FISSEA

Security Awareness, Training, and Education Contest

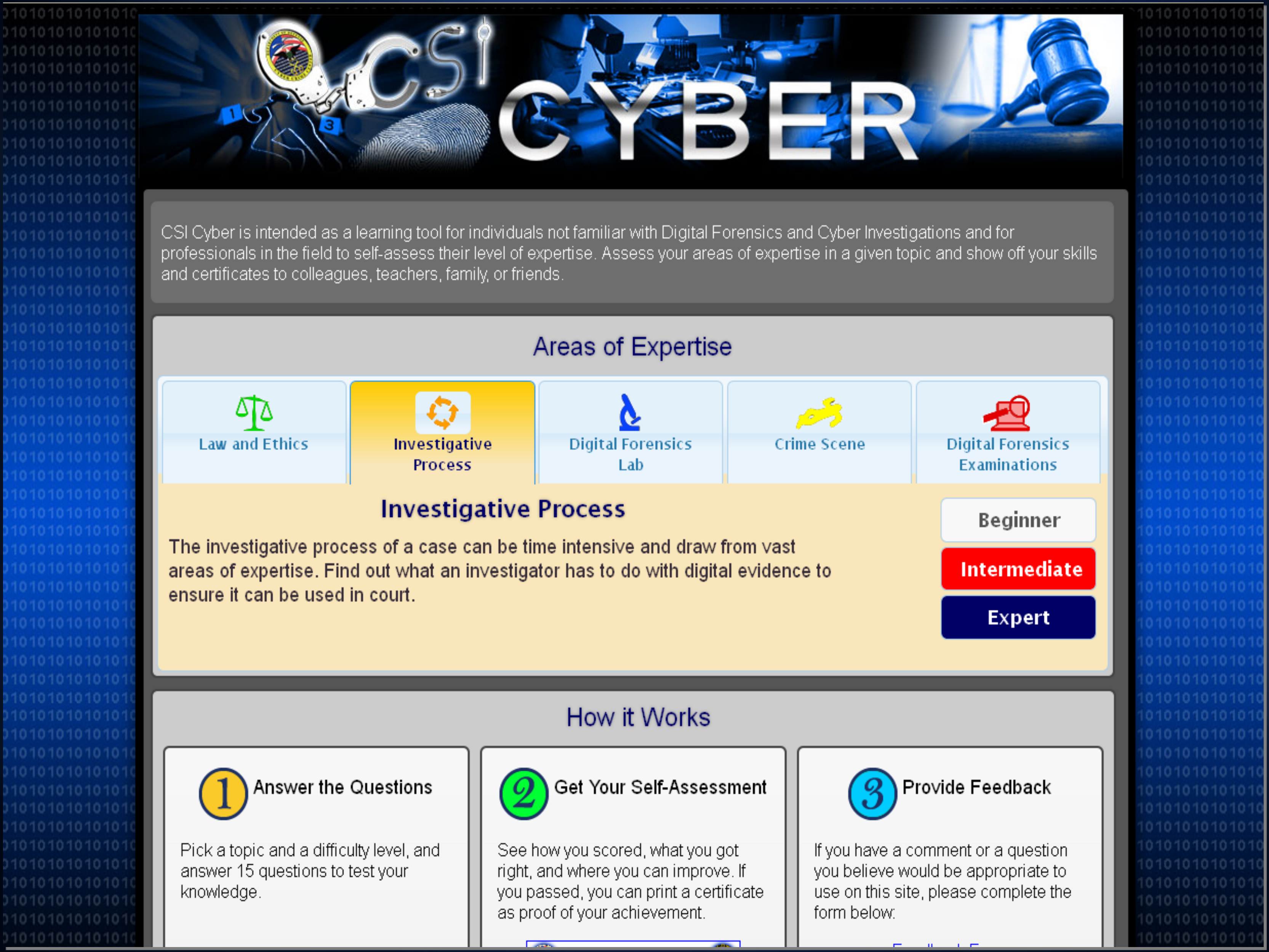
Categories

- Website
- Motivational Item
- Poster
- Newsletter
- Training

Judges

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

Website Entries (4)



CSI Cyber is intended as a learning tool for individuals not familiar with Digital Forensics and Cyber Investigations and for professionals in the field to self-assess their level of expertise. Assess your areas of expertise in a given topic and show off your skills and certificates to colleagues, teachers, family, or friends.

Areas of Expertise

Investigative Process

The investigative process of a case can be time intensive and draw from vast areas of expertise. Find out what an investigator has to do with digital evidence to ensure it can be used in court.

How it Works

1 **Answer the Questions**

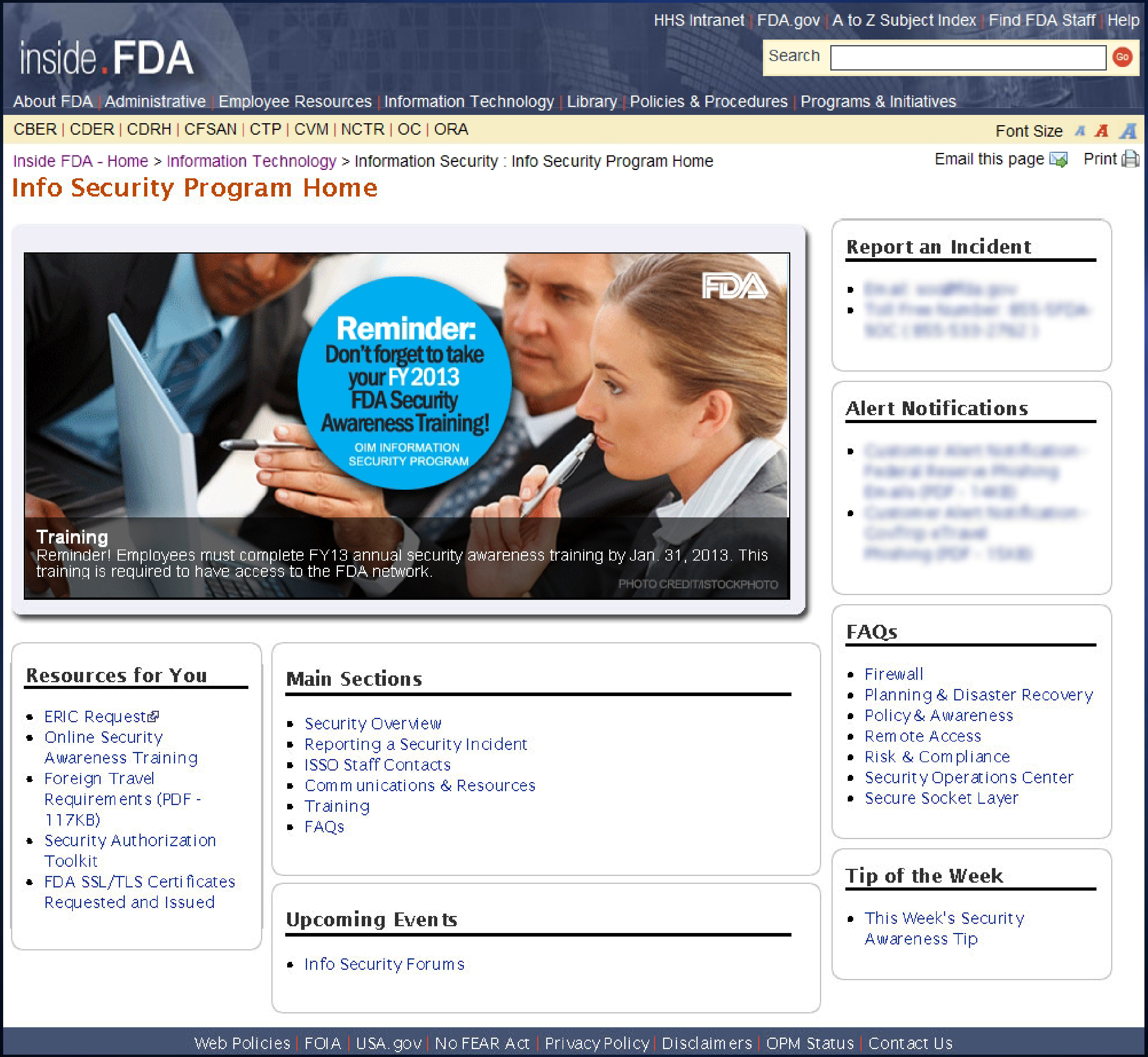
Pick a topic and a difficulty level, and answer 15 questions to test your knowledge.

2 **Get Your Self-Assessment**

See how you scored, what you got right, and where you can improve. If you passed, you can print a certificate as proof of your achievement.

3 **Provide Feedback**

If you have a comment or a question you believe would be appropriate to use on this site, please complete the form below.



HHS Intranet | FDA.gov | A to Z Subject Index | Find FDA Staff | Help

inside.FDA

Search Go

About FDA | Administrative | Employee Resources | Information Technology | Library | Policies & Procedures | Programs & Initiatives

CBER | CDER | CDRH | CFSAN | CTP | CVM | NCTR | OC | ORA

Font Size A A A

Inside FDA - Home > Information Technology > Information Security : Info Security Program Home

Email this page Print

Info Security Program Home

FDA

Reminder: Don't forget to take your FY 2013 FDA Security Awareness Training!

OIM INFORMATION SECURITY PROGRAM

Training

Reminder! Employees must complete FY13 annual security awareness training by Jan. 31, 2013. This training is required to have access to the FDA network.

