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 fake website asking you 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.

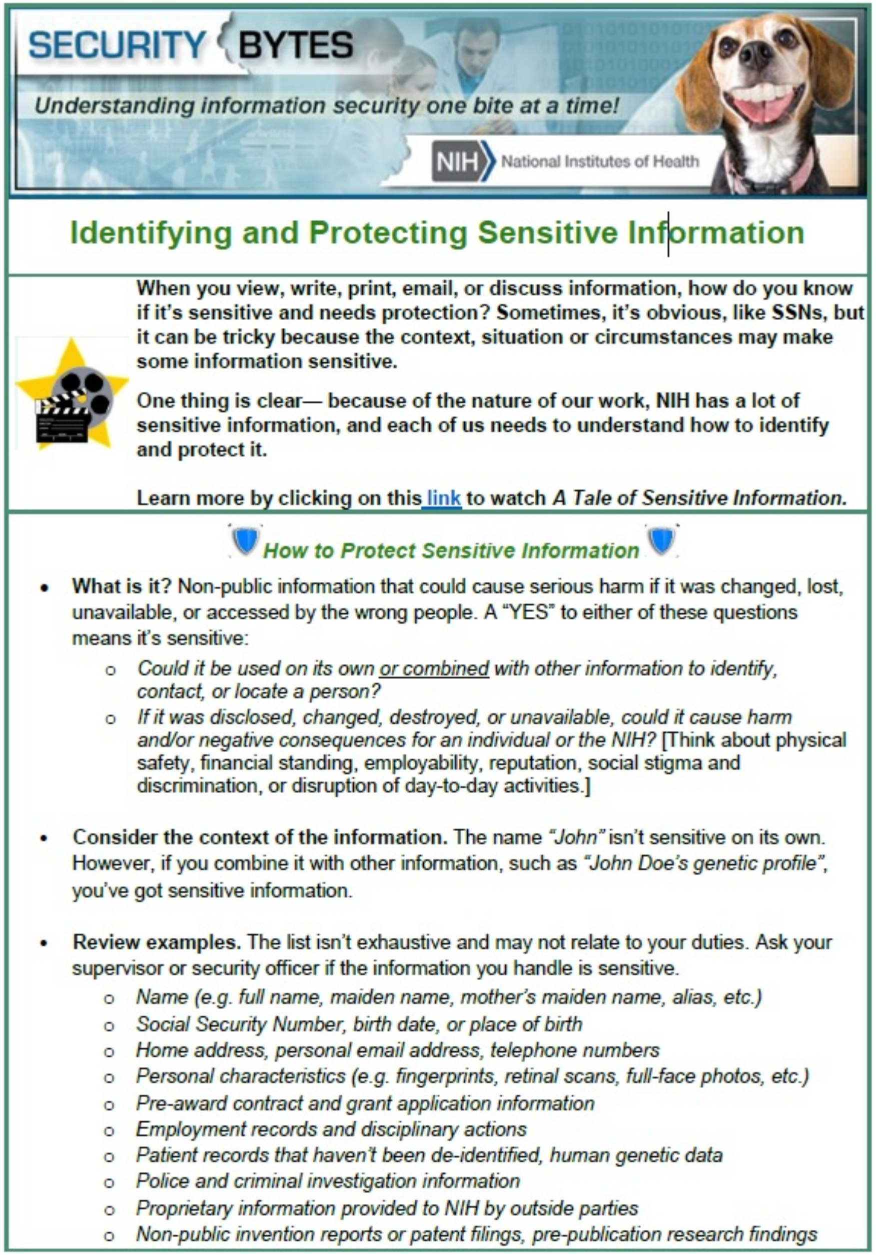
Directions: Don't respond to unfamiliar texters requesting personal information. Beware of messages from non-phone-numbers like "4325." That's a tactic scammers use to mask their identity by using email-to-text services that conceal their actual phone number. DON'T RESPOND!!

Recipe #4 - Don't 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!!



SECURITY BYTES

Understanding information security one bite at a time!

NIH National Institutes of Health

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.

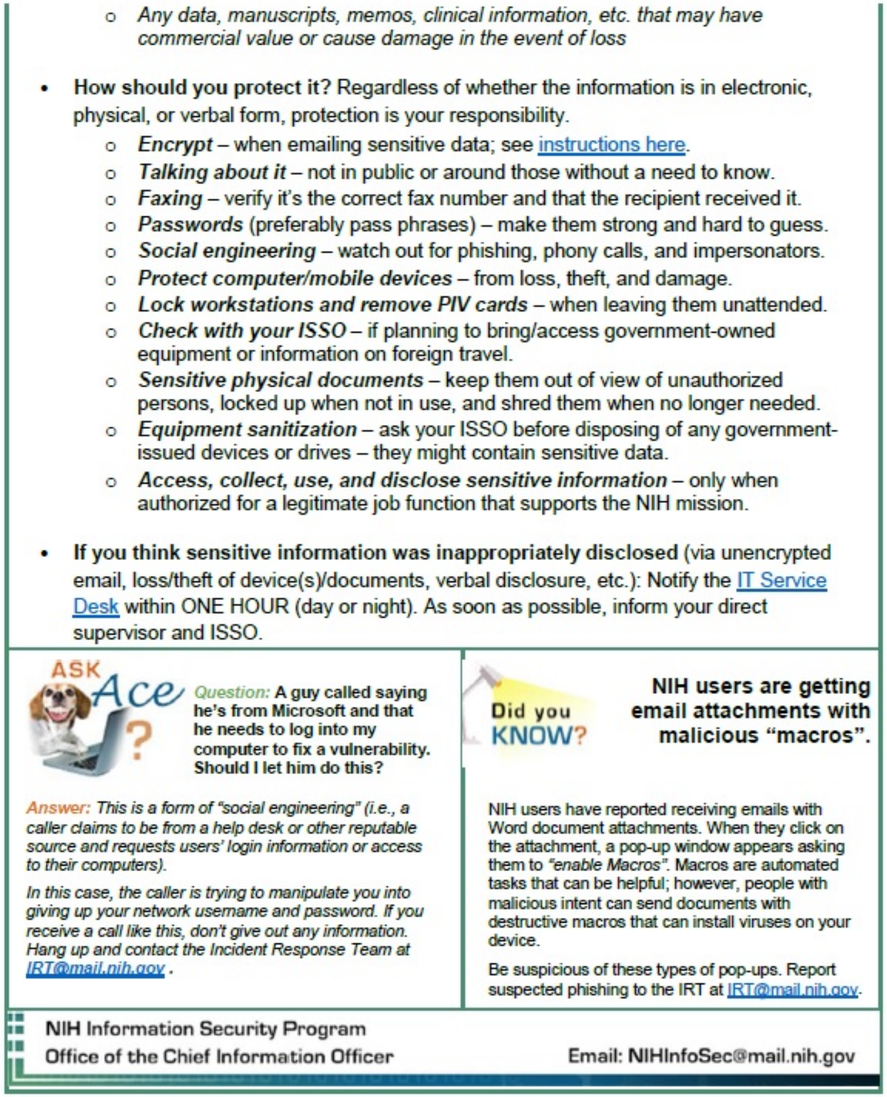
Learn more by clicking on this link to watch *A Tale of Sensitive Information.*

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, retinal 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*



  - *Any data, manuscripts, memos, clinical information, etc. that may have commercial value or cause damage in the event of loss*

- **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.

ASK Ace ?

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 or other reputable source and requests users' login information 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 .

Did you KNOW?

