

FISSEA

Security Awareness, Training, and Education

Contest

Gretchen Morris, CISSP
FISSEA Working Group Member

March 2017

Contest

Categories

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

Judges

- ⊕ Not affiliated with any of the groups that submitted entries
- ⊕ From various positions and industries

Website Entries (4)

“Keep Me Safe Online” Page

This page features articles about keeping safe online which include:

- Passwords
- Free Downloads and Tools
- Banking, Shopping & Payments
- Social Networking
- Scams & Spams

The screenshot displays the MySECURITY Awareness.com website. At the top, the logo and navigation menu are visible. The main content area is titled "Keep Me Safe Online" and is divided into several sub-sections: "Malware", "Free Downloads", "Banking/Shopping/Payments", "Social Networking", and "Spam & Scams".

The "Malware" section features four articles:

- MALWARE**: Understand the origins of malware and how to avoid becoming infected so you can peruse the Internet with more confidence.
- Keep Your Mobile Device Secure**: Learn the steps you need to take to protect and keep your mobile device secure from malware.
- Beware of Spyware**: Protect your computer from spyware and viruses that can cause it to run slowly or give fraudsters access to your personal information.
- What is it? Why Should I Care? MALWARE**: Learn what malware is, how it can gain access to your computer, and what you can do to protect yourself.

The "Free Downloads" section features three articles:

- Protect yourself from Malware**: Here are a few ways to protect yourself from malware.
- Free Firewall Test**: Take advantage of this FREE firewall test to make sure you are not leaving yourself open to attack!
- VIPRE**: The VIPRE Rescue is designed to disinfect a system that's so infected that a user can't install VIPRE.

The "Social Networking" section features one article:

- FREE ANTI-VIRUS SCAN**: Free Anti-Virus Scan by Kaspersky Lab

The "Spam & Scams" section features one article:

- TRY NEW Norton Security Scan**: Download and install Norton Security Scan

HHS Intranet Home



Each month the HHS intranet features a CyberCARE rotating banner that links to a cybersecurity topic. Every other 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.

Home Page Banner for March 2016



PHI for Sale?

Is your fitness tracker a threat to your privacy? When it comes to fitness trackers and other wearable technology, do the risks outweigh the benefits? Is this like the discovery of electricity: illuminating when used properly, but potentially dangerous and deadly when mismanaged? [Read more...](#)

Strategic Themes

We have written monthly themes around privacy, highlighting fitness trackers and the info they share,

I'd Like to Buy Your PHI



Raise your hand if you wear a fitness tracker!

No, wait, you don't need to raise your hand. We can see it there on your wrist. *Nice band.*

Day in and day out, fitness trackers provide a constant reminder to stay motivated, keep moving, and challenge your friends to make sure they stay active, too. At night, these wonderful trackers can tell you how much actual sleep you're getting versus the number of times you're restless.

...a parent's guide to apps, translating teen-speak and helping parents understand some of the cybersecurity risks present in popular apps.

Allow Us to Translate

Do you "speak teen?" It's okay if you don't; I stopped trying to be cool years ago. While I might not understand the lingo, I know that kids are using apps on their phones I have never heard of, and I want to understand the cyber-risk they face.

We all know that it takes a village, and the CyberCARE team wants to be part of your village. We are here to translate teen for you, and

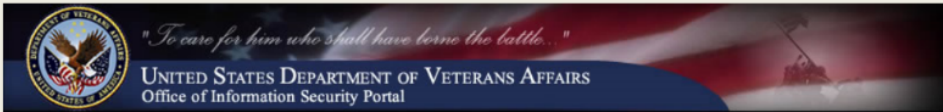


... and articles with a fairy-tale theme exposing some nefarious social engineering schemes, like how your LinkedIn profile could be helping hackers infiltrate the network

The Fairest LinkedIn Profile of Them All How your LinkedIn profile is helping the hackers

Once upon a time, a graphic designer got an email full of praise, telling her she was the finest in the land and asking for her advice. Pleased and flattered, the designer opened the attachment to the email, not realizing it held a virus. Her computer was hacked, and her network had been infiltrated. This is social engineering.





- SASA IAM Policy Alignment
 - Publications
 - FICAM Compliance Checklist
 - IAM Organizations
 - Websites of Interest
 - Latest Security Updates
 - SME Corner / FAQ
 - Contact Us
 - Site Changes Log
 - Surveys
-
- Recycle Bin
 - All Site Content



About IAM Security Center

The vision of the IAM Security Center is to provide the VA intranet user community with a single source of information pertaining to Federal and departmental security relating to Identity and Access Management (IAM). Particular emphasis is on Federal and departmental directives, policies and handbooks, other VA IAM related organizations, and specific information pertaining to VA application system Project Managers, Chief Information Officers, and Information Security Officers.

Locate Your Information Security Officer

Locate Your Privacy Officer

Locate Your Facility

The Security Scoop

Read Current Issue Now

Subscribe

for the latest security updates

Missed an issue?

View Archives

Did You Find What You Were Looking For?

Take this short survey to help us get to know you, so we can better serve you.

FICAM Compliance Checklist

The FICAM Compliance Checklist is a tool designed to help ISOs (or designees) ensure services, systems, and applications are meeting the Access Control and Identification and Authentication FISMA controls through the use of VA's FICAM Services.

SASA IAM Policy Alignment

See this image for policies that map to Identity and Access Management Services.

IAM Organization

Check out the Office of Information Security and Office of Cyber Security Policy and Compliance organization charts to see where we fit in.

Publications

Find Memorandum, Directives, Special Publications, and Handbooks that are FICAM related here.

Websites of Interest

Look here for links to related offices and programs in VA.

- [Latest Security Updates](#)
- [SME Corner & FAQs](#)
- [Contact Us](#)
- [How Are We Doing?](#)
- [Site Changes Log](#)
- [Get Alerts on Site Changes](#)

Security Video's Page

Security



Date: March 2, 2016

Telephone Security: It's in your hands

Passport employees can [view the video here](#)
 (2:59) A look at the implications of telephone security and how to protect themselves.

↓ [Transcript](#) (DOCX, 36 KB)



Date: February 2, 2015

Put a Halt to Phishing

Passport employees can [view the video here](#)
 (2:52) A look at the implications of phishing and how they do not get "hooked".

↓ [Transcript](#) (DOCX, 29 KB)



Date: January 29, 2015

Physical Security: It starts with you

Passport employees can [view the video here](#)
 (3:27) Check out the latest video from physical security and what employees can do.

↓ [Transcript](#) (DOCX, 24.7 KB)

Reporting Security Incidents

Consistent Use of Icons

Reporting Security Incidents

Security incidents are...

incidents or situations that affect, or have the potential to affect, the department, its assets and/or its employees.