PHOTO CREDIT/ISTOCKPHOTO

Report an Incident

- [redacted]

Alert Notifications

- [redacted]

Resources for You

- ERIC Request
- Online Security Awareness Training
- Foreign Travel Requirements (PDF - 117KB)
- Security Authorization Toolkit
- FDA SSL/TLS Certificates Requested and Issued

Main Sections

- Security Overview
- Reporting a Security Incident
- ISSO Staff Contacts
- Communications & Resources
- Training
- FAQs

Upcoming Events

- Info Security Forums

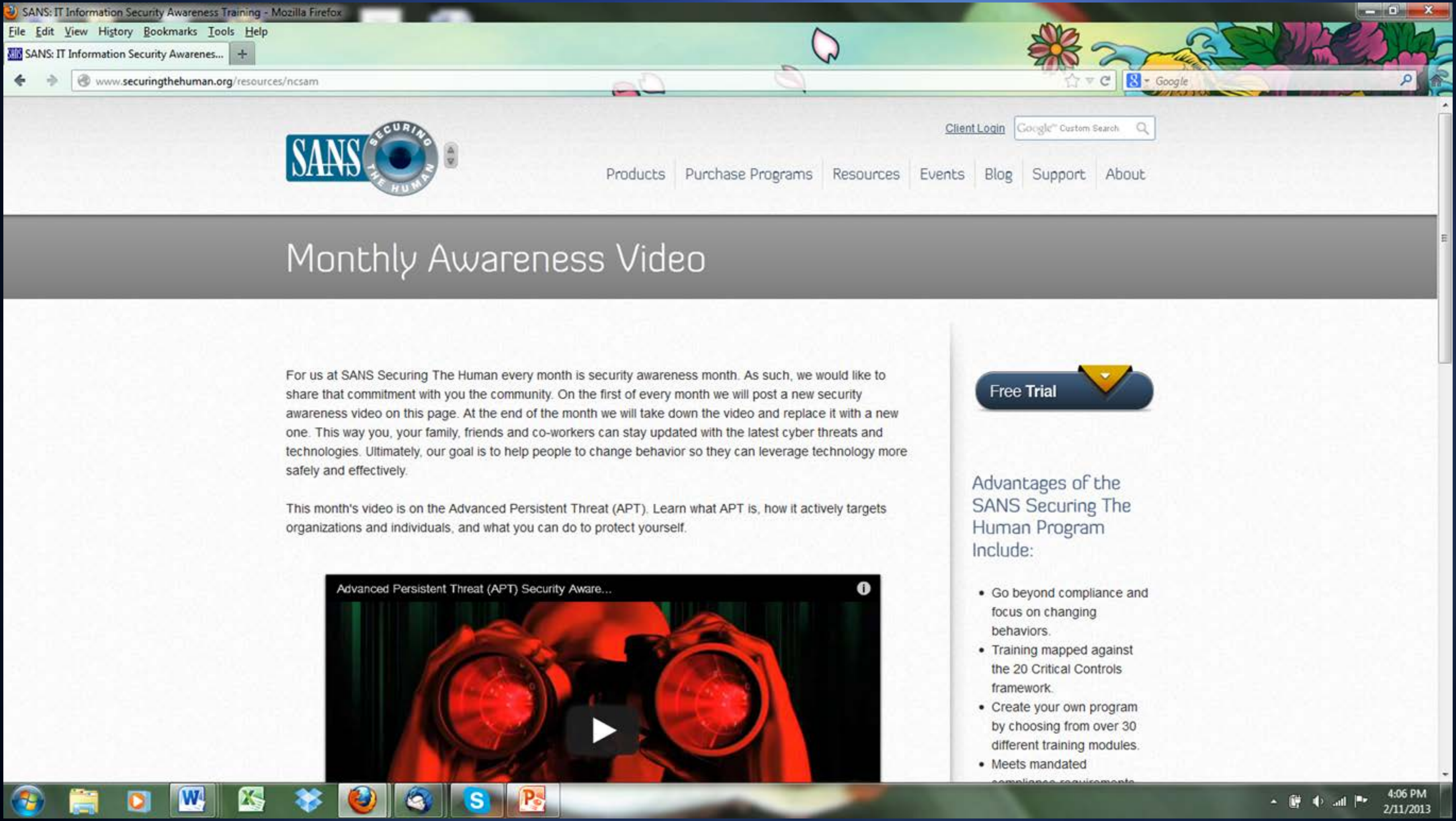
FAQs

- Firewall
- Planning & Disaster Recovery
- Policy & Awareness
- Remote Access
- Risk & Compliance
- Security Operations Center
- Secure Socket Layer

Tip of the Week

- This Week's Security Awareness Tip

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


SANS: IT Information Security Awareness Training - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SANS: IT Information Security Awarenes...
www.securingthehuman.org/resources/ncsam
Google
Client Login
Google Custom Search
SANS SECURING THE HUMAN
Products
Purchase Programs
Resources
Events
Blog
Support
About
Free Trial
Advanced Persistent Threat (APT) Security Aware...
4:06 PM
2/11/2013

Monthly Awareness Video

For us at SANS Securing The Human every month is security awareness month. As such, we would like to share that commitment with you the community. On the first of every month we will post a new security awareness video on this page. At the end of the month we will take down the video and replace it with a new one. This way you, your family, friends and co-workers can stay updated with the latest cyber threats and technologies. Ultimately, our goal is to help people to change behavior so they can leverage technology more safely and effectively.

This month's video is on the Advanced Persistent Threat (APT). Learn what APT is, how it actively targets organizations and individuals, and what you can do to protect yourself.

Advantages of the SANS Securing The Human Program Include:

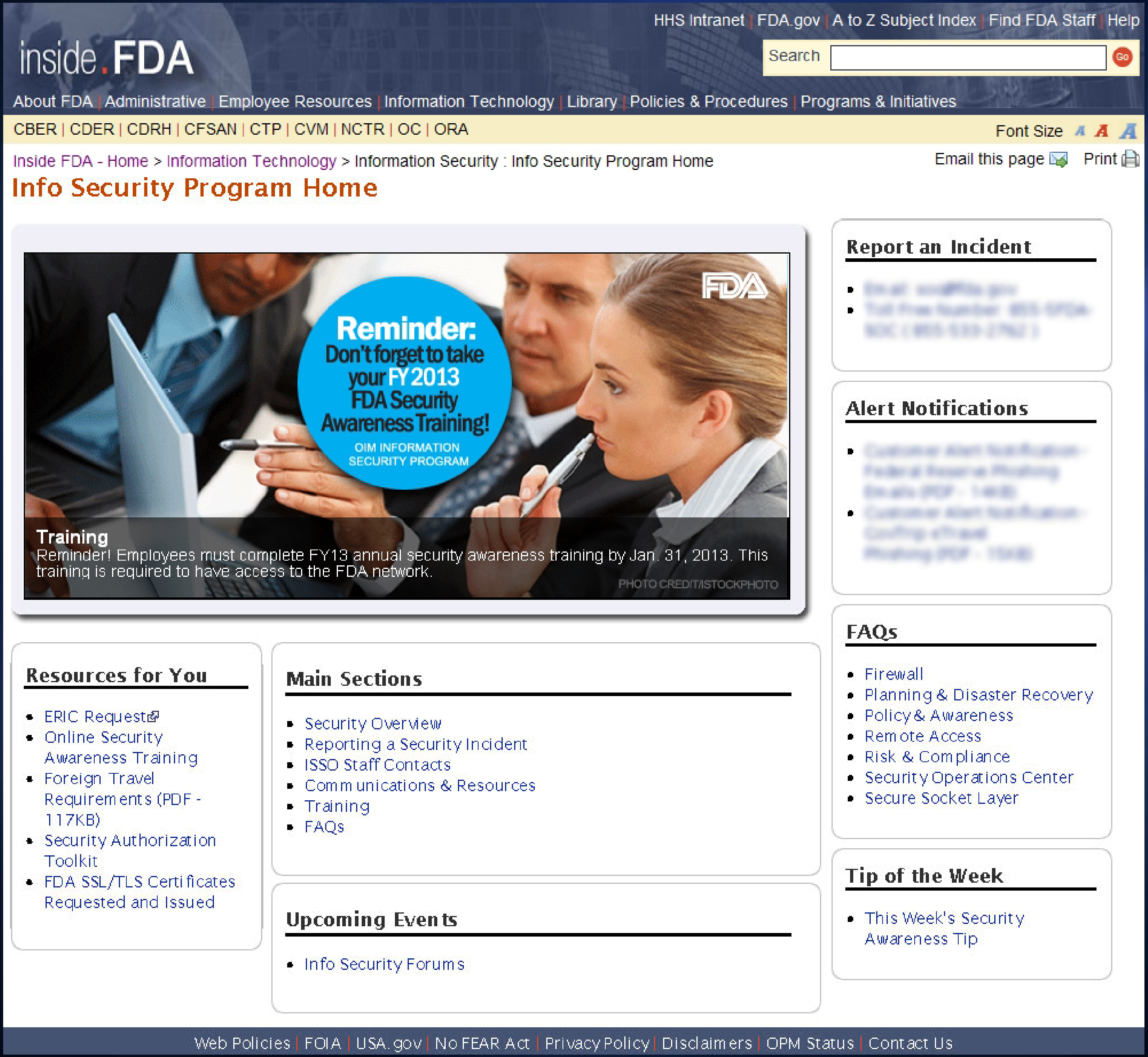
- Go beyond compliance and focus on changing behaviors.
- Training mapped against the 20 Critical Controls framework.
- Create your own program by choosing from over 30 different training modules.
- Meets mandated

ITWD Quick Clips -- Creating a Strong Password

Website Winner!

Sara Fitzgerald
and Kimberly Conway

Organization:
Food & Drug Administration
(FDA)



HHS Intranet | FDA.gov | A to Z Subject Index | Find FDA Staff | Help
inside.FDA
Search
Go
About FDA | Administrative | Employee Resources | Information Technology | Library | Policies & Procedures | Programs & Initiatives
CBER | CDER | CDRH | CFSAN | CTP | CVM | NCTR | OC | ORA
Font Size A A A
Email this page
Print

Inside FDA - Home > Information Technology > Information Security : Info Security Program Home

Info Security Program Home

Reminder: Don't forget to take your FY 2013 FDA Security Awareness Training!

OIM INFORMATION SECURITY PROGRAM

FDA

Training

Reminder! Employees must complete FY13 annual security awareness training by Jan. 31, 2013. This training is required to have access to the FDA network.