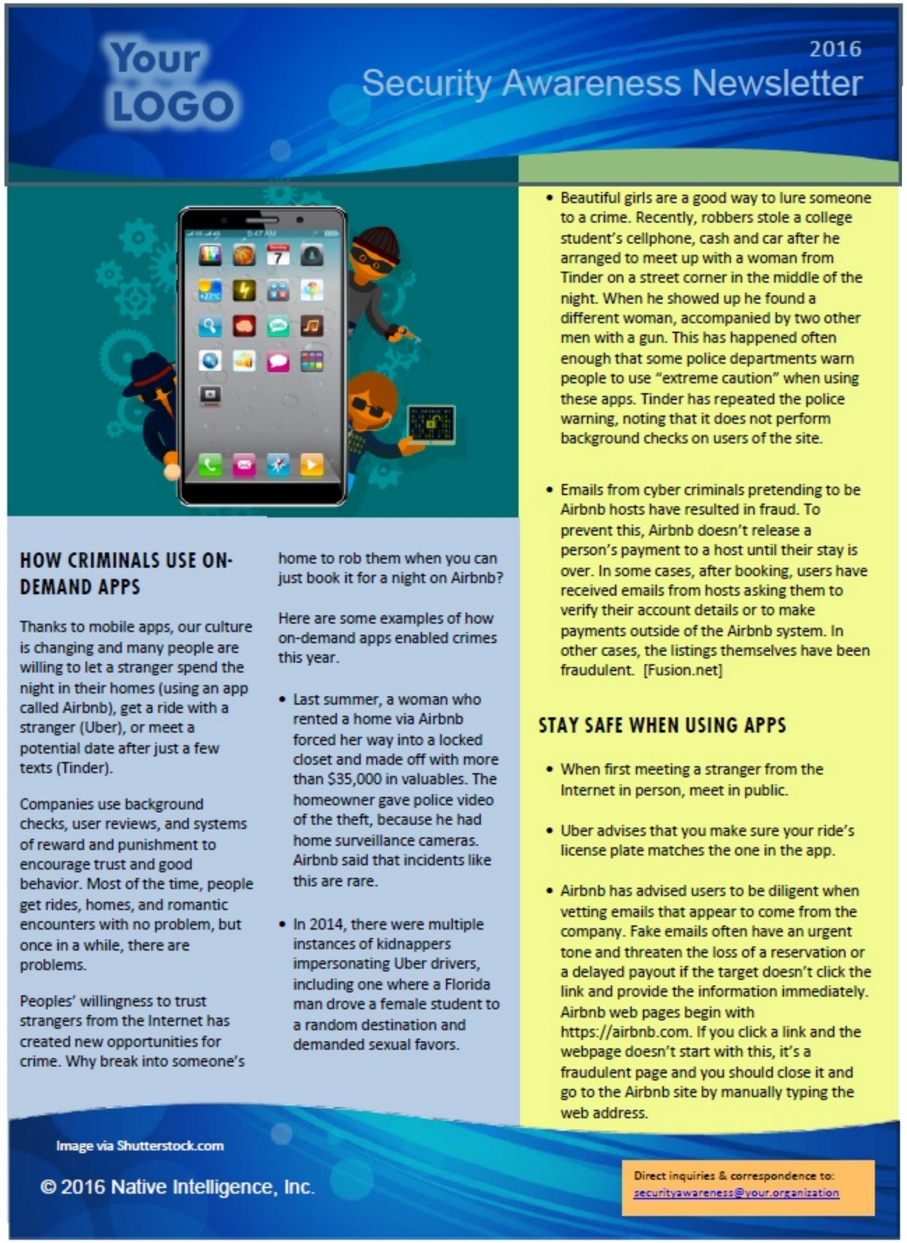
NIH users are getting email attachments with malicious "macros".

NIH users have reported receiving emails with Word document attachments. When they click on the attachment, a pop-up window appears asking them to *"enable Macros"*. Macros are automated tasks that can be helpful; however, people with malicious intent can send documents with destructive macros that can install viruses on your device.

Be suspicious of these types of pop-ups. Report suspected phishing to the IRT at IRT@mail.nih.gov.

NIH Information Security Program
Office of the Chief Information Officer

Email: NIHInfoSec@mail.nih.gov



Your LOGO

2016

Security Awareness Newsletter

- Beautiful girls are a good way to lure someone to a crime. Recently, robbers stole a college student's cellphone, cash and car after he arranged to meet up with a woman from Tinder on a street corner in the middle of the night. When he showed up he found a different woman, accompanied by two other men with a gun. This has happened often enough that some police departments warn people to use "extreme caution" when using these apps. Tinder has repeated the police warning, noting that it does not perform background checks on users of the site.

- Emails from cyber criminals pretending to be Airbnb hosts have resulted in fraud. To prevent this, Airbnb doesn't release a person's payment to a host until their stay is over. In some cases, after booking, users have received emails from hosts asking them to verify their account details or to make payments outside of the Airbnb system. In other cases, the listings themselves have been fraudulent. [Fusion.net]

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 rides, homes, and romantic encounters with no problem, but once in a while, there are problems.

Peoples' 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 random destination and demanded sexual favors.

STAY SAFE WHEN USING APPS

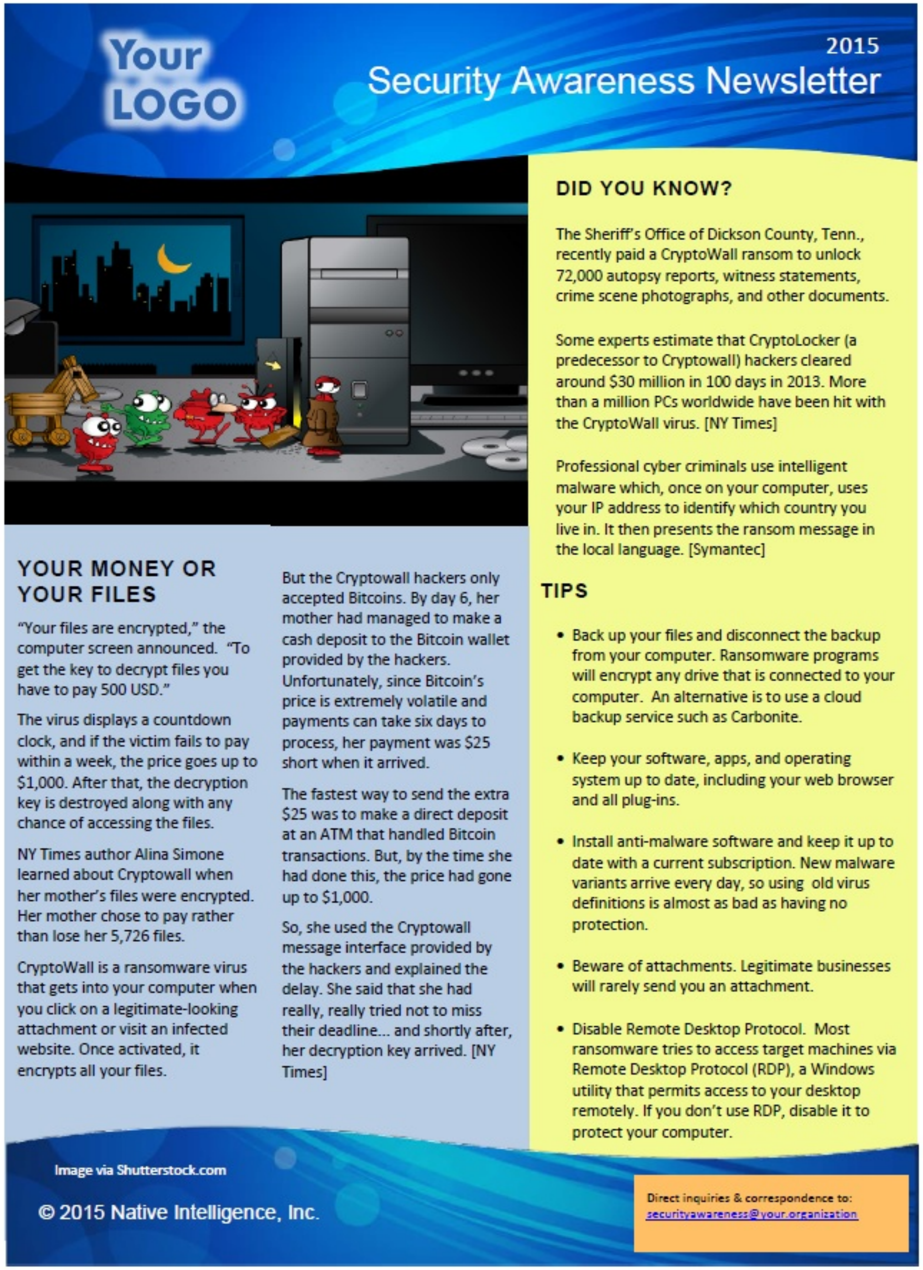
- When first meeting a stranger from the Internet in person, meet in public.