Reporting a Security Incident... Knowing what to do

1. Employee

- Take necessary measures to protect individuals, information and assets
- Call Emergency Services / 911 if necessary and advise your Team Leader / Manager immediately *
- Report the incident to your Team Leader / Manager as soon as possible

2. Team Leader / Manager

- Report the incident immediately to your [Regional Security Office \(RSO\)](#)
- Call Emergency Services / 911 if necessary and advise your RSO immediately *
- Complete and send the [Security Incident Report \(ADM 3061\)](#) (*opens new window*) form to your RSO as soon as possible

* Only Managers with delegated authority can disclose personal information to the police

As needed, consult the [How to Report Security Incidents for ESDC Employees](#) (PDF, 22 KB) decision making diagram to quickly determine the course of action.

Refer to the table below for more information and guidance on the types of Security Incidents:

Types of Security Incidents

 Violence or threats of violence Threats or acts of violence	 Involving information	 Loss or theft of public assets and public goods
 User Compromise	 Denial of Service Attack	 Malicious Code
 Loss, Damage or Theft of Departmental Device	 Phishing Attack	 Spam

Website Winner!

The Security Training and Awareness Program Team

Organization:

**Employment and Social
Development Canada (ESDC)**

Security Video's Page

Security



Date: March 2, 2016

Telephone Security: It's in

Passport employees can [view the video here](#)

(2:59) A look at the implications of telephone security and how to protect themselves.

↓ [Transcript](#) (DOCX, 36 KB)



Date: February 2, 2015

Put a Halt to Phishing

Passport employees can [view the video here](#)

(2:52) A look at the implications of phishing and how they do not get "hooked".

↓ [Transcript](#) (DOCX, 29 KB)



Date: January 29, 2015

Physical Security: It starts

Passport employees can [view the video here](#)

(3:27) Check out the latest video from physical security and what employees can do.

↓ [Transcript](#) (DOCX, 24.7 KB)

Reporting Security Incidents

Consistent Use of Icons

Reporting Security Incidents

Security incidents are...

incidents or situations that affect, or have the potential to affect, the department, its assets and/or its employees.

Reporting a Security Incident... Knowing what to do

1. Employee

- Take necessary measures to protect individuals, information and assets
- Call Emergency Services / 911 if necessary and advise your Team Leader / Manager immediately *
- Report the incident to your Team Leader / Manager as soon as possible

2. Team Leader / Manager

- Report the incident immediately to your [Regional Security Office \(RSO\)](#)
- Call Emergency Services / 911 if necessary and advise your RSO immediately *
- Complete and send the [Security Incident Report \(ADM 3061\)](#) (*opens new window*) form to your RSO as soon as possible

* Only Managers with delegated authority can disclose personal information to the police

As needed, consult the [How to Report Security Incidents for ESDC Employees](#) (PDF, 22 KB) decision making diagram to quickly determine the course of action.

Refer to the table below for more information and guidance on the types of Security Incidents:

Types of Security Incidents

 Violence or threats of violence Threats or acts of violence	 Involving information	 Loss or theft of public assets and public goods
 User Compromise	 Denial of Service Attack	 Malicious Code
 Loss, Damage or Theft of Departmental Device	 Phishing Attack	 Spam

Motivational Item Entries (3)

1st Place Award



PHISHING

IT WAS IN THE INBOX

A tale of intrigue, phishing, and emotions...

Phishing attacks use emotional triggers to bait you into doing things you shouldn't.

To convince you to click on a link, download an attachment, or surrender sensitive information, these emails play on emotions.

Phishing emails may rush you into action, so you don't have time to make a good decision



If you receive an email that evokes strong emotions, **BE CAUTIOUS!**

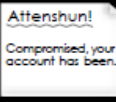
Look out for other characteristics that indicate an email may be phishing:



It's from an unknown sender



The email is unexpected or unsolicited



It contains grammar & spelling errors



Resource Card



From: Oskar Wolf <oskar.acme@bigbadphish.com>
To: You@yourorganization.com
Date: Saturday, May 21, 4:00 am
Subject: Urgent - Account will be deactivated

Generic greeting/salutation: Dear Sir/Madam.
Subject is missing, makes dramatic claims, or doesn't match the message content: It has come to our attenshun that your account may have been compromised.
Typos, grammatical errors, or may seem like it was translated using inferior software: Attenshun!
Hovering over the link reveals an unexpected or changed URL: To prevent the deactivation of your account, please [click here](#) within 24 hours to log in and reset your password.
False sense of urgency: Thank you,
Asks for sensitive data (e.g. login or payment information), or asks you to take action to avoid a negative consequence or to gain something of value: IT Support Desk
Sender claims to be a person/organization of authority, and may include fake copyright notices, antivirus icons, etc.:

If something doesn't seem right with an email, report it immediately to the NIH Information Security Program.



B
E
V
E
R
A
G
E



S
T
I
R
S

Motivational Item Winner!

K Rudolph

Organization:
Native Intelligence, Inc.

Did you
log off?

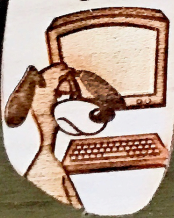


Did you
log off?



Did you
log off?

Did you
log off?



Did you
log off?



Poster Entries (10)

**The road to security is
constant and never ending**

Keep our Veteran's information secure

BE A CYBER SUPER HERO!



Report suspicious activity to
CIRT@state.gov



Building Resilience @ IHS



IHS HOSPITAL

Cybersecurity Tip

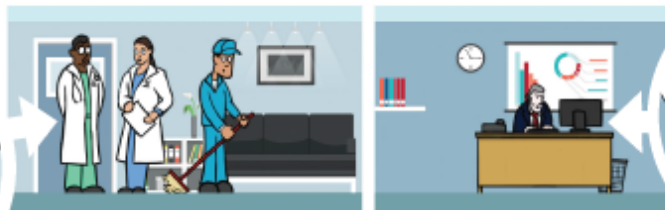
IHS facilities can be particularly vulnerable to cyber and physical intrusions because we have patient data, which can be a lucrative target for criminals. As IHS employees, we are responsible for protecting patient and personal information. Report security incidents, phishing attempts, and other security violations to the IHS Cybersecurity Incident Response Team at csirt@ihs.gov.

The link between cyber and physical security is essential to the resiliency of critical infrastructure. Resilience of essential systems and assets, from power grids to healthcare systems, is vital to our national security, economy, and public health and safety. This week's bulletin looks at the cyber and physical security of IHS healthcare facilities.

In Common Areas, Use Common Sense.