PHOTO CREDIT/ISTOCKPHOTO

Report an Incident

- [redacted]
- [redacted]

Alert Notifications

- [redacted]
- [redacted]

Resources for You

- ERIC Request
- Online Security Awareness Training
- Foreign Travel Requirements (PDF - 117KB)
- Security Authorization Toolkit
- FDA SSL/TLS Certificates Requested and Issued

Main Sections

- Security Overview
- Reporting a Security Incident
- ISSO Staff Contacts
- Communications & Resources
- Training
- FAQs

FAQs

- Firewall
- Planning & Disaster Recovery
- Policy & Awareness
- Remote Access
- Risk & Compliance
- Security Operations Center
- Secure Socket Layer

Upcoming Events

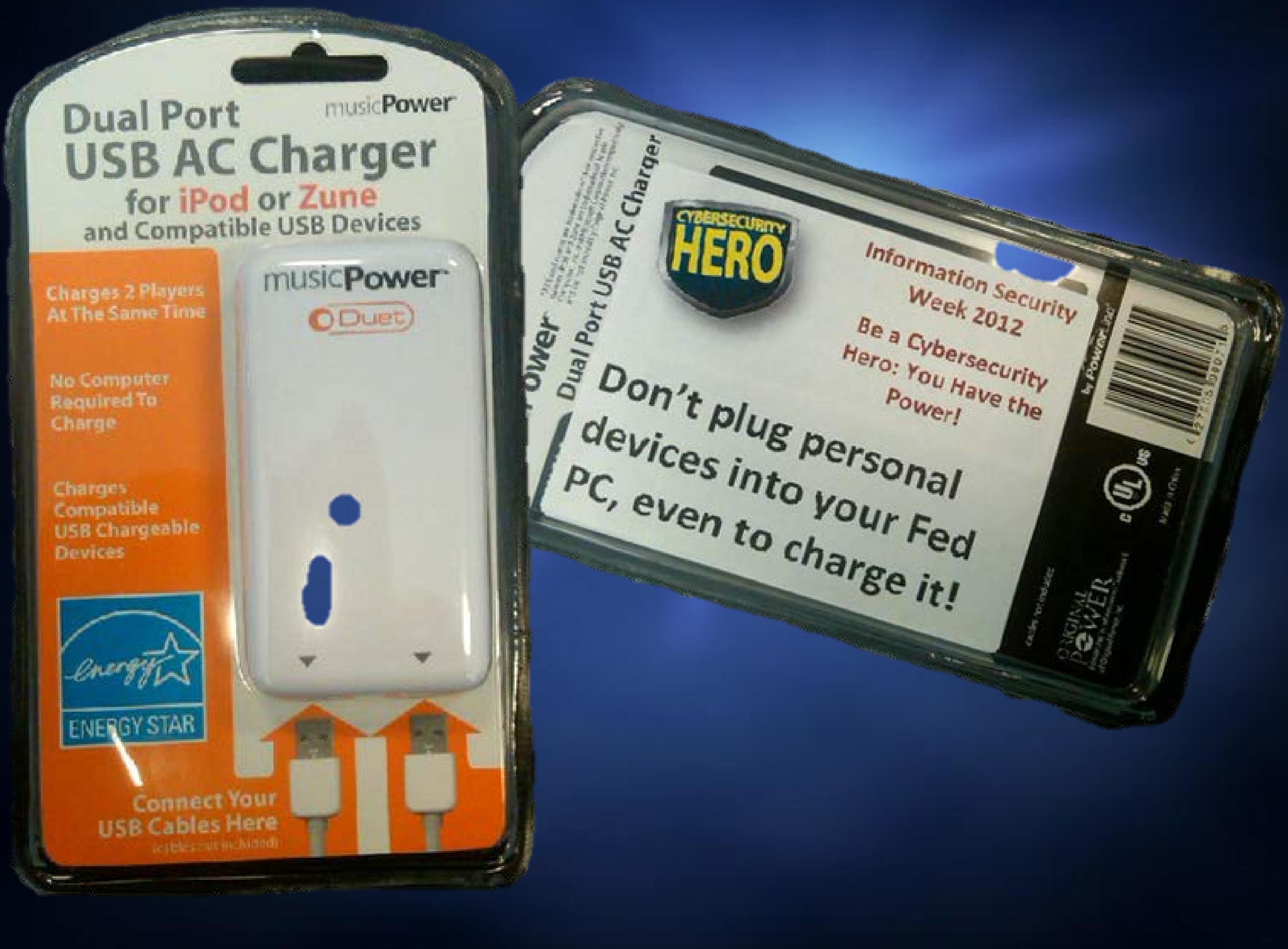
- Info Security Forums

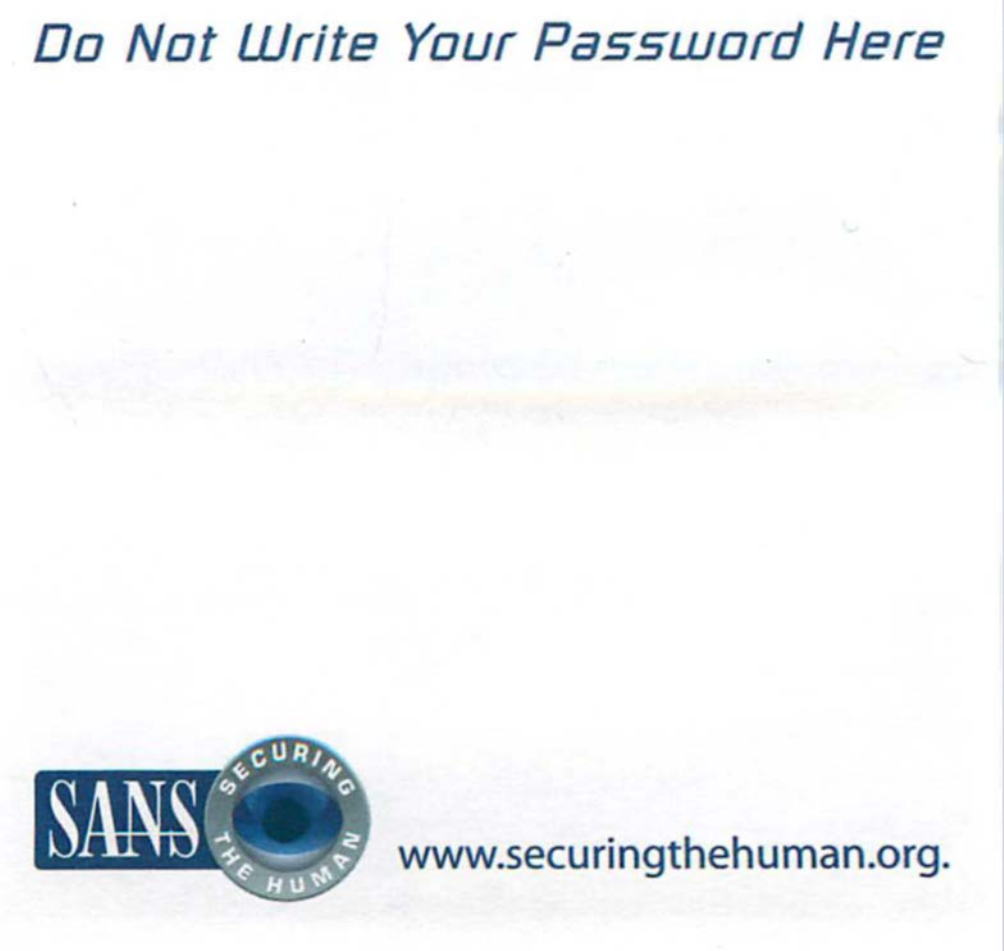
Tip of the Week

- This Week's Security Awareness Tip

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

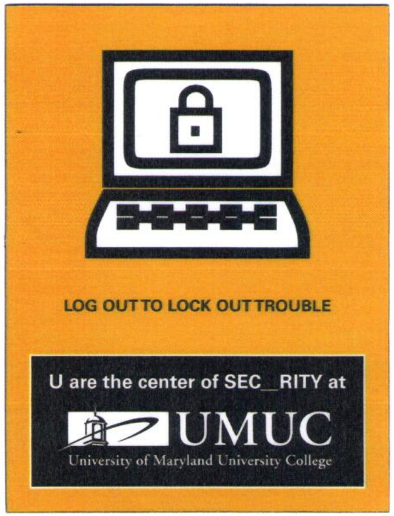
Motivational Item Entries (3)


musicPower
Dual Port
USB AC Charger
for iPod or Zune
and Compatible USB Devices
musicPower
Duet
Charges 2 Players At The Same Time
No Computer Required To Charge
Charges Compatible USB Chargeable Devices
ENERGY STAR
Connect Your USB Cables Here
(cables not included)
Dual Port USB AC Charger
CYBERSECURITY HERO
Information Security Week 2012
Be a Cybersecurity Hero: You Have the Power!
Don't plug personal devices into your Fed PC, even to charge it!
ORIGINAL POWER



Do Not Write Your Password Here

www.securingthehuman.org.