- 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 target 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.

Image via Shutterstock.com

Direct inquiries & correspondence to:
securityawareness@your.organization



Your LOGO

2015

Security Awareness Newsletter

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 cash 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 $1,000.

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

DID YOU KNOW?

The Sheriff's Office of Dickson County, Tenn., recently paid a CryptoWall ransom to unlock 72,000 autopsy reports, witness statements, crime scene photographs, and other documents.

Some experts estimate that CryptoLocker (a predecessor to Cryptowall) hackers cleared around $30 million in 100 days in 2013. More than a million PCs worldwide have been hit with the CryptoWall virus. [NY Times]

Professional cyber criminals use intelligent malware which, once on your computer, uses your IP address to identify which country you live in. It then presents the ransom message in the local language. [Symantec]

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 plug-ins.

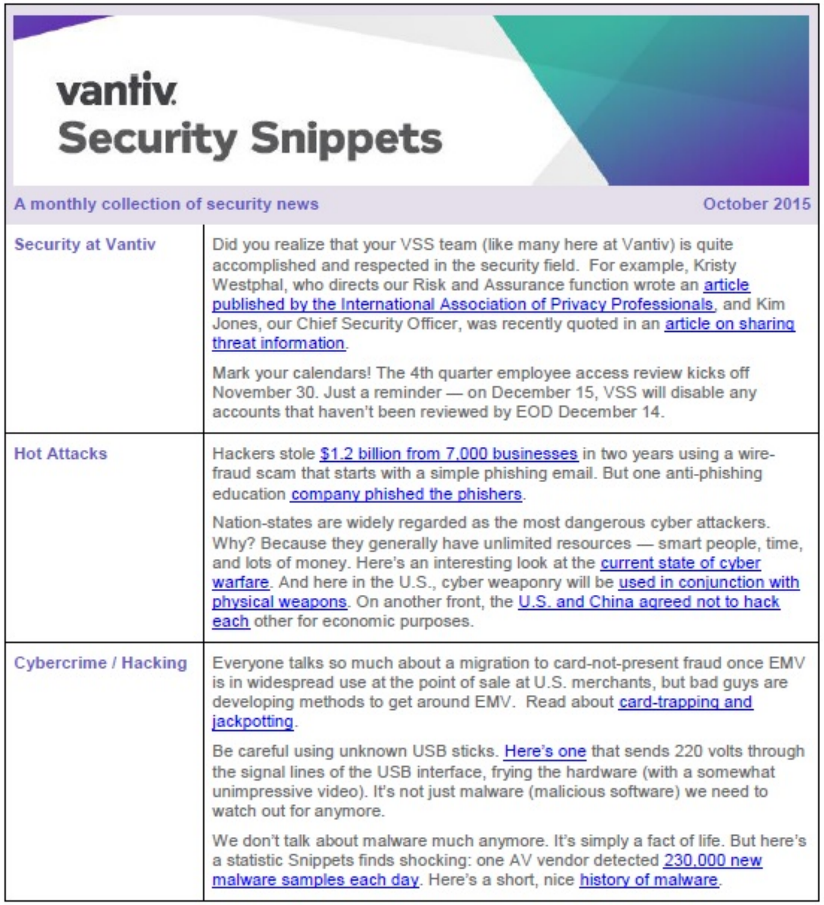
- Install anti-malware software and keep it up to date with a current subscription. New malware variants arrive every day, so using old virus definitions is almost as bad as having no protection.

- 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.

Image via Shutterstock.com

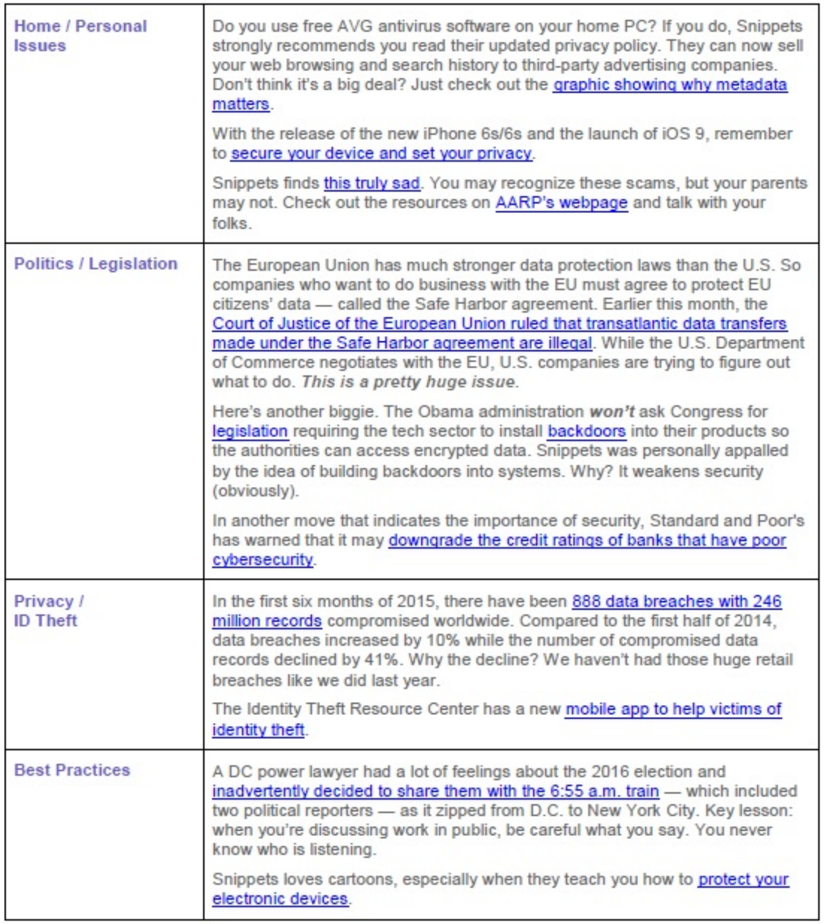
Direct inquiries & correspondence to:
securityawareness@your.organization



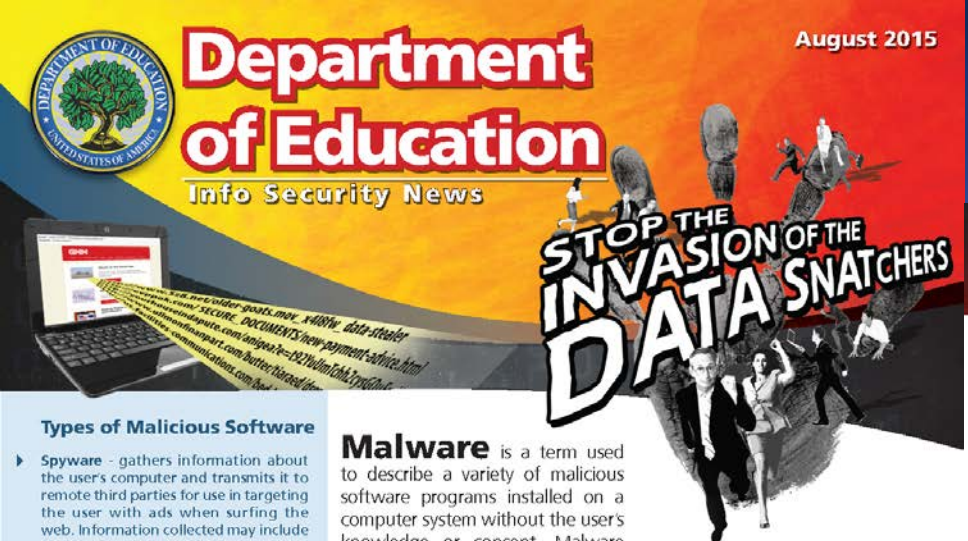
vantiv
Security Snippets

A monthly collection of security news — October 2015

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 calendars! 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-trapping and jackpotting. Be careful using unknown USB sticks. Here's one that sends 220 volts through the signal lines of the USB interface, frying 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 you do, Snippets strongly recommends you 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 graphic 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 truly sad. 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 authorities 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 888 data breaches with 246 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 6:55 a.m. train — 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 devices.