- Be discrete discussing patients in public places like elevators, public hallways, or the cafeteria.
- Ask unaccompanied visitors where they are going and if they have a visitor ID. Someone who is supposed to be there won't mind the questions.
- Never hold a door to a secured area open for anyone who doesn't have appropriate ID.

The lab results came back...



Um... sure, I guess. My password is...



In an Oooupled Office, Be Vigilant Against Scams.

- Don't open or respond to suspicious emails.
- Don't open attachments or downloads without confirming they're legitimate.
- Verify a link is legitimate before clicking on it. Hover over it with the mouse to reveal the web address.
- Never forward spam or chain letters, and beware of phishing attempts.
- Be cautious of telephone scammers claiming to be tech support. Don't give them your password or install their software.
- Never trust unsolicited phone calls or give remote access to any individual unless the identity of that person can be verified.

In a Vacant Office, Consider the Space Public.

- Always remove your PIV card and lock your computer when you walk away.
- Don't leave sensitive papers in trashcans. Dispose of them properly (like by shredding them).
- Secure your portable devices, even while in the office. It takes only a second for someone to snatch a laptop and the IHS data on it.
- Remember that other people (like cleaners and maintenance workers) access open work-spaces outside normal hours.



Patient File (confidential)
Surgery Schedules



In the Patient's Room, Protect Patient Data.

- Protecting patient data is critical because hacking health records could lead to altered drug dosages, tampered treatments, or other devastating scenarios.
- Malicious actors could also use Protected Health information to gain access to medical care or prescription drugs for fraudulent use or to resell on the black market.

In Patient Registration, Be Aware.

- Position your computer screen so that others can't see it.
- Remove documents promptly from fax and copy machines.

Test Screening
Patient Results
Cover Sheet



The doctor can see you now about your weird Foot Fungus!



In the Waiting Room, Be Discrete.

- Avoid conversations about one patient in front of other patients or their visitors.
- Lower voices when discussing patient information in person or over the phone.
- Report suspicious people or activity to the security guard, supervisor, or management official.



DON'T LET PHISHERS HOOK YOUR ACCOUNT!

PROTECT YOURSELF

- >> **Never respond** to any email with personal information. If you need to send sensitive information over the internet, encrypt the file first.
- >> **Be suspicious** of all email messages, especially those with attachments you are not expecting, or from companies you do not do business with.
- >> **Do not click** on links in emails. Type website addresses directly into your browser and contact the business directly by calling to speak with a representative.
- >> If you'd like help protecting your business from phishing attacks contact **info@infosightinc.com**

Anatomy of a phishing email

Sender name and domain is a spoof of a known brand.

Vague, suspicious, and urgent subject line (used as a scare tactic).

Logo of the trusted, known brand is used.

Use of generic greeting.

Use of bad grammar.

Link to a fake website (hovering over the link reveals suspicious URL).

Sense of urgency is expressed.

Copyright, or other way of displaying validity.

From: John Smith <johnsmith@TrustedBankSupport.com>
Sent: Wednesday, November 12, 2016 at 8:38 AM
To: Your Name <youremail@youremailprovider.com>
Subject: Your account has been locked



How to restore your Trusted Bank account.

Dear Valued Member,
To restore your account, you'll need to log in your account.

It's easy:

1. Click the link below to open secure browser window.
2. Confirm your log in of the account, and then follow the instructions.

[Log in your account now](#)

Thank you for your prompt attention to this matter and for using Trusted Bank.

Trusted Bank Member Services Team

©Trusted Bank 2016

THINK OF YOUR **PASSWORD** as a **PASSPORT**



- Keep it **Secure**
- Handle it with **Care**
- No one should use it **BUT YOU**

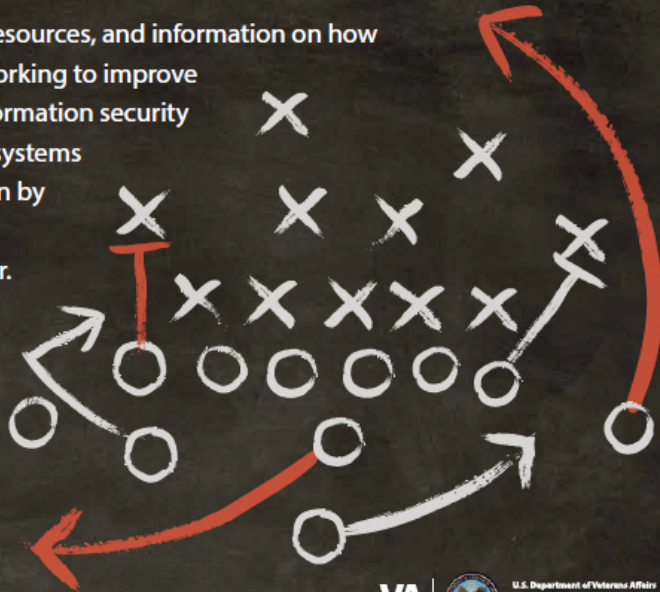
IAM

The Best Offense is a

SECURE DEFENSE

Information Security is top priority at VA

Access tools, resources, and information on how SASA IAM is working to improve the overall information security posture of VA systems and application by visiting the Security Center.



vaww.portal2.va.gov/sites/infosecurity/IAM

VA



U.S. Department of Veterans Affairs
Office of Information and Technology
Cyber Security

IAM

The Best Offense is a

SECURE DEFENSE

The playbook for the SASA IAM Team keeps VA Secure.

The office of Security Architecture and Software Assurance (SASA) Identity and Access Management (IAM) office ensures VA's FICAM services are in compliance with FISMA requirements, and that those FICAM services are being used throughout the VA in fulfilling cybersecurity controls. To learn more visit:

vaww.portal2.va.gov/sites/infosecurity/IAM

VA



U.S. Department of Veterans Affairs
Office of Information and Technology
Cyber Security

PHISHING



A tale of intrigue, phishing, and emotions...

IT WAS IN MY INBOX

Phishing attacks use emotional triggers to bait you into doing things you shouldn't.

To convince you to click on a link, download an attachment, or surrender sensitive information, these emails play on emotions.

Phishing emails may rush you into action, so you don't have time to make a good decision



Curiosity



Greed



Fear



Urgency



Others will tempt you with a reward or prize for your hard work.

Some phishing emails will threaten, scare, or coerce you into taking action.

If you receive an email that evokes strong emotions, **BE CAUTIOUS!**

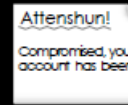
Look out for other characteristics that indicate an email may be phishing:



It's from an unknown sender



The email is unexpected or unsolicited



It contains grammar & spelling errors



A golden retriever is sitting on a sandy beach, looking towards the right. In the background, the ocean waves are visible under a sunset sky with orange and blue hues. A glass bottle with a cork is lying on the sand in front of the dog. A tag is attached to the bottle with a string, and the tag has the text "Free bones!" written on it.