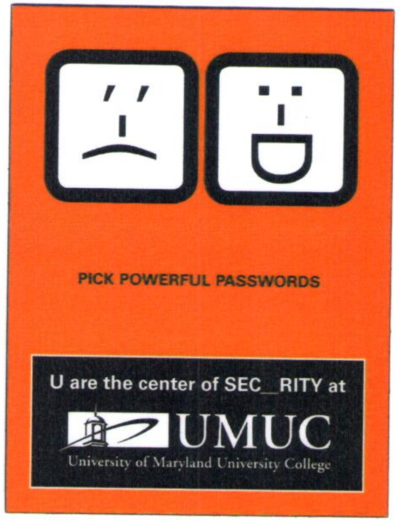


LOG OUT TO LOCK OUT TROUBLE

U are the center of SEC__RITY at

UMUC

University of Maryland University College

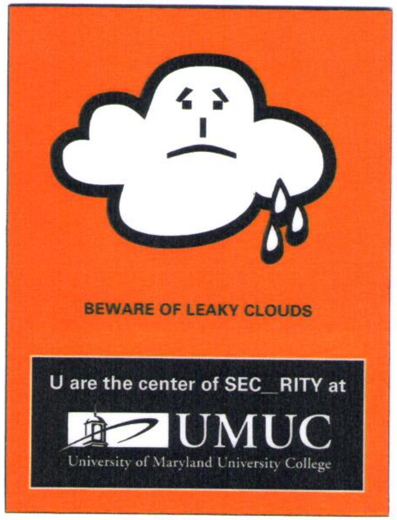


PICK POWERFUL PASSWORDS

U are the center of SEC__RITY at

UMUC

University of Maryland University College

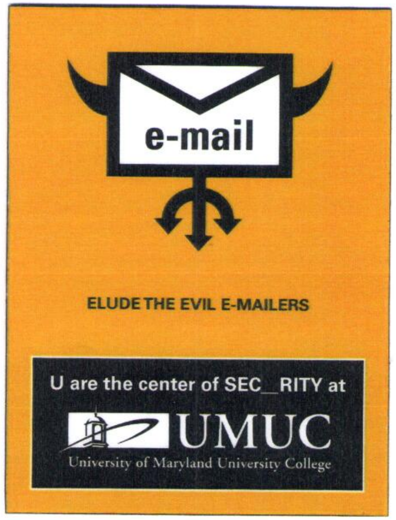


BEWARE OF LEAKY CLOUDS

U are the center of SEC__RITY at

UMUC

University of Maryland University College



ELUDE THE EVIL E-MAILERS

U are the center of SEC__RITY at

UMUC

University of Maryland University College

Motivational Item Winner!

Jennie Blizzard, Shannon Jones, and Shirley Clement

Organization:
Federal Reserve Bank

musicPower
Dual Port
USB AC Charger
for iPod or Zune
and Compatible USB Devices
musicPower
Duet
Charges 2 Players At The Same Time
No Computer Required To Charge
Charges Compatible USB Chargeable Devices
ENERGY STAR
Connect Your USB Cables Here
(cables not included)
Dual Port USB AC Charger
CYBERSECURITY HERO
ORIGINAL POWER

Information Security Week 2012

Be a Cybersecurity Hero: You Have the Power!

Don't plug personal devices into your Fed PC, even to charge it!

Poster Entries (14)

WORKING FROM HOME AND USING A HOME-BASED WIRELESS CONNECTION?

- Use Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy—which can be hacked in minutes). Make sure that the encryption feature is turned on.
- Consider hiding the identity of your wireless network by turning off the identifier broadcaster feature of your router.
- Change your router's pre-set password for administration to something only you know. The longer and more complex the password, the tougher it is to crack.
- Only allow trusted (e.g, your family) computers to access your network.

USEC
A Global Energy Company

Passwords are like bubble gum...

They are strongest when fresh,
should not be shared,
and if left around, create a sticky mess.

DEPARTMENT OF STATE
UNITED STATES OF AMERICA

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

CYBER SECURITY
AWARENESS

***Don’t use the same password** for multiple accounts!*
If hackers successfully discover a password, they immediately assume the victim has used the same password for other accounts. Sometimes this allows access to an important account simply because the same password was also used elsewhere.

Vary your passwords

…so they don’t
fall like dominoes

GLOBAL RISK AND SECURITY

DON'T MAKE YOURSELF AN EASY TARGET

AT WORK OR AT HOME

Personal safety is everyone's business whether it is in their professional or personal lives. Do not get too casual in your approach to safety and become a victim. It is crucial that all associates stay up-to-date on training and remain educated about different security risks. Safety should become a habit that is maintained not only at work but at home. Use common sense and take a more proactive approach. It is vital that associates take the necessary precautions to protect Diebold, themselves and others as part of their daily routine. Personal safety is a 24-hour job, so make it part of your everyday work and home culture to ensure that you do not become a target.

Do you have questions regarding personal safety and steps you can take to ensure you don't become a target? Contact globalriskandsecurity@diebold.com

Security... a team effort but an *individual* responsibility.

DIEBOLD
INNOVATION DELIVERED®

Don't bring back more than memories…

Follow the International Travel Policy

http://[redacted]

NATIONAL INFORMATION SECURITY AWARENESS

UNITED STATES FEDERAL RESERVE SYSTEM

File Edit View Favorites Tools Help
Norton
Google
Gmail
COMPOSE
People (2)
LOFT
Show details
Diabetic Cake Recipe
Anthropologie Tops
Lofts In DC

EMAIL FROM A STRANGER?

CAREFUL… COULD BE DANGER!

Please help me find my lost dog

JANE DOE JDoe@gmail.com

LOST DOG $$$

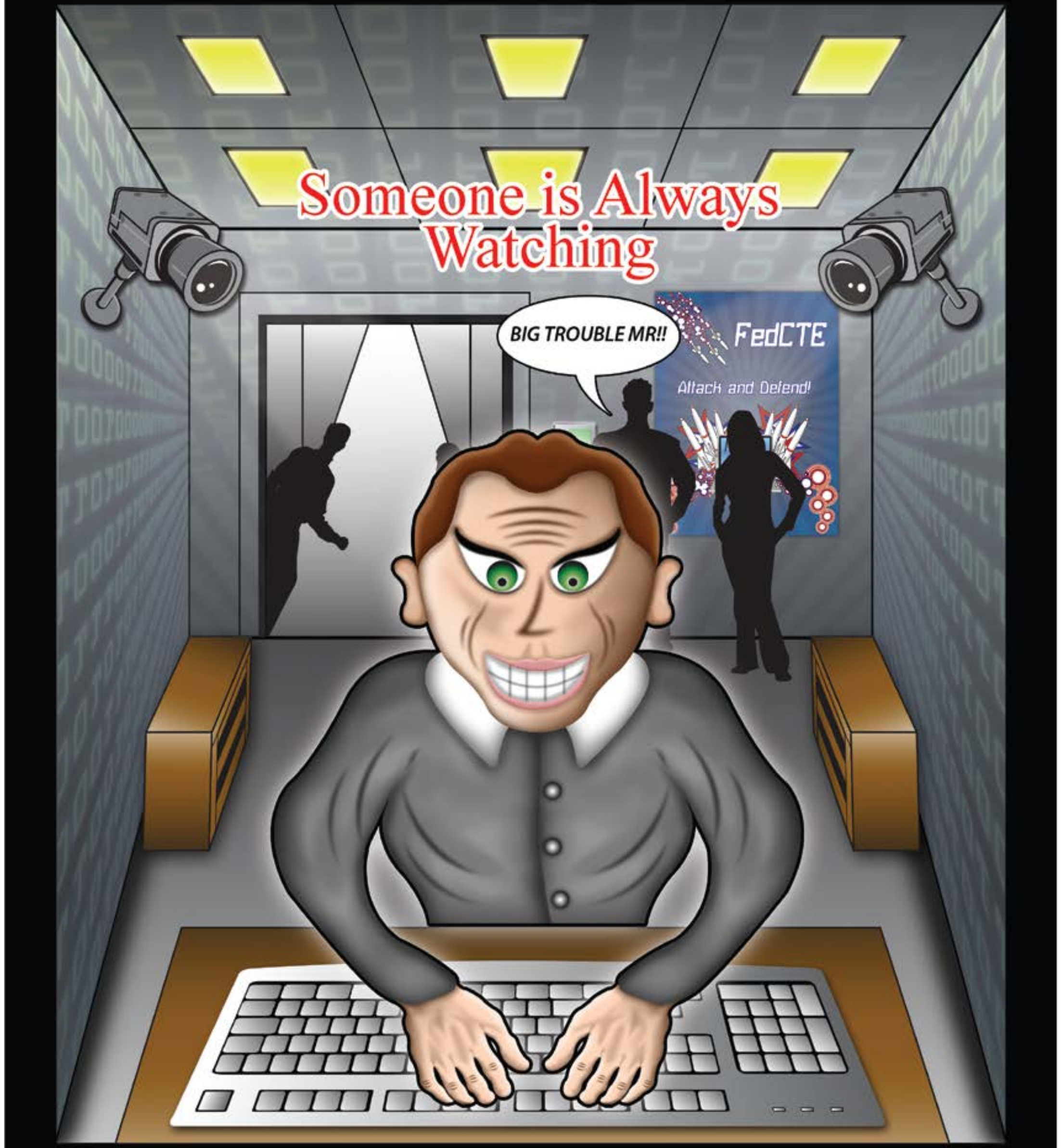
I am emailing anyone that I can about my lost puppy. Please help me find Fluffy. A reward is being offered to anyone who can provide any information about his location.

Please click here for more details.