Department of Education
Info Security News

August 2015

STOP THE INVASION OF THE DATA SNATCHERS

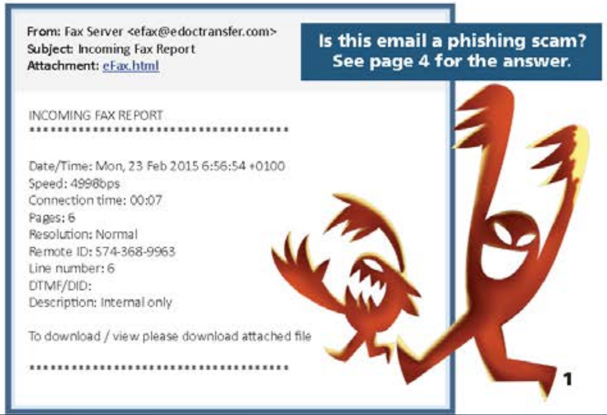
older-goats.mov_x4l6fw_data-stealer
SECURE_DOCUMENTS/new-payment-advice.html
anigea?e=t92YuUmIdhL2ygGhG
butterflaraed

Types of Malicious Software

- **Spyware** - gathers information about the user's computer and transmits it to remote third parties for use in targeting the user with ads when surfing the web. Information collected may include browser type and version, operating system information, websites visited, and IP address.
- **Virus** - infects files or the system areas of a computer's hard drive and are spread through user interaction such as opening an email attachment, clicking a malicious link, or visiting a malicious web page. Once installed, viruses damage or destroy files, sensitive systems and information, send data to remote attackers, and attack other systems.
- **Worm** - spreads from computer to computer without human interaction. These programs propogate viruses, take up valuable memory and network bandwidth, and may allow remote attackers to gain access to infected computers.
- **Trojan Horse** - used to hide a virus or other potentially damaging program. A Trojan horse can be a program that purports to do one action when, in fact, it is performing a malicious action on your computer. Trojan horses can be included in software that you download for free or as attachments in email messages.
- **Ransomware** - extorts money from users by disabling important computer system functionality or encrypting files on the victim's computer as well as on any connected network drives, USB drives, external hard drives, or network file shares.

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 spear 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.



From: Fax Server <efax@edoctransfer.com>
Subject: Incoming Fax Report
Attachment: eFax.html

INCOMING FAX REPORT
****

Date/Time: Mon, 23 Feb 2015 6:56:54 +0100
Speed: 4996bps
Connection time: 00:07
Pages: 6
Resolution: Normal
Remote ID: 574-368-9963
Line number: 6
DTMF/DID:
Description: Internal only

To download / view please download attached file

****

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

Encrypting SPII Using WinZip

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

To compress and encrypt file(s):

1. Browse to and select the files you want to encrypt.
2. Right-click on the file(s), 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 the **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 (0-9), 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.

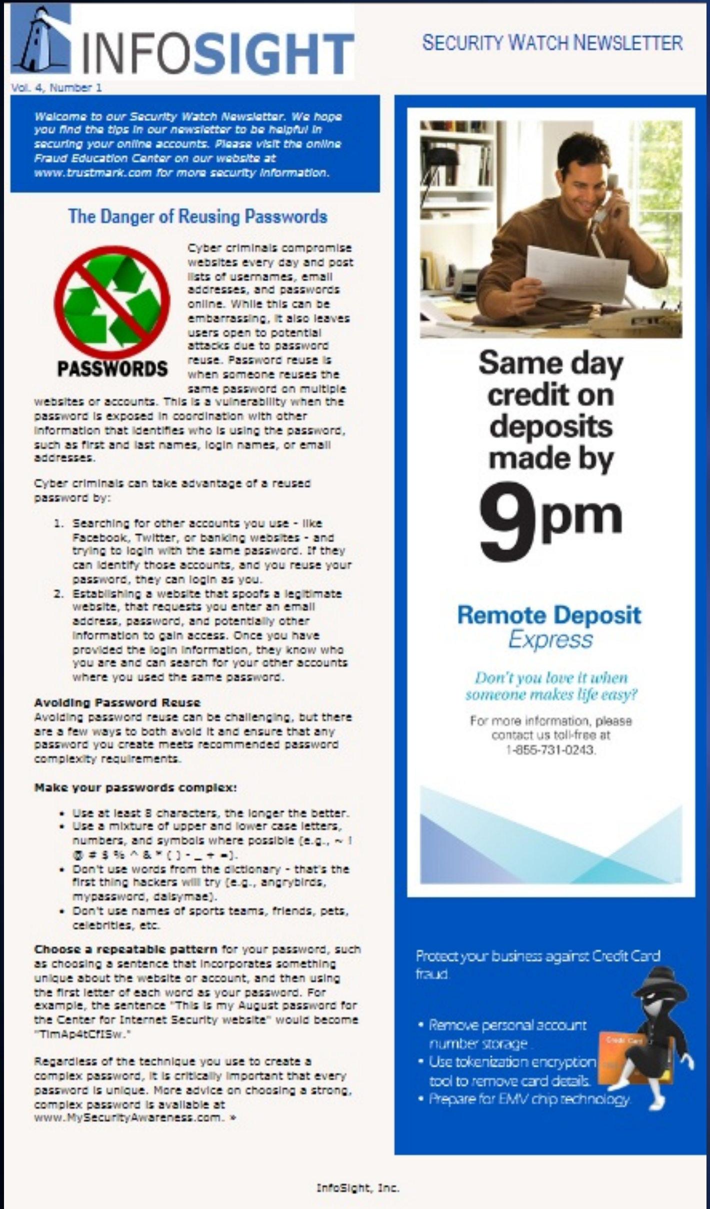
Malvertising

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 ciminals with many entry points along the way to inject 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.



INFOSIGHT

SECURITY WATCH NEWSLETTER

Vol. 4, Number 1

Welcome to our Security Watch Newsletter. We hope you find the tips in our newsletter to be helpful in securing your online accounts. Please visit the online Fraud Education Center on our website at www.trustmark.com for more security information.

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 password reuse. Password reuse is when someone reuses the same password on multiple websites or accounts. This is a vulnerability when the password is exposed in coordination with other information that identifies who is using the password, such as first and last names, login names, or email addresses.

Cyber criminals can take advantage of a reused password by:

1. Searching for other accounts you use - like Facebook, Twitter, or banking websites - and trying to login with the same password. If they can identify those accounts, and you reuse your password, they can login as you.
2. Establishing a website that spoofs a legitimate website, that requests you enter an email address, password, and potentially other information to gain access. Once you have provided the login information, they know who you are and can search for your other accounts where you used the same password.

Avoiding Password Reuse
Avoiding password reuse can be challenging, but there are a few ways to both avoid it and ensure that any password you create meets recommended password complexity requirements.