**Unexpected
message?**

© 2017 Native Intelligence, Inc.

Be careful with attachments.

Fry the Phishers



Don't respond to links
on **unsolicited** emails.

Protect your passwords and
don't reveal them to anyone.

Don't open **attachments**
from unsolicited emails.

REPORT PHISHING AND SOCIAL ENGINEERING ATTEMPTS:

OFFICE OF THE CHIEF INFORMATION OFFICER
SYSTEMS SUPPORT DIVISION CYBERSECURITY BRANCH
INFORMATION.ASSURANCE@MARSHALLCENTER.ORG

IDENTITY
THEFT

BE ALERT
STAY SAFE ONLINE

PERSONALLY IDENTIFIABLE INFORMATION (PII) STOLEN



STOP-THINK-CONNECT

Learn best practices to stay safe and secure online at: <https://www.stopthinkconnect.org/>

Poster Winner!

**K Rudolph, G. Mark Hardy,
Niomi Rosenberg, Andrew Ellis,
John Ippolito, & Sam Carter**

**Organization:
Native Intelligence, Inc.**

A golden retriever is sitting on a sandy beach, looking towards the right. In the background, the ocean waves are breaking under a dramatic sunset sky with orange, yellow, and blue hues. A glass bottle with a cork is lying on the sand in front of the dog. A tag is attached to the bottle with a string, and the tag has the text "Free bones!" written on it. The dog's expression is one of curiosity or concern.

**Unexpected
message?**

© 2017 Native Intelligence, Inc.

Be careful with attachments.

Newsletter Entries (5)

National Cybersecurity Awareness Month

National Cybersecurity
Awareness Month



OCTOBER 2016

WEEK 4

The Internet of Things

Each year, manufacturers think up new ways to connect mundane, physical objects to the digital world. From toys to thermostats, toasters to TVs, and even toothbrushes to toilets, we're connecting, monitoring, and managing everyday tasks online.

The Internet of Things (IoT) is a growing phenomenon forcing major changes in the way we operate in our daily lives. With our expanding footprint of interconnectivity comes an expanding surface area of vulnerabilities for hackers to exploit. Why would a hacker exploit your toothbrush, and why should you care?

Halloween Cyber Tricks?

Hacking IoT devices like toothbrushes or coffee makers may seem like a benign prank, but these vulnerabilities can put your and your loved ones' personal information and safety at risk!

- IoT devices have been hijacked in order to send spam or host illicit pornography.
- Personal information has been compromised by IoT devices like: the Samsung smart fridge that exposed email credentials; climate-control systems that resulted in the 2013 Target credit card breach; and even barbie dolls that were connected to smart phones.
- Hackers have demonstrated the deadly potential to take over IoT products like: automobile engine and break systems; medical devices like Wi-Fi enabled pacemakers and drug-infusion pumps; and Wi-Fi enabled sniper rifles.
- Information about daily lives gained from Internet connected thermostats and door locks can provide burglars valuable information about your habits.



NCSAM Tips of the Week!

- Consider first whether your toothbrush or toaster needs to be "smart." If it does, make sure to purchase the ones with built-in security, and let the other companies know why you won't buy their unsecured products.
- Change the default passwords and give each device a unique password. Look for encryption options, enable security features, and apply patches or "firmware" updates when recommended.
- Never connect IoT devices at work without IT approval, and limit the number of devices that connect to the Internet at home. Software is available to enable a group of smart devices within the home (like light bulbs and door locks) to communicate with each other rather than the Internet.

InfoSight's Security Watch Newsletter



Welcome to InfoSight's Security Watch Newsletter!

Everyday there seems to be a new online threat to pay attention to. Our goal is to educate individuals and business about being cyber aware, and provide you with a selection of tips, tools and resources to help everyone from falling victim to the many cyber threats we all face.

Phishing: Don't Get Hooked

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received an email with a similar message? It's a scam called "phishing" — A phishing email can look just like it comes from a financial institution, e-commerce site, government agency or any other service or business. It involves hackers and cyber-criminals who are looking to lure personal information from unsuspecting victims. It often urges users to act quickly, to collect personal & financial information or infect your machine with malware and viruses.

How Do You Avoid Being a Victim?

- Don't email personal or financial information. Email is NOT a secure method of transmitting personal

information. Before sending sensitive information over the Internet, check the security of the website. (Look for https://)

- Pay attention to the website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Contact the company using information provided on an account statement, not information provided in an email.
- Keep a clean machine. Install and maintain anti-virus software, firewalls, and email filters to reduce spam.

What to Do if You Think You are a Victim?

- Forward spam that is phishing for information to spam@uce.gov. Also alert



In this edition you will find:

1. Phishing: Don't Get Hooked
2. Online Privacy: What are you sharing?
3. Top Cyber Security Threats

the company being impersonated in the phishing email so they can be alert.

- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.
- File a report with the FBI's Internet Crime Complaint Center. (<http://www.ic3.gov>)

Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts.

Online Privacy: What are you sharing?

1. Never give out your full name, address, birth date, or any other personally identifiable information that could be used to impersonate you or gain access to your accounts.
2. Read the privacy policies posted on websites and mobile apps before using their website, purchasing their product, or downloading their mobile app.
3. Update the privacy and security settings on your social networking sites to control who sees your posts and adjust them to your personal comfort level. Don't rely on the default settings. Be aware that both well-meaning and questionable people use social networks to gather information about you.
4. Don't post anything online that you wouldn't mind seeing on the front page of a newspaper.
5. Make sure that your password is long and complex. Don't reuse passwords on multiple accounts. Instead, choose unique passwords for each account, especially your online banking account.
6. Log out of websites and browsers when you're finished using them. Never leave your online accounts open.
7. Be wary of sites that offer a reward or prize in exchange for your contact information.

Whether you use a Web based email service, keep files, or upload photos to, everything you write, upload, or post gets stored in a server that belongs to the online service, not to you



Every day, you give away personal information about yourself, sometimes without even realizing it. You do this when you take advantage of all kinds of services, including Internet searches, social networking, mobile and more. What private information are you sharing that you shouldn't? Use these tips to protect yourself:

Top Cyber Security Threats of 2017

It's a dangerous world out there in cyberspace. Security threats are escalating every year and have become more malicious with cybercriminals stealing financial and personal information. Here's a quick look at some of today's top computer security threats:

1. **Malware or Ransomware.** Exploits, malware and, more specifically, ransomware are increasing through vectors ranging from social networks to mobile devices to "secure" websites. As computer and operating system security continues to improve so will cybercriminals' new techniques to bypass these defenses.
2. **Mobile Threats.** Attackers are turning their attention to launching mobile banking attacks. Keep in mind that if your smartphone becomes infected, it can infect your computer and your home or work network too.
3. **Threats to Mobile Payments.** Electronic currency has made sending money extremely easy. Buying or selling, and sending money from a mobile device is becoming more popular. Hackers know this and are increasingly targeting mobile devices to steal money.
4. **Attacks on SMBs.** Small businesses believe they are immune to cyber-attacks. Truth is, small companies are typically less equipped to defend against an attack and hackers take advantage of that.
5. **User Errors.** Computers are great. For many transactions, they are often better and more reliable than people. Humans make mistakes when using computers, especially when they're not savvy about computer security. Even if you think you're doing all you can to avoid common security threats, you'd probably be surprised at how easily an outsider can find, and take advantage of, common mistakes.