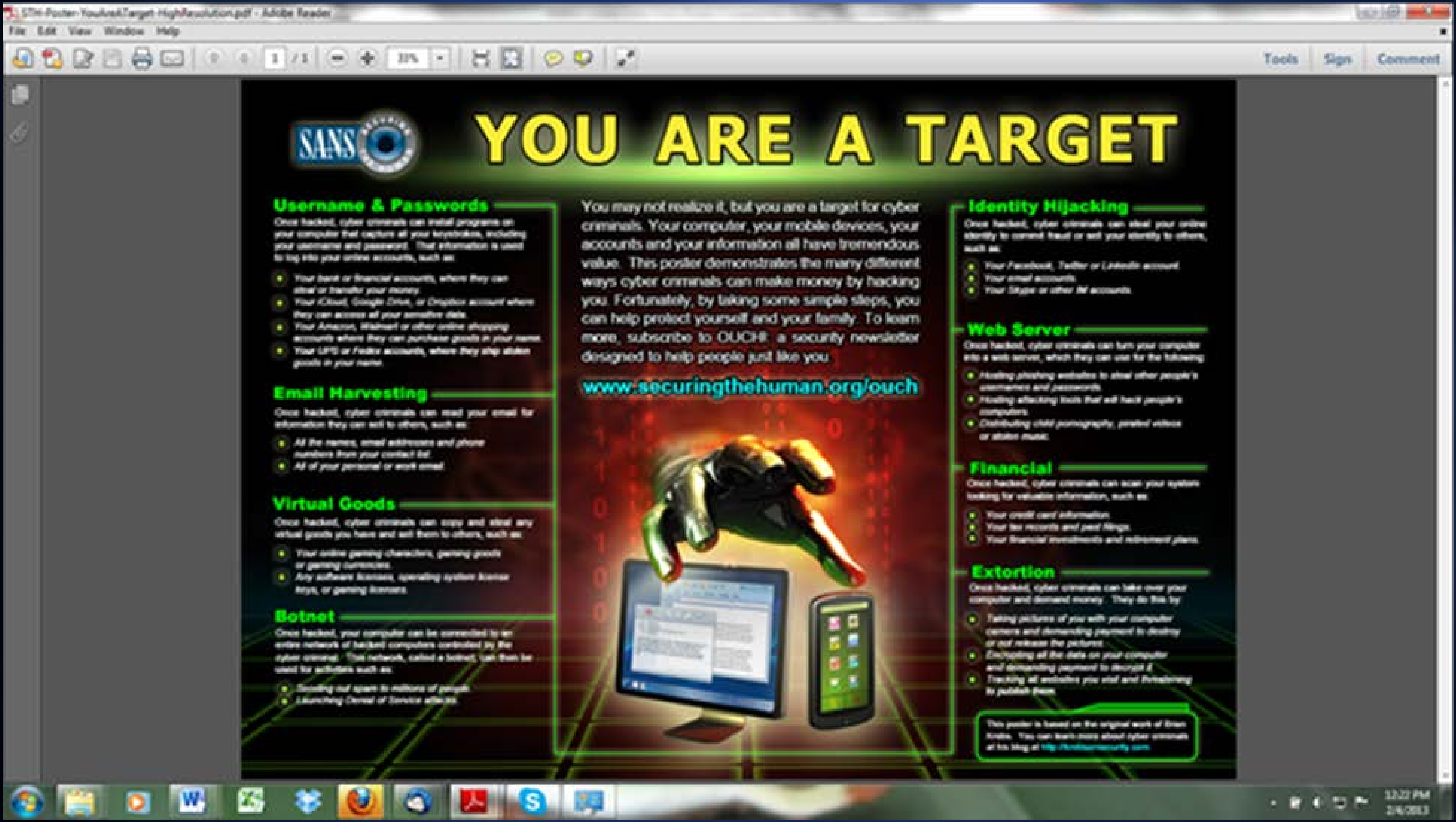
Please check out our website for more information:

http://inside.fda.gov:9003/it/ITSecurity/Communications/ucm244443.htm

CONTINUOUS MONITORING



05/27/11, 11:05 PM, (TBD)


STH-Poster-YouAreATarget-HighResolution.pdf - Adobe Reader
File Edit View Window Help
1 / 1
33%
Tools
Sign
Comment
SANS
12:22 PM
2/6/2013

YOU ARE A TARGET

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH! a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

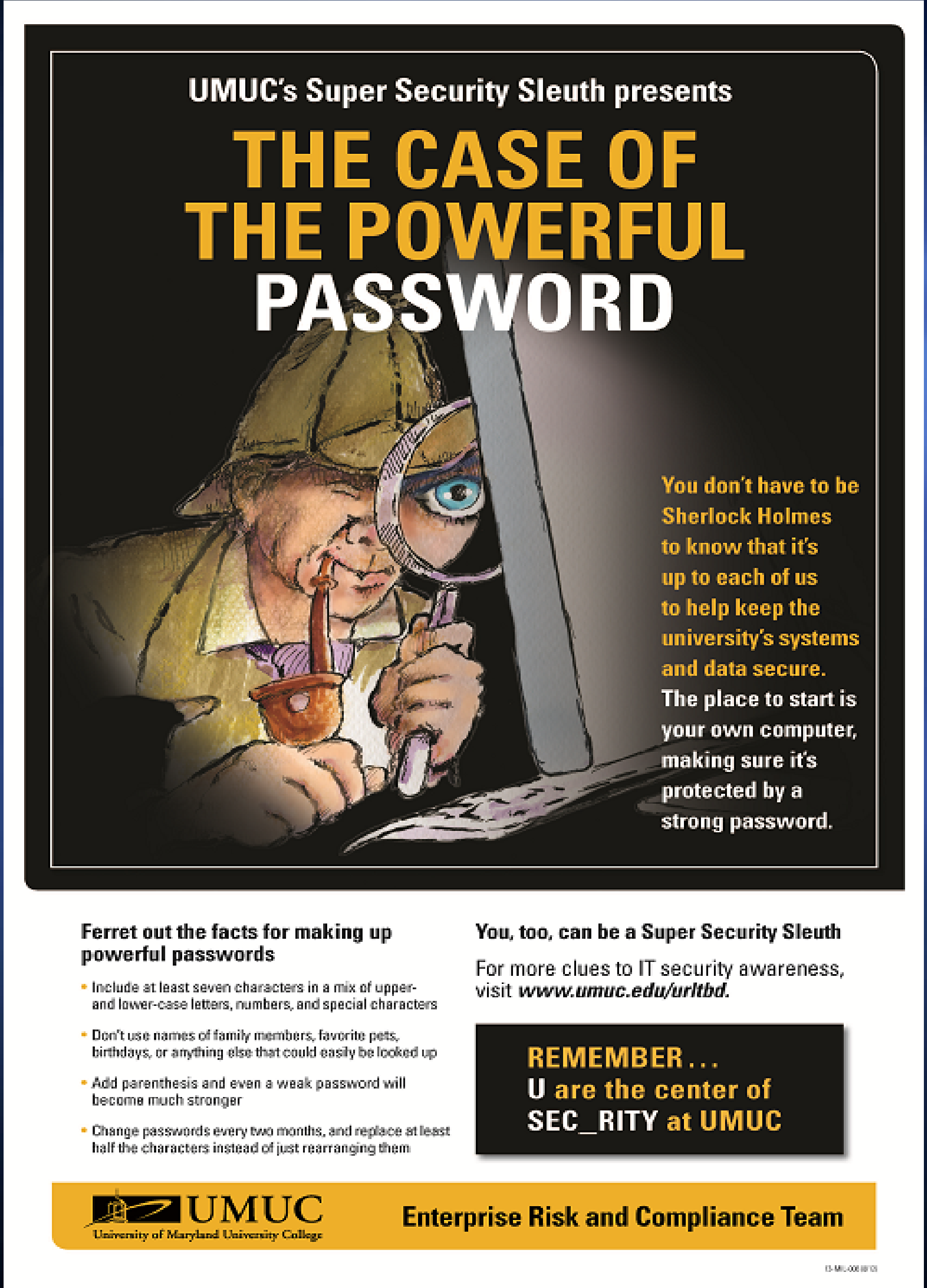
This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

“We will protect Veterans’ information as if it were our own.”

– *Christopher Wlaschin*

ADAS for Security Operations, Information Security
Office of Information and Technology
US Department of Veterans Affairs

ITWD
IT WORKFORCE DEVELOPMENT



UMUC's Super Security Sleuth presents

THE CASE OF THE POWERFUL PASSWORD

You don't have to be Sherlock Holmes to know that it's up to each of us to help keep the university's systems and data secure. The place to start is your own computer, making sure it's protected by a strong password.

Ferret out the facts for making up powerful passwords

- Include at least seven characters in a mix of upper- and lower-case letters, numbers, and special characters
- Don't use names of family members, favorite pets, birthdays, or anything else that could easily be looked up
- Add parenthesis and even a weak password will become much stronger
- Change passwords every two months, and replace at least half the characters instead of just rearranging them

You, too, can be a Super Security Sleuth

For more clues to IT security awareness, visit ***www.umuc.edu/urltbd.***

REMEMBER . . .
U are the center of
SEC_RITY at UMUC

UMUC
University of Maryland University College

Enterprise Risk and Compliance Team

DON'T GET HOOKED

Beware of Phishing Scams

Do not open unsolicited emails or emails from someone you don't know.

Do not click on links to web sites, download attachments, or enter personal financial data on forms accompanying suspicious emails.

Do not forward chain emails or post email addresses to web sites.

GTS
Global Training Solutions Inc.

learn. act. protect.
PROTECTING TVA'S CYBER ASSETS IS EVERYONE'S RESPONSIBILITY
TVA

ED-DEFENDERS PRESENTS

Posts Are Forever Forever Forever

DEPARTMENT OF EDUCATION ED-DEFENDERS

BEST PRACTICES FOR USING SOCIAL MEDIA SITES:

- Understand and follow Department policies for use of social media.
- Use unique passwords
- Be cautious about how much personal information you provide on social networking sites.
- Don't trust that a message is really from who it says it's from.
- Be selective about who you accept as a friend on a social network and share personal information only with people you know.
- Just like email, use caution before clicking a link or URL in a message.
- Learn about and use privacy and security settings on your social network sites.
- Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache. Posts are forever!

I'M READY

I

ARE YOU?

@you: th!^k ur $@fe?

Likes: Hockey

Attends church

Job

Politically active

College

Carpools to work

Two sons play T-ball

Favorite Restaurant: Mels Diner

Dislikes: Black and White movies

Cruisin to Bahamas on Vacation

Software used

Home address

Single

Languages spoken

Political Affiliations & Donations

Brother is turning 50

Lived at same address for 5 years

Works at a Company with 100,000 employees

Favorite Web site: Sports

Geographic location

Dislikes: Broccoli

Owns an iPad

Serves as a board member

Education Level

Hometown

Volunteers

Zip Code is 21401

Likes: Green Living

Sister is a dentist

Lives in San Diego

Frequent Flyer

Phone number

Runs in 5Ks

Likes: Sushi

High School Attended

Favorite Celebrities

IT Defense Worker

Likes: Online News

$350 Shoes

Likes: Rain

Banks Online

Owns a Ducati

Has a wife and three kids

Coaches

INFORMATION ASSURANCE

Defenders of the Domain

Frequency Management

AFI-33-106
AFI 33-118

Primary Unit IAO is: ***<u>***Enter Name & Phone Number***</u>***

Alternate Unit IAO is: ***<u>***Enter Name & Phone Number***</u>***

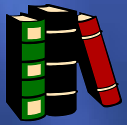
440 AW Information Assurance Office – 440aw.ia@us.af.mil
Pope Comm Focal Point – Pope.cfp@us.af.mil

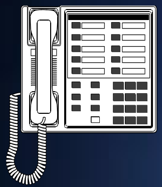
<u>Classified Processing</u>
AFSSI 7700
AFSSI 7702
AFSSI 7703

AFI 33-200

Computer Security (COMPUSEC)
AFMAN 33-282

Information Assurance (IA) Management
AFI 33-200





Telephone System /Circuits
AFI 33-111
AFI 33-116
Telecommunications Monitoring and Assessment Program, **AFI 10-712**

ALL Removable Media requires IA approval!