Make your passwords complex:

- Use at least 8 characters, the longer the better.
- Use a mixture of upper and lower case letters, numbers, and symbols where possible (e.g., ~ ! @ # $ % ^ & * ( ) - _ + =).
- Don't use words from the dictionary - that's the first thing hackers will try (e.g., angrybirds, mypassword, daisymae).
- Don't use names of sports teams, friends, pets, celebrities, etc.

Choose a repeatable pattern for your password, such as choosing a sentence that incorporates something unique about the website or account, and then using the first letter of each word as your password. For example, the sentence "This is my August password for the Center for Internet Security website" would become "TimAp4tCfISw."

Regardless of the technique you use to create a complex password, it is critically important that every password is unique. More advice on choosing a strong, complex password is available at www.MySecurityAwareness.com. »

Same day credit on deposits made by 9pm

Remote Deposit *Express*

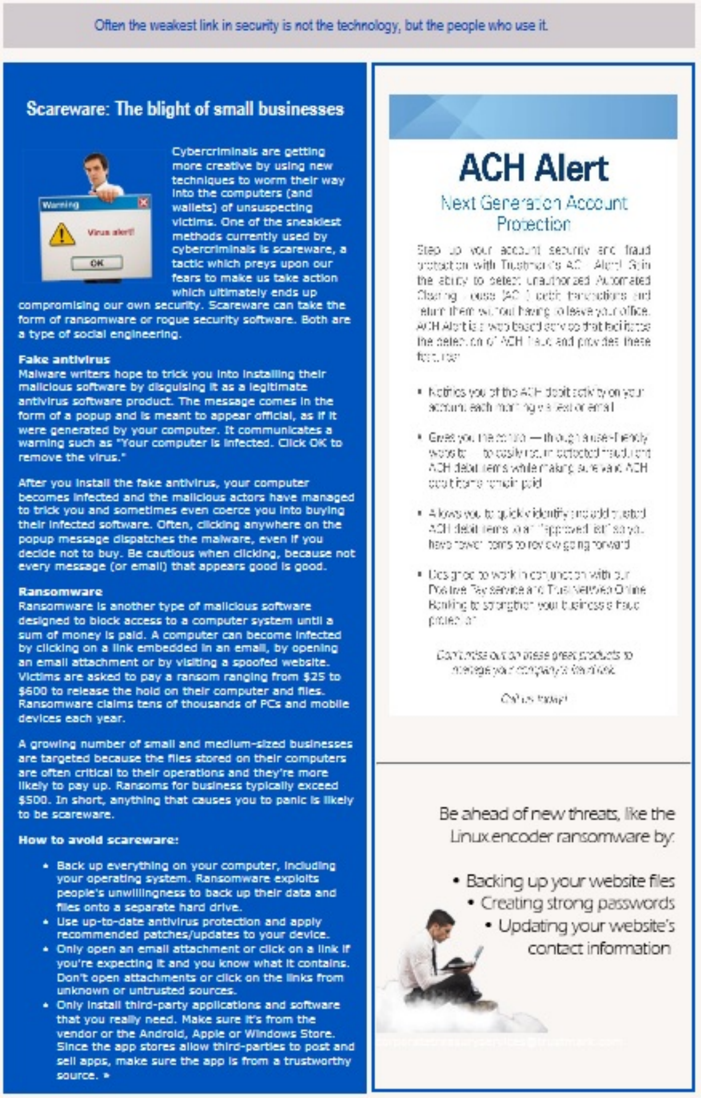
Don't you love it when someone makes life easy?

For more information, please contact us toll-free at 1-855-731-0243.

Protect your business against Credit Card fraud

- Remove personal account number storage
- Use tokenization encryption tool to remove card details.
- Prepare for EMV chip technology

InfoSight, Inc.



Often the weakest link in security is not the technology, but the people who use it.

Scareware: The blight of small businesses

Cybercriminals are getting more creative by using new techniques to worm their way into the computers (and wallets) of unsuspecting victims. One of the sneakiest methods currently used by cybercriminals is scareware, a tactic which preys upon our fears to make us take action which ultimately ends up compromising our own security. Scareware can take the form of ransomware or rogue security software. Both are a type of social engineering.

Fake antivirus
Malware writers hope to trick you into installing their malicious software by disguising it as a legitimate antivirus software product. The message comes in the form of a popup and is meant to appear official, as if it were generated by your computer. It communicates a warning such as "Your computer is infected. Click OK to remove the virus."

After you install the fake antivirus, your computer becomes infected and the malicious actors have managed to trick you and sometimes even coerce you into buying their infected software. Often, clicking anywhere on the popup message dispatches the malware, even if you decide not to buy. Be cautious when clicking, because not every message (or email) that appears good is good.

Ransomware
Ransomware is another type of malicious software designed to block access to a computer system until a sum of money is paid. A computer can become infected by clicking on a link embedded in an email, by opening an email attachment or by visiting a spoofed website. Victims are asked to pay a ransom ranging from $25 to $600 to release the hold on their computer and files. Ransomware claims tens of thousands of PCs and mobile devices each year.

A growing number of small and medium-sized businesses are targeted because the files stored on their computers are often critical to their operations and they're more likely to pay up. Ransoms for business typically exceed $500. In short, anything that causes you to panic is likely to be scareware.

How to avoid scareware:

- Back up everything on your computer, including your operating system. Ransomware exploits people's unwillingness to back up their data and files onto a separate hard drive.
- Use up-to-date antivirus protection and apply recommended patches/updates to your device.
- Only open an email attachment or click on a link if you're expecting it and you know what it contains. Don't open attachments or click on the links from unknown or untrusted sources.
- Only install third-party applications and software that you really need. Make sure it's from the vendor or the Android, Apple or Windows Store. Since the app stores allow third-parties to post and sell apps, make sure the app is from a trustworthy source. »

ACH Alert

Next Generation Account Protection

Step up your account security and fraud protection with Trustmark's ACH Alert! Gain the ability to detect unauthorized Automated Clearing House (ACH) debit transactions and return them without having to leave your office. ACH Alert is a web based service that facilitates the detection of ACH fraud and provides these features:

- Notifies you of the ACH debit activity on your account each morning via text or email
- Gives you the control — through a user-friendly website — to easily return detected fraudulent ACH debit items while making sure valid ACH debit items remain paid
- Allows you to quickly identify and add trusted ACH debit items to an "approved list" so you have fewer items to review going forward
- Designed to work in conjunction with our Positive Pay service and TrustNetWeb Online Banking to strengthen your business's fraud protection

Don't miss out on these great products to manage your company's fraud risk.

Call us today!

Be ahead of new threats, like the Linux encoder ransomware by:

- Backing up your website files
- Creating strong passwords
- Updating your website's contact information

Newsletter Winner!

IHS Division of Information Security

Organization:

Indian Health Service, Office of Information Technology, Division of Information Security

Better New Security COOK BOOK

Fry a Better Phish

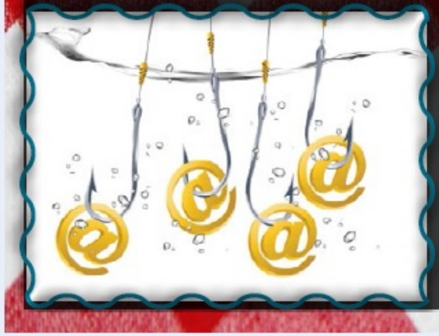
Best Phish Bait on the Market

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 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 unappetizing phishing campaign. While there is no magic solution for combatting 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!

National Cyber Security Awareness Month October 2015

OUR SHARED RESPONSIBILITY

Fry a Better Phish

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 irt@ihs.gov!!

If you receive a phishing attempt at work, contact local IT staff.
Or file a report at: https://disirf.ihs.gov

If you were tricked by a phishing email at home, file a report with the Federal Trade Commission: www.ftc.gov/Complaint

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 fake website asking you 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 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!!