The Security Scoop

October, 2016

Introduction to SASA IAM

FICAM Compliance

One of the five goals of the Federal Identity, Credential, and Access Management (FICAM) Roadmap is to "Improve Security Posture across the Federal Enterprise", with an objective of "Enabling Cybersecurity Programs". This comes through FICAM services supporting and augmenting existing security controls. Agencies must ensure their FICAM program meets all relevant Federal Information Security Management Act (FISMA) requirements by:



Selecting, implementing, assessing, and authorizing the appropriate system security controls for their FICAM systems.



Monitoring the effectiveness of those controls on an ongoing basis to support responsibility and accountability in the overall security of their FICAM system.

Our Mission

The mission of the Security Architecture and Software Assurance (SASA) Identity and Access Management (IAM) office is to ensure VA's FICAM services are in compliance with FISMA requirements, and second that those FICAM services are being used throughout the VA in fulfilling cybersecurity controls.



Explore the FICAM Checklist

A [tool](#) designed to help security professionals ensure services, systems, and applications are FICAM compliant.

Help Us Get to Know You

Take this [short survey](#). Your answers will help us better serve you.



Our Responsibilities

The tasks and responsibilities of the SASA IAM office are as follows:

- Ensure all aspects of information security are followed and implemented for FICAM programs in the VA.
- Validate process, system, and procedural compliance of FICAM systems and programs with Federal and VA information security policies and standards.
- Ensure VA systems and applications are using FICAM systems to improve their overall information security posture.
- Consolidate VA's expertise on FICAM systems in the areas of system security and compliance risk management as it relates to the implementation and use of FICAM systems.

Subscribe Now!!

For the latest security updates



Don't Let Phishers Catch You in Their Net

Falling for phishing could result in identity theft, viruses, and more.



How to Spot A Phishing Email

- Be skeptical about any email that uses your emotions against you.
- Beware of out-of-the-ordinary email addresses, subject lines, dates, times, and signature blocks.
- Don't trust an unexpected attachment, especially if it came from someone you don't know.
- If you are unsure about the legitimacy of an email, don't trust any links or contact information in it.



Watch

"The Phishing Detective"



ASK

Ace

Question: I think I fell for a phishing email — what should I do?

Answer: Contact the [IT Service Desk](#) as soon as possible. Remember to report suspicious emails to the [NIH Information Security Program](#) right away.



Did you
KNOW?

NIH runs phishing simulations to help build your awareness & resiliency.

Simulations give you a realistic experience in a safe environment. There's no penalty for falling for a simulation, but if you do, please take time to review the educational material afterwards.

TEEX Cyber Times

February 2017

The Internet Through the Eyes of Shakespeare

February is the month of love and at TEEX, we love cybersecurity! In honor of Valentine's Day, we are taking a look at what Shakespeare thinks about social media and the Internet.

To be or not to be, that is the question.

Shakespeare must have known the hazards that awaited us with the rise of the Internet and social media; and many people are asking themselves the same question: To be on online or not to be online?

If your answer to this question is yes, then Shakespeare has a few tips to help keep you safe and be a noble digital citizen.



Tip #1: "Love all, trust a few, do wrong to none."

It seems like every day there is a new story about someone being, saying, or doing something on social media that is harmful to others in the form of cyberbullying, trolling, posting insensitive videos, etc. Social media was created to share life experiences, whether that is sharing pictures of your newborn, new pet, graduating from college or simply wishing a friend or loved one "happy birthday". Social media is a part of the Internet that provides a platform for people to express themselves (both positively and negatively). However, the internet and social media can be used to execute crimes and as a place of contention and hate.



Here are some positive ways to use social media and methods on how to be safe doing it.

When posting on social media sites:

Love all: Keep it light. People visit their Facebook page and other social media sites for many reasons. Most want to check up on friends and family, share uplifting messages and things they like, or share photos of their vacation and family. Here are some ways to keep it light.

- ♥ Don't use it as a place to broadcast your hatred of other people, famous or otherwise.
- ♥ Use Facebook and other social media sites to make each other laugh and impact one another positively. Don't use it as a place to berate someone's looks, choices, or point of view.

TEEX Cyber Times

February 2017

♥ We all love a good laugh, but don't post embarrassing photos or videos of others, unless you have their permission. It's better to be laughed with than to be laughed at!

Trust a few: Lock down your Facebook page.

People are using social media sites to gather information before they initiate cyber and physical attacks. If you leave your photos, friends list, and posts open to anyone, you are providing the bad guys with information to further their attack. Explore the security and privacy settings to see your options for securing your Facebook page.

Do wrong to none: Think about what you post on social media and how it may impact others. Once you post something on social media, it no longer belongs to you and there is no guarantee it will stay within your group of friends. A picture of someone in a compromising situation could do irreparable harm to their career, reputation, or family.

Tip #2: "Love is blind, and lovers cannot see, the pretty follies that themselves commit"

Most of us love the Internet. We can use it to catch up on what is going on in the world, buy whatever you want, watch cat videos, and communicate with friends. Who wouldn't love that? But we shouldn't let our love of the Internet blind us to the hazards associated with it. Malicious websites can unknowingly download malware to your computer without you knowing, public Wi-Fi connections can be setup by criminals to steal your personal information, and hackers can create websites that look legitimate to record your login information so they can use it to access your accounts. Below are a few tips to prevent Internet blindness:

♥ Not all browsers are equal when it comes to secure browsing. Firefox and Chrome are considered to be more secure than other popular browsers because of the security features they offer.



LOVE

Newsletter Winner!

IHS Policy and Security Awareness Team

**Organization:
Indian Health Service**

National Cybersecurity Awareness Month

National Cybersecurity
Awareness Month



OCTOBER 2016

WEEK 4

The Internet of Things

Each year, manufacturers think up new ways to connect mundane, physical objects to the digital world. From toys to thermostats, toasters to TVs, and even toothbrushes to toilets, we're connecting, monitoring, and managing everyday tasks online.