No Wireless Keyboards or Mice!

Remove Your CAC When You Leave!

Protect Personally Identifiable Information (PII)!

Protect Classified Signals at All Times!

Air Force Certification & Accreditation Program,
AFI 33-210

Network Management **AFI 33-115 Vol I**

Licensing Network Users **AFI 33-115 Vol II**

Commanders Guidance and Responsibilities,
AFI 33-101

Information Assurance Assessment and Assistance Program, **AFI 33-230**

Feb 2013
440 CF/SCXS

Poster Winner!

Alexis Benjamin

Organization:
Department of State,
Office of Computer Security

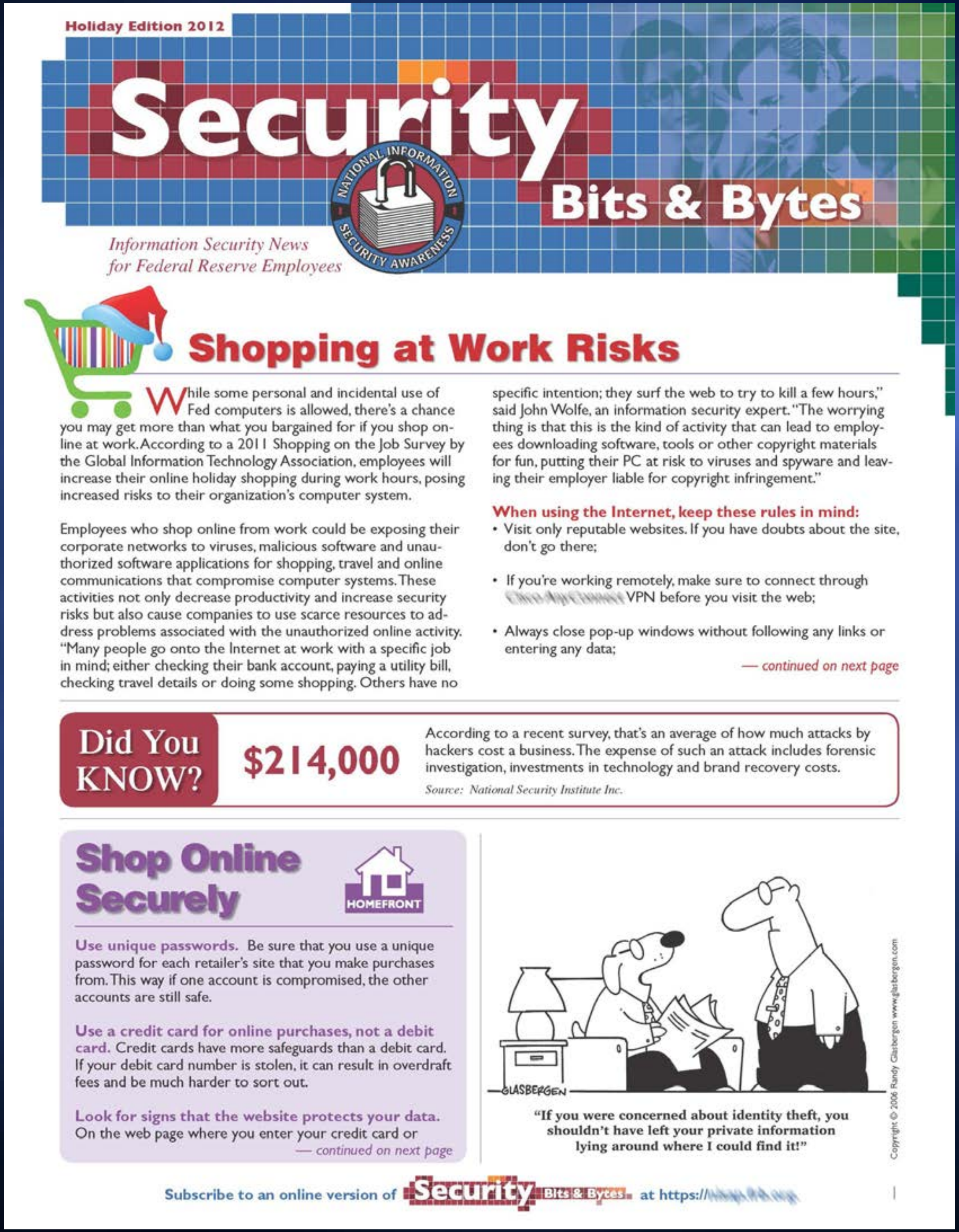
Passwords are like bubble gum…

They are strongest when fresh,
should not be shared,
and if left around, create a sticky mess.

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

CYBER SECURITY
AWARENESS

Newsletter Entries (6)



Holiday Edition 2012

Security Bits & Bytes

Information Security News for Federal Reserve Employees

Shopping at Work Risks

While some personal and incidental use of Fed computers is allowed, there's a chance you may get more than what you bargained for if you shop online at work. According to a 2011 Shopping on the Job Survey by the Global Information Technology Association, employees will increase their online holiday shopping during work hours, posing increased risks to their organization's computer system.

Employees who shop online from work could be exposing their corporate networks to viruses, malicious software and unauthorized software applications for shopping, travel and online communications that compromise computer systems. These activities not only decrease productivity and increase security risks but also cause companies to use scarce resources to address problems associated with the unauthorized online activity. "Many people go onto the Internet at work with a specific job in mind; either checking their bank account, paying a utility bill, checking travel details or doing some shopping. Others have no specific intention; they surf the web to try to kill a few hours," said John Wolfe, an information security expert. "The worrying thing is that this is the kind of activity that can lead to employees downloading software, tools or other copyright materials for fun, putting their PC at risk to viruses and spyware and leaving their employer liable for copyright infringement."

When using the Internet, keep these rules in mind:

- Visit only reputable websites. If you have doubts about the site, don't go there;
- If you're working remotely, make sure to connect through [redacted] VPN before you visit the web;
- Always close pop-up windows without following any links or entering any data;

— continued on next page

Did You KNOW? **$214,000**

According to a recent survey, that's an average of how much attacks by hackers cost a business. The expense of such an attack includes forensic investigation, investments in technology and brand recovery costs.

Source: National Security Institute Inc.

Shop Online Securely

Use unique passwords. Be sure that you use a unique password for each retailer's site that you make purchases from. This way if one account is compromised, the other accounts are still safe.

Use a credit card for online purchases, not a debit card. Credit cards have more safeguards than a debit card. If your debit card number is stolen, it can result in overdraft fees and be much harder to sort out.

Look for signs that the website protects your data. On the web page where you enter your credit card or

— continued on next page

"If you were concerned about identity theft, you shouldn't have left your private information lying around where I could find it!"

IT Defender

From the OIM Information Security Program

February 2012

Issue 7

Inside this issue:

Report an Incident

If you suspect lost, misplaced or stolen equipment or a breach of Personally Identifiable Information (PII), notify your equipment manager **AND** contact the FDA IT Security Operations Center (SOC) at:

- **Email:** [redacted]
- **Toll Free Number:** [redacted]

Are you trading security for convenience?

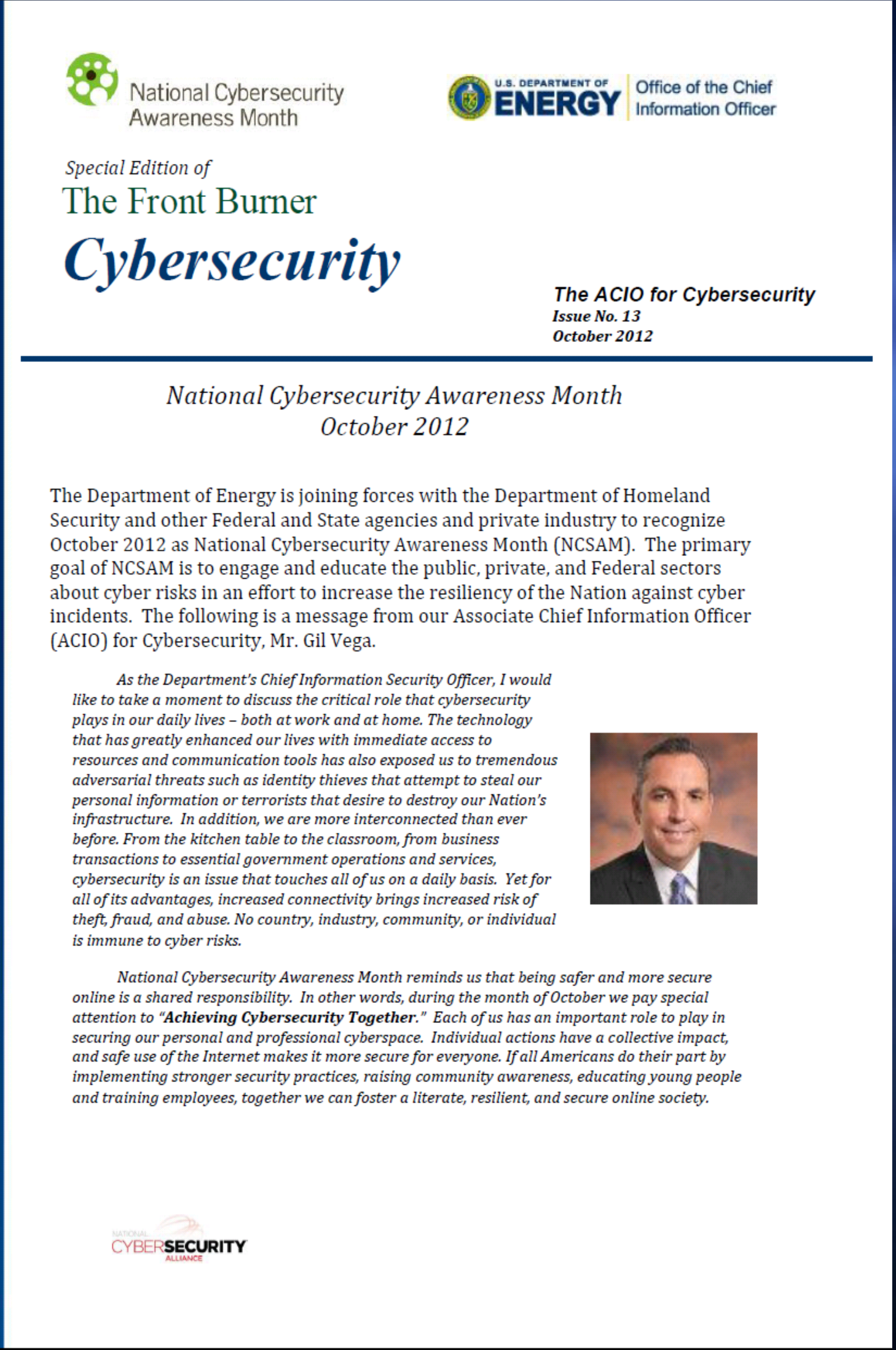
Think your iPhone or Droid is secure? You're not alone. The majority of mobile device users feel that way… the truth is, these devices are not as secure as you might think. And we're not talking about people wanting to highjack your Angry Birds apps to erase your high scores either.