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=Regfcjtqa08

Video 6:
https://vimeo.com/infosightinc/review/71762956/3a70dcbc50

Video Winner!

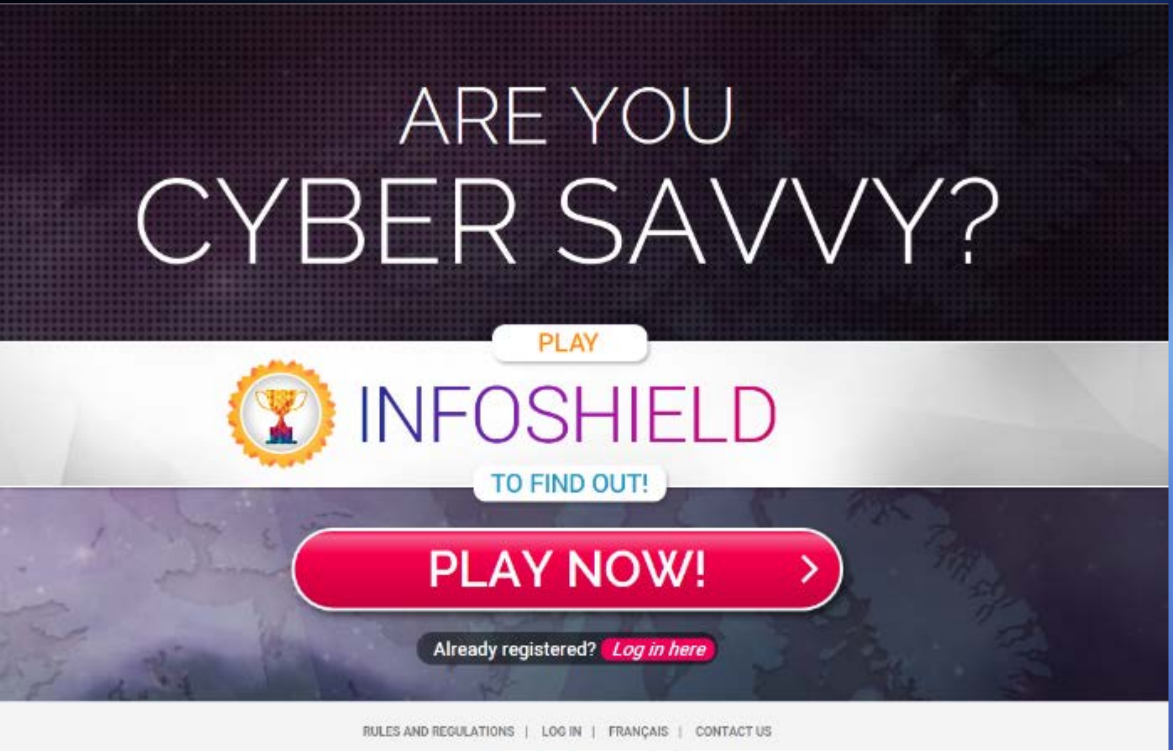
Cheryl Seaman &
Stephanie Erickson

Organization:

The National Institutes of Health

https://youtu.be/3hHnT1szO7c

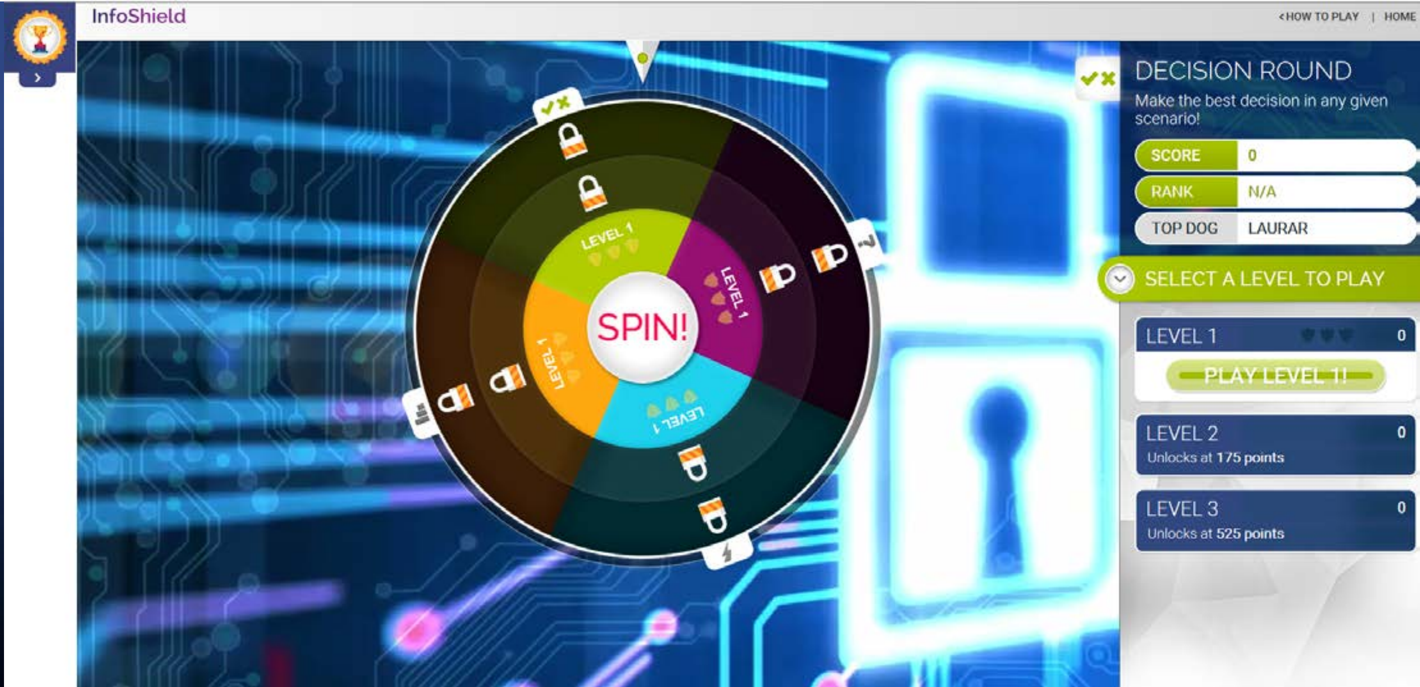
Training Entries (3)



ARE YOU
CYBER SAVVY?

PLAY INFOSHIELD TO FIND OUT!

PLAY NOW!
Already registered? Log in here
RULES AND REGULATIONS | LOG IN | FRANÇAIS | CONTACT US



InfoShield

DECISION ROUND

Make the best decision in any given scenario!