The Internet of Things (IoT) is a growing phenomenon forcing major changes in the way we operate in our daily lives. With our expanding footprint of interconnectivity comes an expanding surface area of vulnerabilities for hackers to exploit. Why would a hacker exploit your toothbrush, and why should you care?

Halloween Cyber Tricks?

Hacking IoT devices like toothbrushes or coffee makers may seem like a benign prank, but these vulnerabilities can put your and your loved ones' personal information and safety at risk!

- IoT devices have been hijacked in order to send spam or host illicit pornography.
- Personal information has been compromised by IoT devices like: the Samsung smart fridge that exposed email credentials; climate-control systems that resulted in the 2013 Target credit card breach; and even barbie dolls that were connected to smart phones.
- Hackers have demonstrated the deadly potential to take over IoT products like: automobile engine and break systems; medical devices like Wi-Fi enabled pacemakers and drug-infusion pumps; and Wi-Fi enabled sniper rifles.
- Information about daily lives gained from Internet connected thermostats and door locks can provide burglars valuable information about your habits.

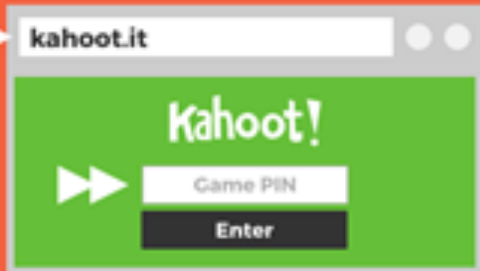


NCSAM Tips of the Week!

- Consider first whether your toothbrush or toaster needs to be "smart." If it does, make sure to purchase the ones with built-in security, and let the other companies know why you won't buy their unsecured products.
- Change the default passwords and give each device a unique password. Look for encryption options, enable security features, and apply patches or "firmware" updates when recommended.
- Never connect IoT devices at work without IT approval, and limit the number of devices that connect to the Internet at home. Software is available to enable a group of smart devices within the home (like light bulbs and door locks) to communicate with each other rather than the Internet.

Training Entries (10)

Join at **kahoot.it**
with Game PIN:
9399



Full Screen



0
Players

Kahoot!

Start

i Waiting for players...

“SUPER CEE GEE”

First Three Episodes

by: Dr. LMB Pailen, CISSP

Super Cybersecurity Grandma

EPISODE 1 - PHISHING AND RANSOMWARE



Dr. LMB Pailen

Super Cybersecurity Grandma

Episode 2 - Cyber Bullying



Dr. Lmb Pailen

Super Cybersecurity Grandma

Episode 3 - The Internet of Things



Dr. Lmb Pailen

Phishing and Ransomware

Cyber Bullying

Internet of Things

What Did I Miss?

Superbowl Party!

Hi, IHS User

1. This message has typos.

2. The Super Bowl is on a Sunday, not a Saturday.

Wow, what a game! Too celebrate, I am having a superbowl party Saturday!

Open the attached e-vite for logistics and to RSVP. Hope to see you there!

PhootballPhan Phillip

3. Be cautious of any message asking you to open an attachment you were not expecting.

4. Even if you think you know this sender, be sure to verify that they actually sent it, especially when it's a personal message delivered to your IHS.gov email address.





Small Business Cybersecurity Workbook

Prepared By:

Tim Villano & Lyman Terni



ARTEMIS
GLOBAL SECURITY, LLC



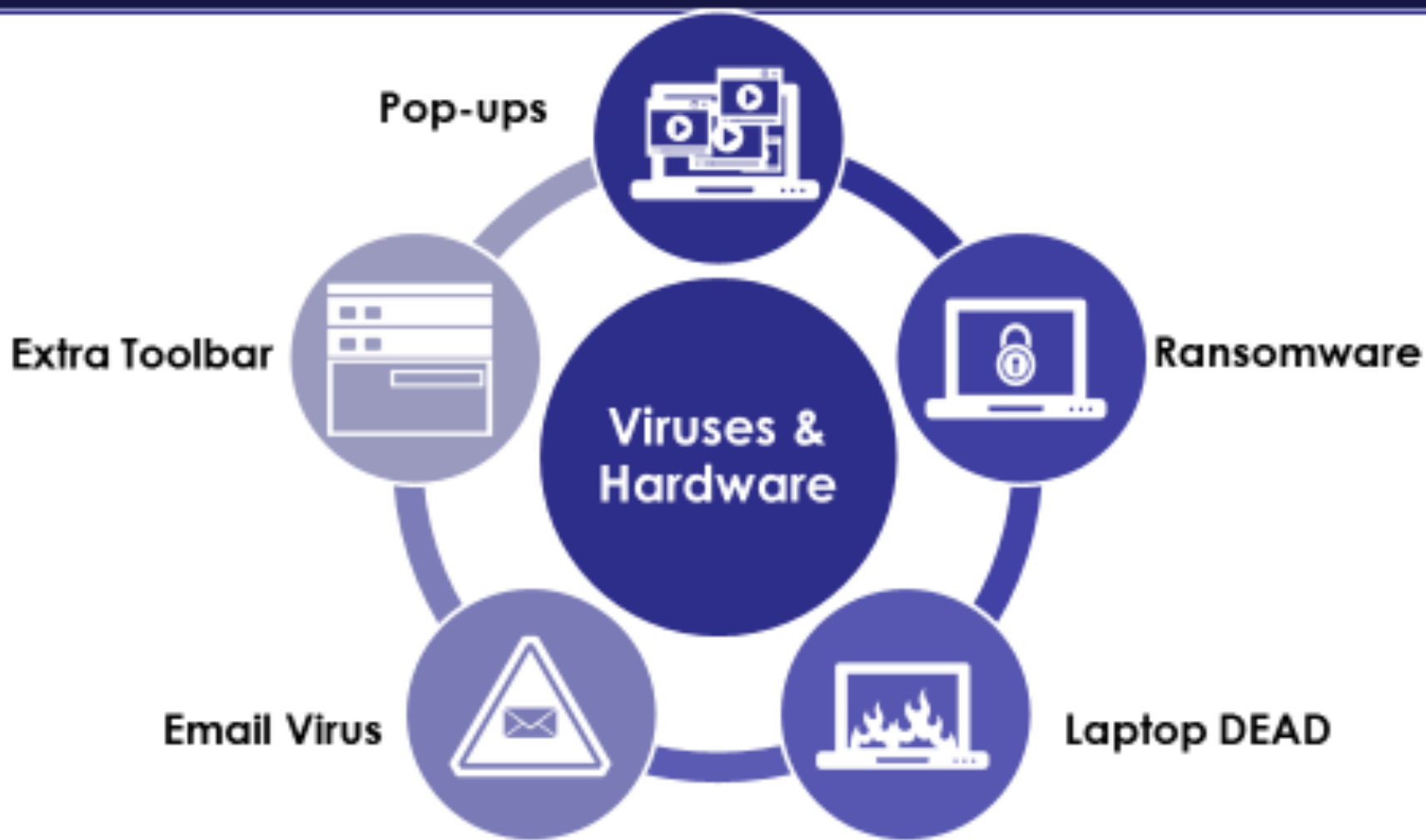
Presented By:

AMERICA'S **SBDC** Small Business
DELAWARE Development
Center



Office of Economic Innovation & Partnerships

Responding to a Cyber Attack



Phishing Our Global Audience - The Nielsen Way

Translated content

From: Special Promotions Team <freecreditmonitor@idshield.com>
 Date: Tue, Jan 17, 2017 at 12:00 PM
 Subject: Free Credit-Monitoring Service
 To:

English

Dear Valued Customer,

Some retail establishments recently received some negative press due to a data breach of customer credit card

De: Equipo de Promociones Especiales <monitordecreditogratis@idshield.com>
 Fecha: 24 de enero de 2017, 11:33
 Asunto: Servicio gratuito de control de crédito
 Para:

Spanish

Apreciable cliente,

Recientemente se han originado algunas noticias negativas de establecimientos de venta al por menor debido a una violación de los datos de la tarjeta de crédito de sus clientes y otros

From: Time de Promoções Especiais <freecreditmonitor@idshield.com>
 Date: 2017-02-09 15:41 GMT-06:00
 Subject: Serviço Gratuito de Monitoramento de Crédito
 To:

Portuguese

Prezado Cliente,

Alguns varejistas receberam recentemente algumas notícias negativas devido a violação dos dados de cartões de crédito dos clientes e outras informações pessoais. Eles valorizam você como cliente, e querem que você se sinta confiante de que eles irão tomar as precauções de segurança necessárias para proteger suas informações pessoais quando você compra em suas lojas e usam o cartão de crédito no site.

Como medida de boa fé, eles estão oferecendo um serviço de monitoração de crédito para todos seus valiosos clientes por um ano (seria um valor de \$150). Para ter a vantagem deste serviço gratuito, por favor use o link que segue abaixo em até 48 horas:
<http://www.affiliatedcompanies.com/freecreditmonitoring>

Obrigado pelo seu apoio!
Time de Promoções Especiais

The resulting behavior change

Savvy associates within other areas of the business are independently sending warnings to their co-workers, notifying them of the phishes.

Below is just one example of how proactive our workforce is becoming!

Dear all,

Some Brussels users recently received "Phishing" e-mail containing a link to an https site asking to connect the link for getting a voucher (see the message below)

Dear Valued Shopper,

As a frequent shopper in our retail facilities, you have earned some extra special rewards this month! We'd like to reward you with \$50 gift card.

[Click Here](#) to access your voucher for \$50 off your next purchase. This card is redeemable for a limited time, so act now!

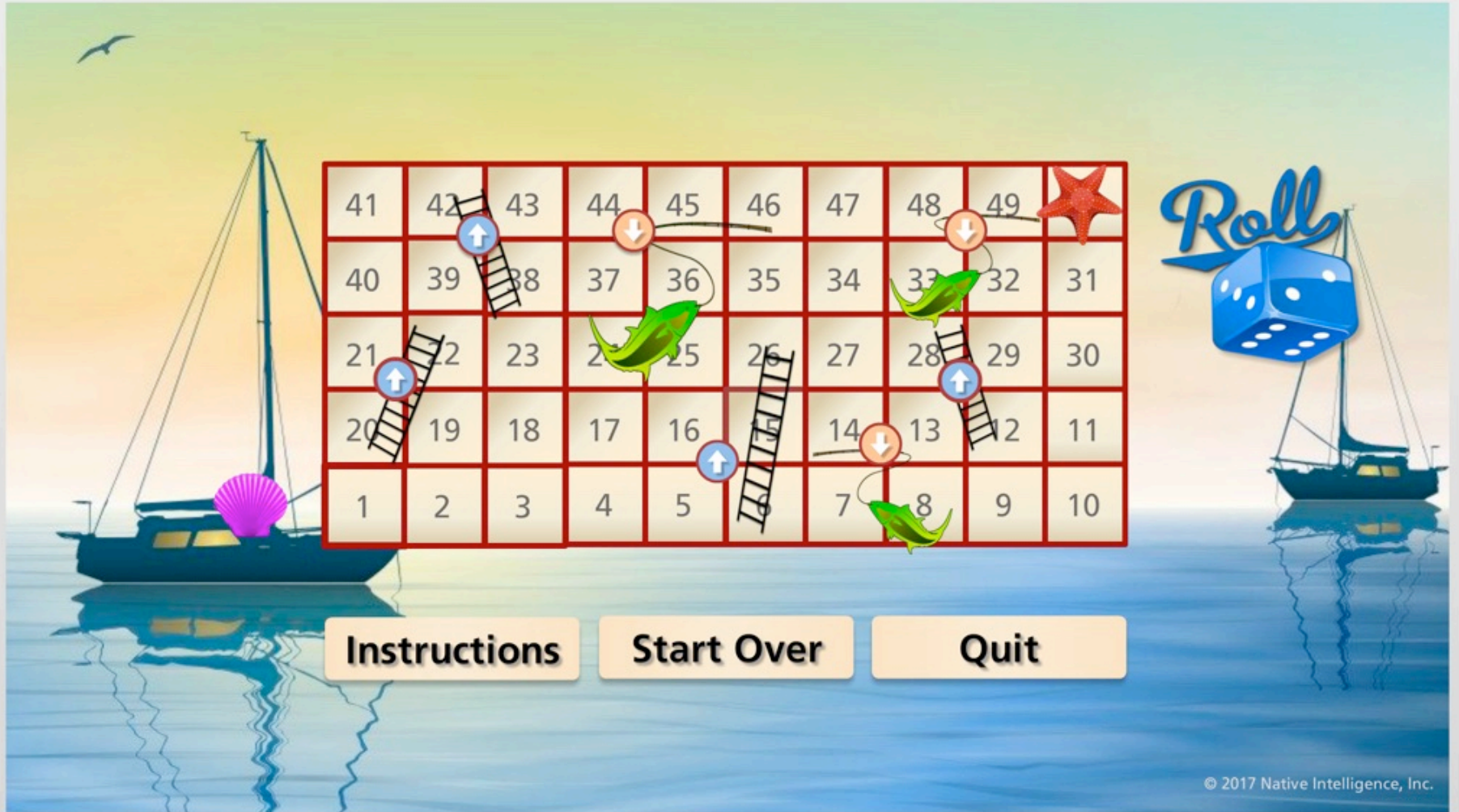
Sincerely,
The ExxonMobil Rewards Team

As a reminder, please remember to **never trust** that kind of e-mail and **never** communicate information's by connecting such sites.