"Smartphones today handle a great quantity of private and sensitive data, in a highly portable, network-connected mobile computer. The data stored and transmitted can include security credentials, personal financial information, private communications, sensitive company data and more.

The appWatchdog tests focus on what is stored on the device. Smartphone apps handle usernames, passwords and private app data, all of which should be stored securely or not at all. In the event of a lost device or malware infection, data stored insecurely can be compromised."

– Source: www.viaforensics.com "Mobile App Security Study"

Perhaps the hottest topic with regard to mobile app security is banking. In fact, according to Juniper Research, over 200 million people took advantage of mobile banking in 2010, and they say that number will double by 2013. It's quick, easy and readily available from our back



National Cybersecurity Awareness Month

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Special Edition of

The Front Burner

Cybersecurity

The ACIO for Cybersecurity
Issue No. 13
October 2012

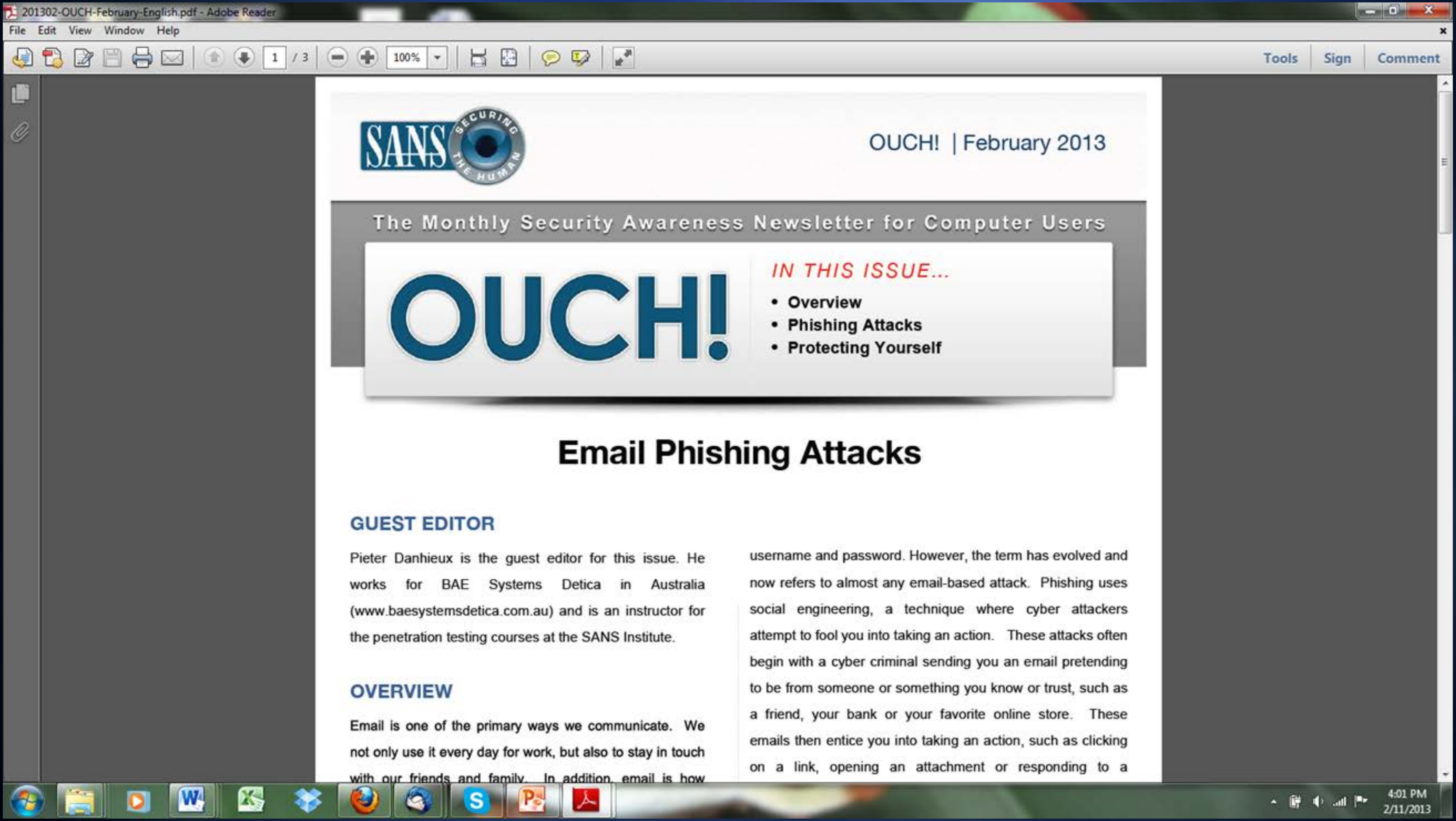
National Cybersecurity Awareness Month
October 2012

The Department of Energy is joining forces with the Department of Homeland Security and other Federal and State agencies and private industry to recognize October 2012 as National Cybersecurity Awareness Month (NCSAM). The primary goal of NCSAM is to engage and educate the public, private, and Federal sectors about cyber risks in an effort to increase the resiliency of the Nation against cyber incidents. The following is a message from our Associate Chief Information Officer (ACIO) for Cybersecurity, Mr. Gil Vega.

As the Department's Chief Information Security Officer, I would like to take a moment to discuss the critical role that cybersecurity plays in our daily lives – both at work and at home. The technology that has greatly enhanced our lives with immediate access to resources and communication tools has also exposed us to tremendous adversarial threats such as identity thieves that attempt to steal our personal information or terrorists that desire to destroy our Nation's infrastructure. In addition, we are more interconnected than ever before. From the kitchen table to the classroom, from business transactions to essential government operations and services, cybersecurity is an issue that touches all of us on a daily basis. Yet for all of its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. No country, industry, community, or individual is immune to cyber risks.

*National Cybersecurity Awareness Month reminds us that being safer and more secure online is a shared responsibility. In other words, during the month of October we pay special attention to "**Achieving Cybersecurity Together**." Each of us has an important role to play in securing our personal and professional cyberspace. Individual actions have a collective impact, and safe use of the Internet makes it more secure for everyone. If all Americans do their part by implementing stronger security practices, raising community awareness, educating young people and training employees, together we can foster a literate, resilient, and secure online society.*

NATIONAL CYBERSECURITY ALLIANCE


201302-OUCH-February-English.pdf - Adobe Reader
File Edit View Window Help
1 / 3
100%
Tools
Sign
Comment
4:01 PM
2/11/2013

OUCH! | February 2013

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE…

- Overview
- Phishing Attacks
- Protecting Yourself

Email Phishing Attacks

GUEST EDITOR

Pieter Danhieux is the guest editor for this issue. He works for BAE Systems Detica in Australia (www.baesystemsdetica.com.au) and is an instructor for the penetration testing courses at the SANS Institute.

OVERVIEW

Email is one of the primary ways we communicate. We not only use it every day for work, but also to stay in touch with our friends and family. In addition, email is how

username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a

ITWD Insights - December 2012

ITWD
IT WORKFORCE DEVELOPMENT

ITWD Insights text only

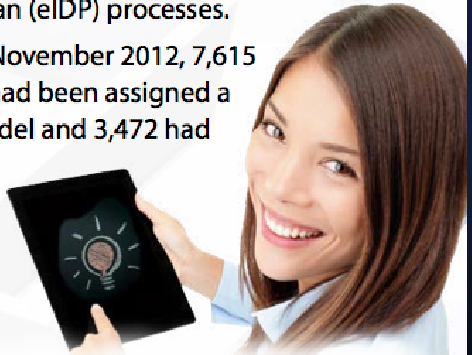
Competency Models – A Look Back at 2012

ITWD's vision of creating an environment of learning excellence has driven the organization's efforts over the last 12 months. 2012 has been a year of growth and change for ITWD, and the results have been a stronger, better training program for the IT professionals in VA's Office of Information Technology.

The OIT competency model program plays an instrumental role in accomplishing ITWD's mission of preparing VA's information technology professionals to better serve our nation's Veterans through the delivery of targeted, competency-based skills and development programs. By the end of 2012, ITWD will have released a total of 13 competency models to the IT workforce.