SCORE	0
RANK	N/A
TOP DOG	LAURAR

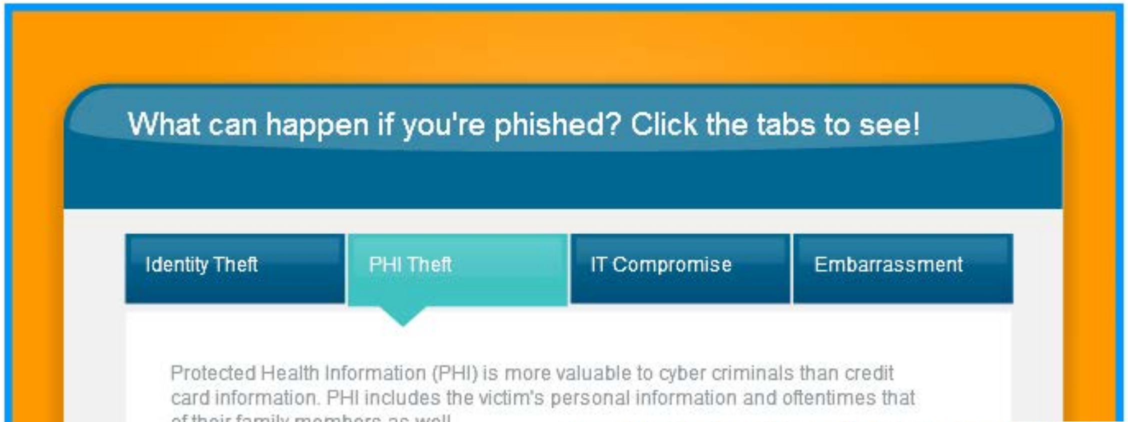
SELECT A LEVEL TO PLAY

LEVEL 1 0

LEVEL 2 0
Unlocks at 175 points

LEVEL 3 0
Unlocks at 525 points

Don't Take the Bait Interactive Activity

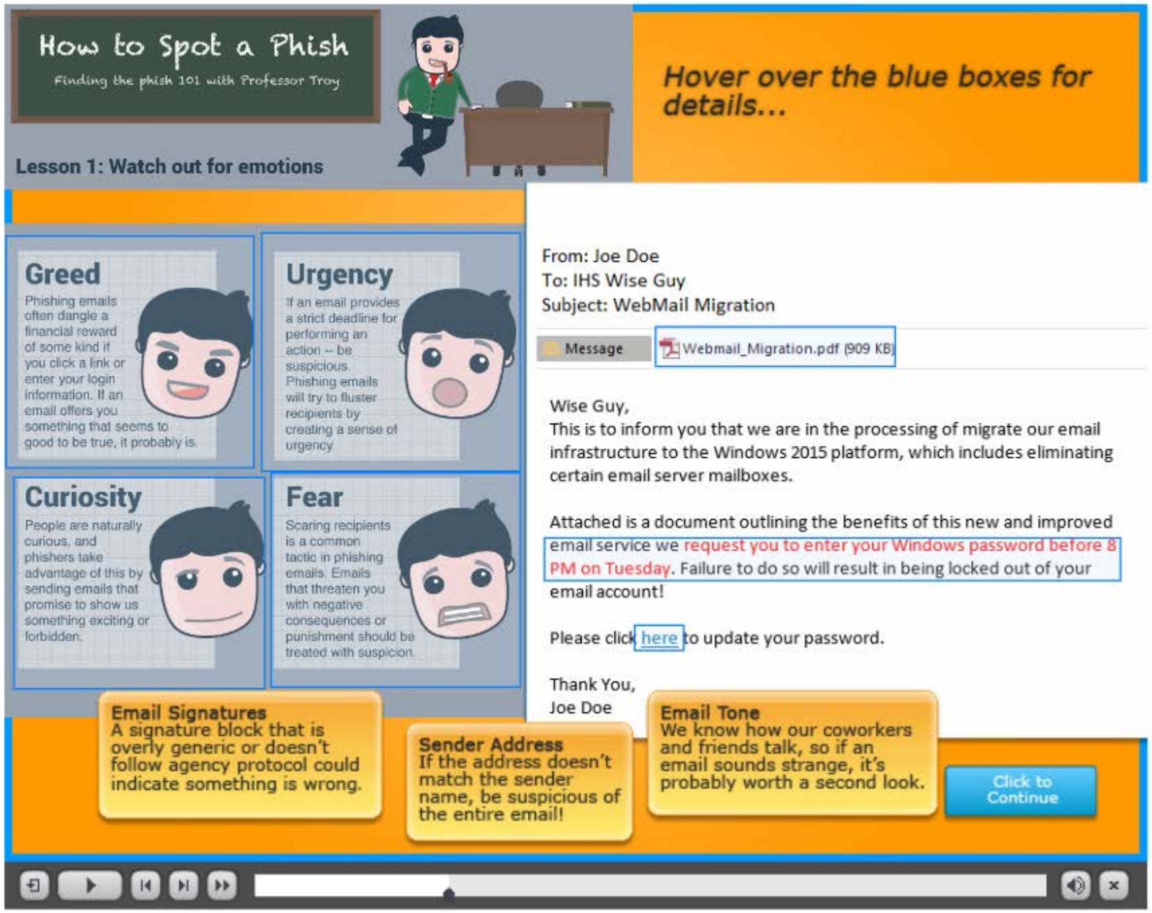


What can happen if you're phished? Click the tabs to see!

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

PHI thieves can file fraudulent reimburseme caps, change their medical history and diag

Don't Take the Bait Interactive Activity



Hover over the blue boxes for details...

Lesson 1: Watch out for emotions

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

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

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

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

From: Joe Doe
To: IHS Wise Guy
Subject: WebMail Migration

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

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

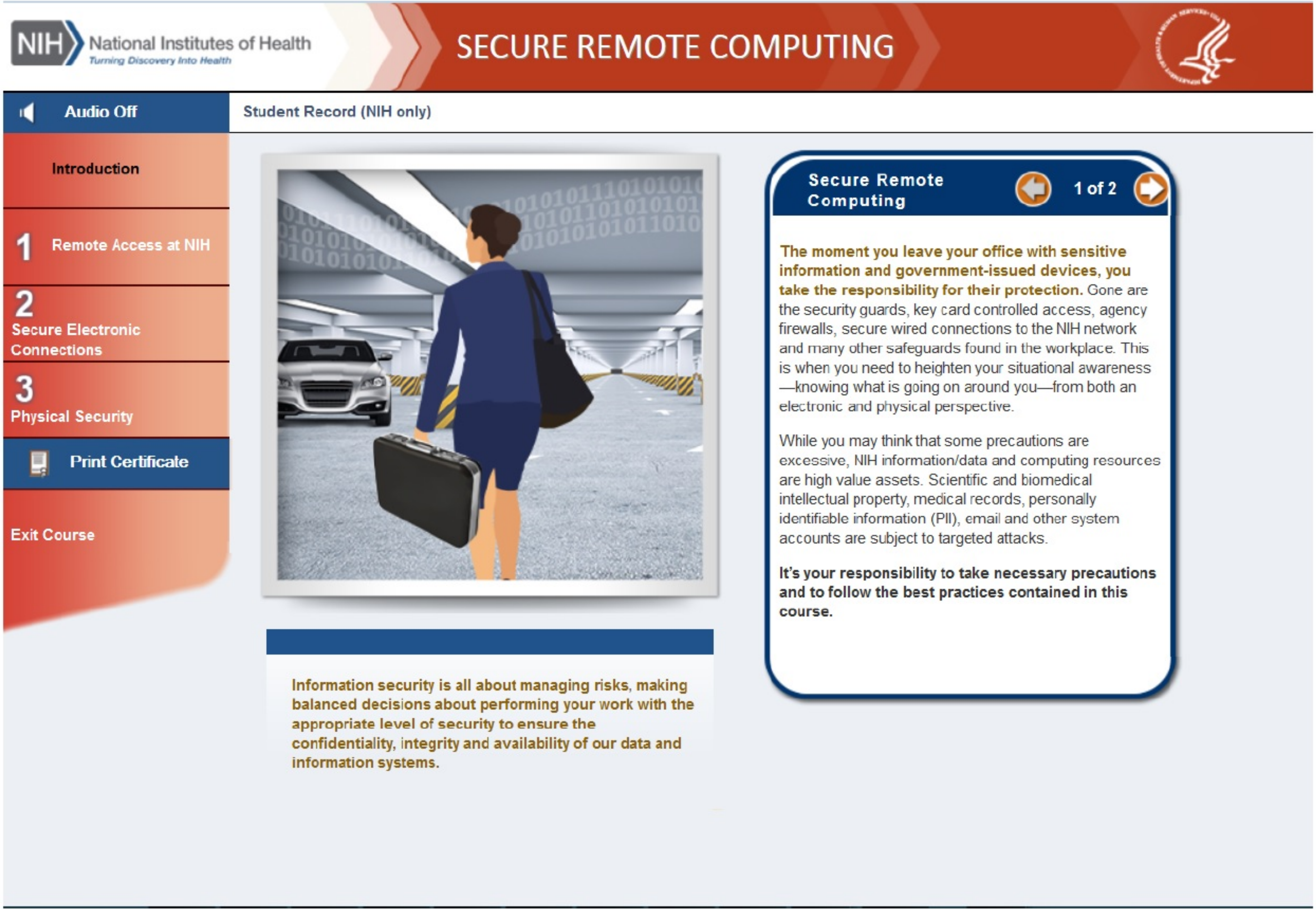
Please click here to update your password.