Please don't "click" any kind of such link neither and, remember, only by "clicking" onto the link you are taking a risk.

In case of any question, please don't hesitate to contact local IT
Kind regards
Olivier

Phishing Game



Instructions

Start Over

Quit

CELEBRATE

SECURITY WEEK!



Take the
**SECURITY AWARENESS
WEEK CHALLENGE**

You could **WIN \$1,000!**

PLAY NOW 

Already registered? [log in here](#)

[OFFICIAL RULES](#) | [GET HELP](#) | [FAQ](#) | [WINNERS](#) | [LOG IN](#)

gravida nibh vel velit auctor aliquet. Aenean sollicitudin, lorem quis bibendum auctor, nisi elit consequat ipsum, nec sagittis sem nibh id elit. Duis sed odio sit amet nibh vulputate cursus a sit amet mauris. Morbi accumsan ipsum velit. Nam nec tellus a odio tincidunt auctor a ornare odio. Sed non mauris vitae erat consequat auctor eu in elit. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Mauris in erat justo. Nullam ac urna eu felis dapibus condimentum sit amet a augue. Sed non neque elit. Sed ut imperdiet nisi. Proin condimentum fermentum nunc. Etiam pharetra, erat sed fermentum feugiat, velit mauris egestas quam, ut aliquam massa nisi quis neque. Suspendisse in orci enim.

Cyber Threats	Types of Attackers	Cyber Attack Phases	Social Engineering	Cyber Security	Potpourri
\$100	\$100	\$100	\$100	\$100	\$100
\$200	\$200	\$200	\$200	\$200	\$200
\$300	\$300	\$300	\$300	\$300	\$300
\$400	\$400	\$400	\$400	\$400	\$400
\$500	\$500	\$500	\$500	\$500	\$500



TWO FORMS OF KIPS TRAINING

KIPS Live



- up to 80 trainees in the same room
- the same language for all participants
- a trainer and an assistant on site
- printed materials are essential

More limitations, but stronger engagement due to on-site presence and face-to-face competition. Plays as a team-building event as well.

KIPS Online



- up to 300 teams (= 1000 trainees) simultaneously, from any location
- different teams can choose a game interface in different languages
- a trainer leads a session via WebEx

Perfect for global organizations or public activities. Can be combined with KIPS Live to add some remote teams to the on-site event.

Training Winner!

IHS Policy and Security Awareness Team

**Organization:
Indian Health Service**

What Did I Miss?

Superbowl Party!

Hi, IHS User

1. This message has typos.

2. The Super Bowl is on a Sunday, not a Saturday.

Wow, what a game! Too celebrate, I am having a superbowl party Saturday!

Open the attached e-vite for logistics and to RSVP. Hope to see you there!

PhootballPhan Phillip


3. Be cautious of any message asking you to open an attachment you were not expecting.

4. Even if you think you know this sender, be sure to verify that they actually sent it, especially when it's a personal message delivered to your IHS.gov email address.



Video Entries (11)



 ITWD SecUre – Inspector SecUre – Cell Phone Security

<https://youtu.be/pE3zx3y8d9I>

SOCIAL MEDIA CYBERSECURITY


What you need to know
before you Share, Like,
Co



|| 🔊 🔍 0:04 []

<https://www.powtoon.com/c/gdEXHINYovi/1/m>



 MissionSecure Geisinger

<https://youtu.be/xVKxGQ6dBpg>

CSE's Top 10 IT Security Actions

THREAT SURFACE BEFORE THE TOP 10

- 1 USE SHARED SERVICES CANADA INTERNET GATEWAYS
- 2 PATCH OPERATING SYSTEMS AND APPLICATIONS
- 3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES
- 4 HARDEN OPERATING SYSTEM
- 5 SEGMENT AND SEPARATE INFORMATION
- 6 PROVIDE TAILORED AWARENESS AND TRAINING
- 7 MANAGE DEVICES AT THE ENTERPRISE LEVEL
- 8 APPLY PROTECTIONS AT THE HOST LEVEL
- 9 ISOLATE WEB-FACING APPLICATIONS
- 10 IMPLEMENT APPLICATION WHITELISTING

THREAT SURFACE AFTER THE TOP 10

00:00:46 00:02:31 CC




IFDS Clean Desk Policy Commercial

<https://youtu.be/KBJCO6F4r2g>

Actually, security incidents still happen at IHS more often than they should.



 Learning from Past Incidents

<https://youtu.be/PT72ztJmpG8>




InfoSightInc.com 

Three Proven Steps to Keep Your Business Safe from Cyber Attacks

<https://www.youtube.com/watch?v=MstyimSBW0I>



 Sorry-An Awareness Video from Nielsen

<https://youtu.be/jBO5bhZgX0U>

Identity and Access Management (IAM)

IAM Security Center



Locate Your
Information
Security Officer

Locate
Privacy

Locate Your Facility

Read Security Scoop

Subscribe now for
latest security updates

Latest Security Updates

SME Corner / FAQs

Contact Us

How Are We Doing

About IAM Security Center



The vision of the 'IAM Security Center' is to provide the VA intranet user community with a single source of information pertaining to Federal and departmental security relating to Identity and Access Management (IAM). Particular emphasis is on Federal and departmental directives, policies and handbooks, other VA IAM related organizations, and specific information pertaining to VA application system Project Managers, facility level Chief Information Officers, and Information Security Officers.



Did You Find
What You're Looking For?

Take this short survey to help us get to know you, so we can better serve you.



FICAM Compliance
Checklist

The FICAM Compliance Checklist is a tool designed to help ISOs (or designees) ensure services, systems, and applications are meeting the Access Control and Identification and Authentication FISMA controls through the use of VA's FICAM Services.



0:30

▶ VideoScribe



<http://sho.co/182H5>



<https://videocast.nih.gov/summary.asp?live=21835>

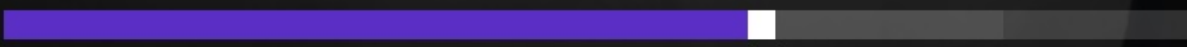
Email Security



F
i
l
t
e
r
s



0:05:26



0:03:03



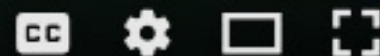
Video Winner!

**Rita John, John Creery,
Chelsea O'Hara, Nellie
MacNeil, Kyle Bachan, Tim
Herman, Rosanne Trudel,
& Sapna Kalhan**

**Organization:
IFDS Canada**



0:12 / 2:08



IFDS Clean Desk Policy Commercial

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!*