Thank You,
Joe Doe

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

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

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


NIH National Institutes of Health
Turning Discovery Into Health
Audio Off
Student Record (NIH only)
Introduction
1 Remote Access at NIH
2 Secure Electronic Connections
3 Physical Security
Print Certificate
Exit Course
1 of 2

SECURE REMOTE COMPUTING

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.

Secure Remote Computing

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.

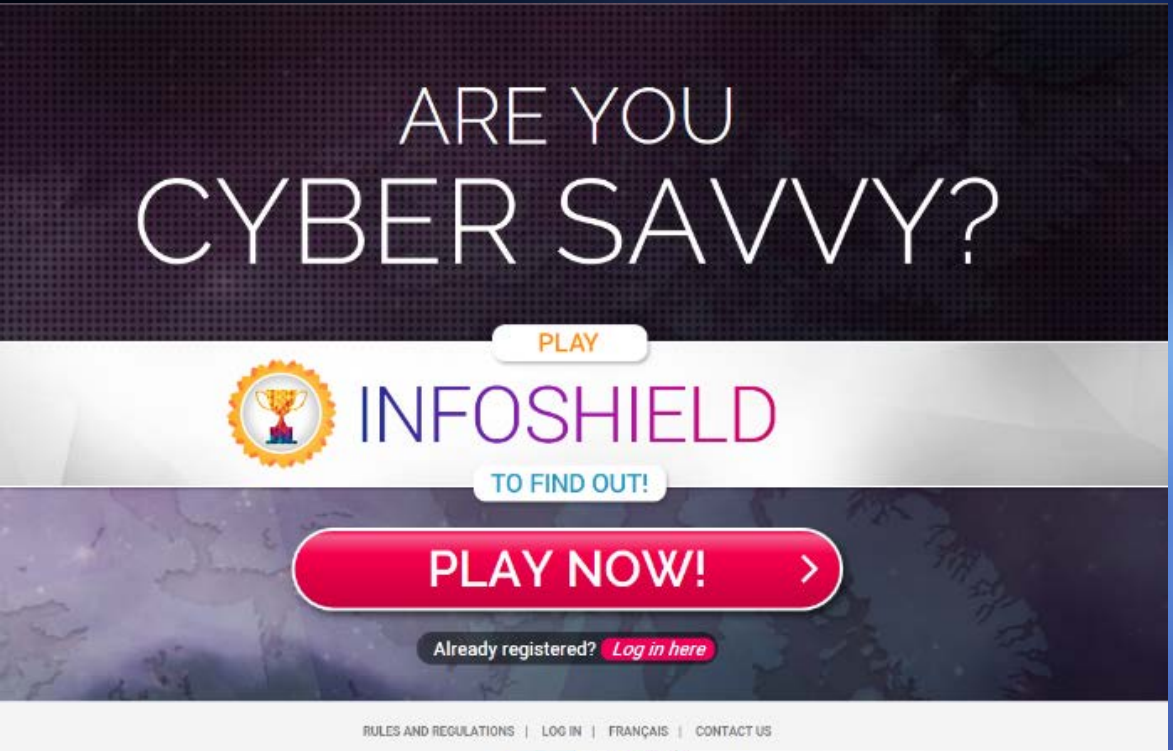
It's your responsibility to take necessary precautions and to follow the best practices contained in this course.

Training Winner!

The ESDC Security Training and Awareness Program Team

Organization:

Employment and Social Development Canada (ESDC)



ARE YOU

CYBER SAVVY?

PLAY

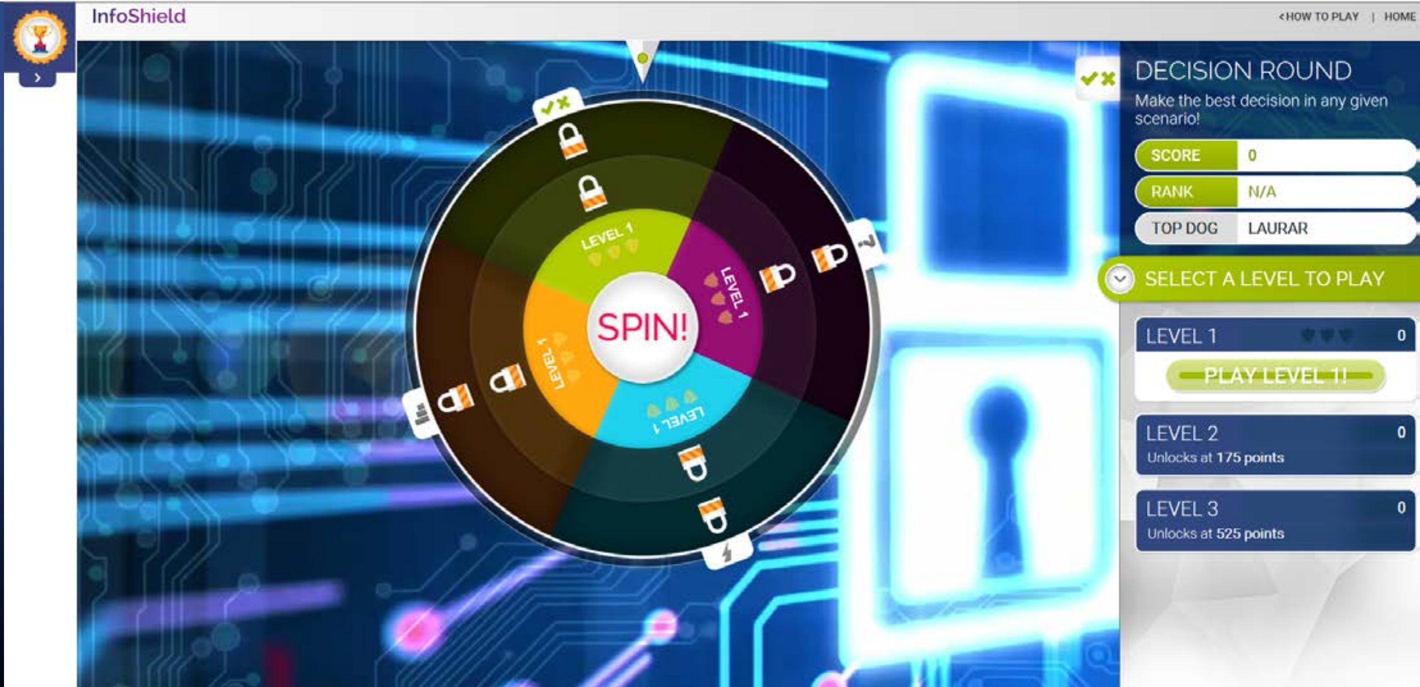
INFOSHIELD

TO FIND OUT!

PLAY NOW! ›

Already registered? *Log in here*

RULES AND REGULATIONS | LOG IN | FRANÇAIS | CONTACT US



InfoShield

‹ HOW TO PLAY | HOME

DECISION ROUND

Make the best decision in any given scenario!

SCORE	0
RANK	N/A
TOP DOG	LAURAR

SELECT A LEVEL TO PLAY

LEVEL 1 0

PLAY LEVEL 1!

LEVEL 2 0

Unlocks at 175 points

LEVEL 3 0

Unlocks at 525 points

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!