Throughout the year ITWD built on the success of existing competency models such as the Information Security Officer (ISO) Competency Model, Supervisor Competency Model and Software Developer Competency Model to implement additional role-based models for Internet, Network Security Operations Center, IT Project and Program Managers, Operating Systems, Systems Analysis, Data Mangers, Network Administrators, Systems Administrators, Customer Support and Enterprise Architect professionals. Incorporating feedback from the field, ITWD also worked with various groups within OIT to review and streamline the competencies included in the Core Competency Model. Core competencies are part of all models and are relevant to all roles—enhancing and simplifying the self-assessment and electronic individual development plan (eIDP) processes.

By the end of November 2012, 7,615 OIT employees had been assigned a competency model and 3,472 had completed their self-assessments in the Talent Management System (TMS).



continued page 3 .....A Look Back at 2012

from ITWD

DEPARTMENT OF EDUCATION · UNITED STATES OF AMERICA

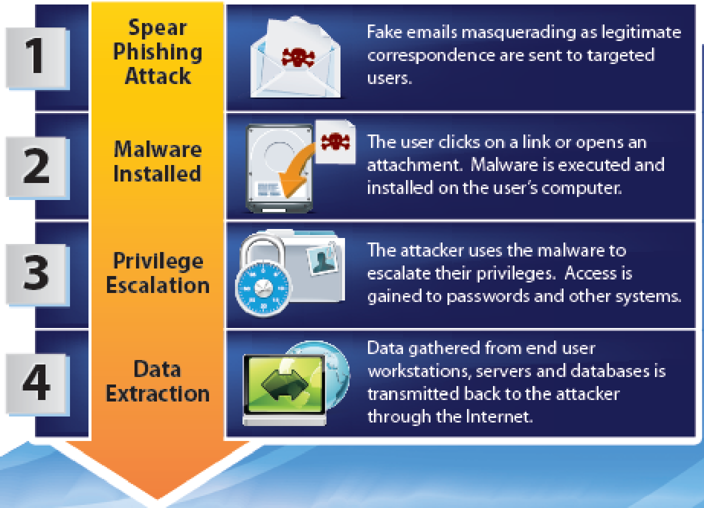
Info Security News

March 2013

In today's busy world we are more interconnected than ever before and are in constant communication with others. Email, messaging and even social networking have become the norm. Yet, for all its advantages, these methods of connecting and communicating can increase your vulnerability to cyber-attacks. One common attack, spear phishing, uses fake emails which masquerade as legitimate correspondence to convince recipients in a targeted organization to provide confidential information which may result in a data breach. For example, the email message might appear as if it came from your supervisor, human resources, the IT department, or from another government agency, or an association. Spear phishing can place you, the Department of Education (ED) and others at risk.

Let's look at the following realistic, yet fictitious scenario to learn more about how spear phishing attacks can happen.

It started out just like any other day. After arriving at the office, you log on to the network and check your email. As you go through your email, you come across one from the Department's Office of the Inspector General (OIG) with the subject line of "Final Request – Attention Required." The body of the email states that you had failed to respond to their first request for information and that a response back was required before the end of the week. That's odd, you don't remember getting the first email. You decide to click the embedded link and provide the basic information on your project to their SharePoint site. After all, you don't want to risk creating a finding in an audit report. That afternoon you notice that your computer is running really slow and you can't seem to get anything done. After opening a ticket with the Help Desk, the Department's IT team determines that your computer is running malware and that it may have spread further into the network. Oh, no….



1 **Spear Phishing Attack** — Fake emails masquerading as legitimate correspondence are sent to targeted users.

2 **Malware Installed** — The user clicks on a link or opens an attachment. Malware is executed and installed on the user's computer.

3 **Privilege Escalation** — The attacker uses the malware to escalate their privileges. Access is gained to passwords and other systems.

4 **Data Extraction** — Data gathered from end user workstations, servers and databases is transmitted back to the attacker through the Internet.

A VIEW TO A SPILL

Newsletter Winner!

Deborah Coleman

Organization:
The Department of Education, Office of the Chief Information Officer

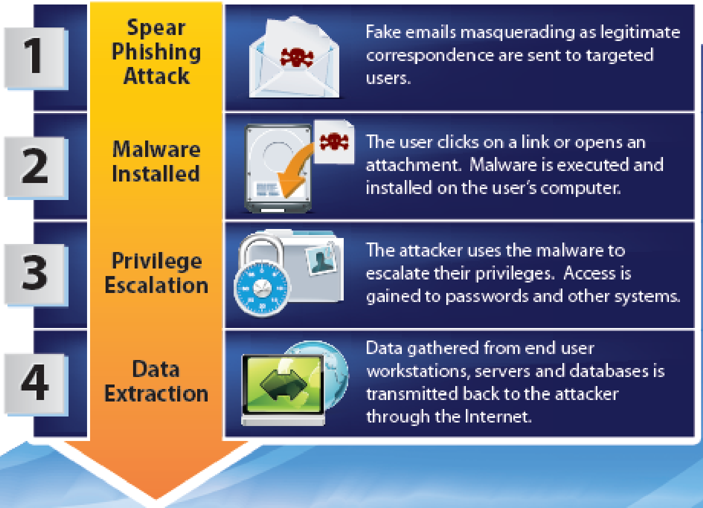
Info Security News

March 2013

In today's busy world we are more interconnected than ever before and are in constant communication with others. Email, messaging and even social networking have become the norm. Yet, for all its advantages, these methods of connecting and communicating can increase your vulnerability to cyber-attacks. One common attack, spear phishing, uses fake emails which masquerade as legitimate correspondence to convince recipients in a targeted organization to provide confidential information which may result in a data breach. For example, the email message might appear as if it came from your supervisor, human resources, the IT department, or from another government agency, or an association. Spear phishing can place you, the Department of Education (ED) and others at risk.

Let's look at the following realistic, yet fictitious scenario to learn more about how spear phishing attacks can happen.

It started out just like any other day. After arriving at the office, you log on to the network and check your email. As you go through your email, you come across one from the Department's Office of the Inspector General (OIG) with the subject line of "Final Request – Attention Required." The body of the email states that you had failed to respond to their first request for information and that a response back was required before the end of the week. That's odd, you don't remember getting the first email. You decide to click the embedded link and provide the basic information on your project to their SharePoint site. After all, you don't want to risk creating a finding in an audit report. That afternoon you notice that your computer is running really slow and you can't seem to get anything done. After opening a ticket with the Help Desk, the Department's IT team determines that your computer is running malware and that it may have spread further into the network. Oh, no….



1 Spear Phishing Attack — Fake emails masquerading as legitimate correspondence are sent to targeted users.

2 Malware Installed — The user clicks on a link or opens an attachment. Malware is executed and installed on the user's computer.

3 Privilege Escalation — The attacker uses the malware to escalate their privileges. Access is gained to passwords and other systems.

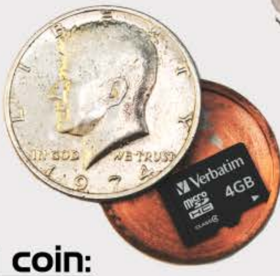
4 Data Extraction — Data gathered from end user workstations, servers and databases is transmitted back to the attacker through the Internet.

A VIEW TO A SPILL

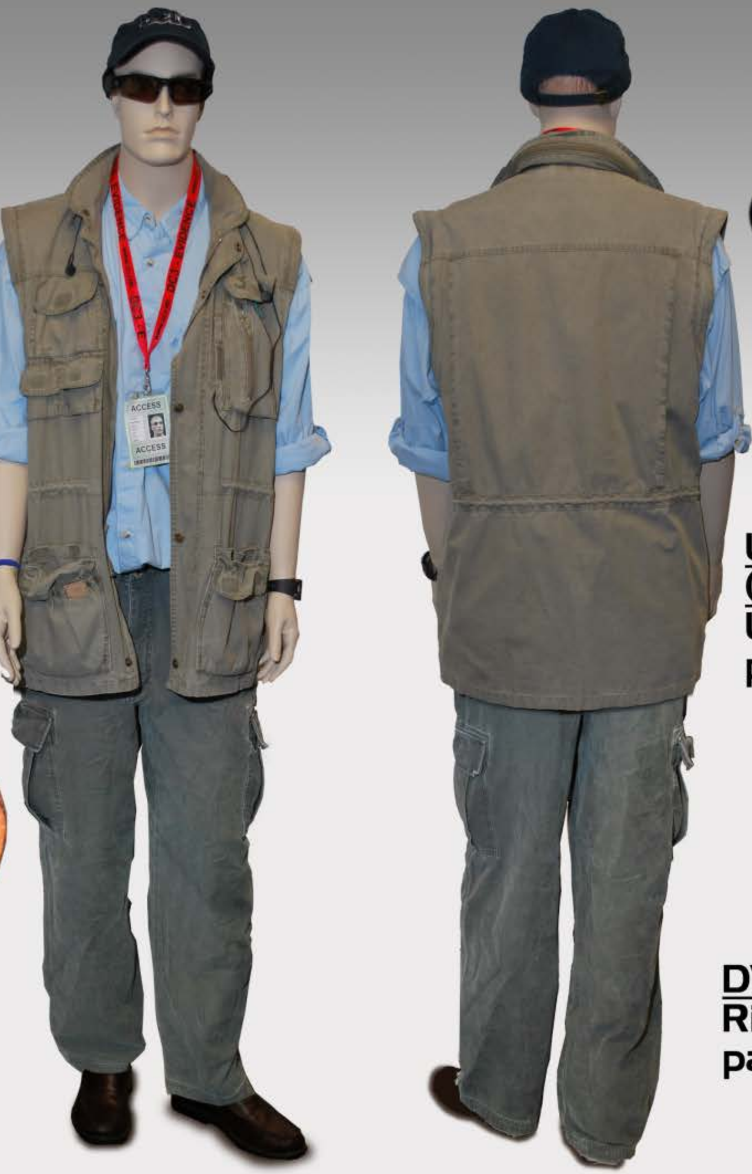
Training Entries (6)

C4 Crime Case Evidence Map

USB PEN:
Clipped on top
right vest pocket



Spy coin:
Right hand pants
pocket



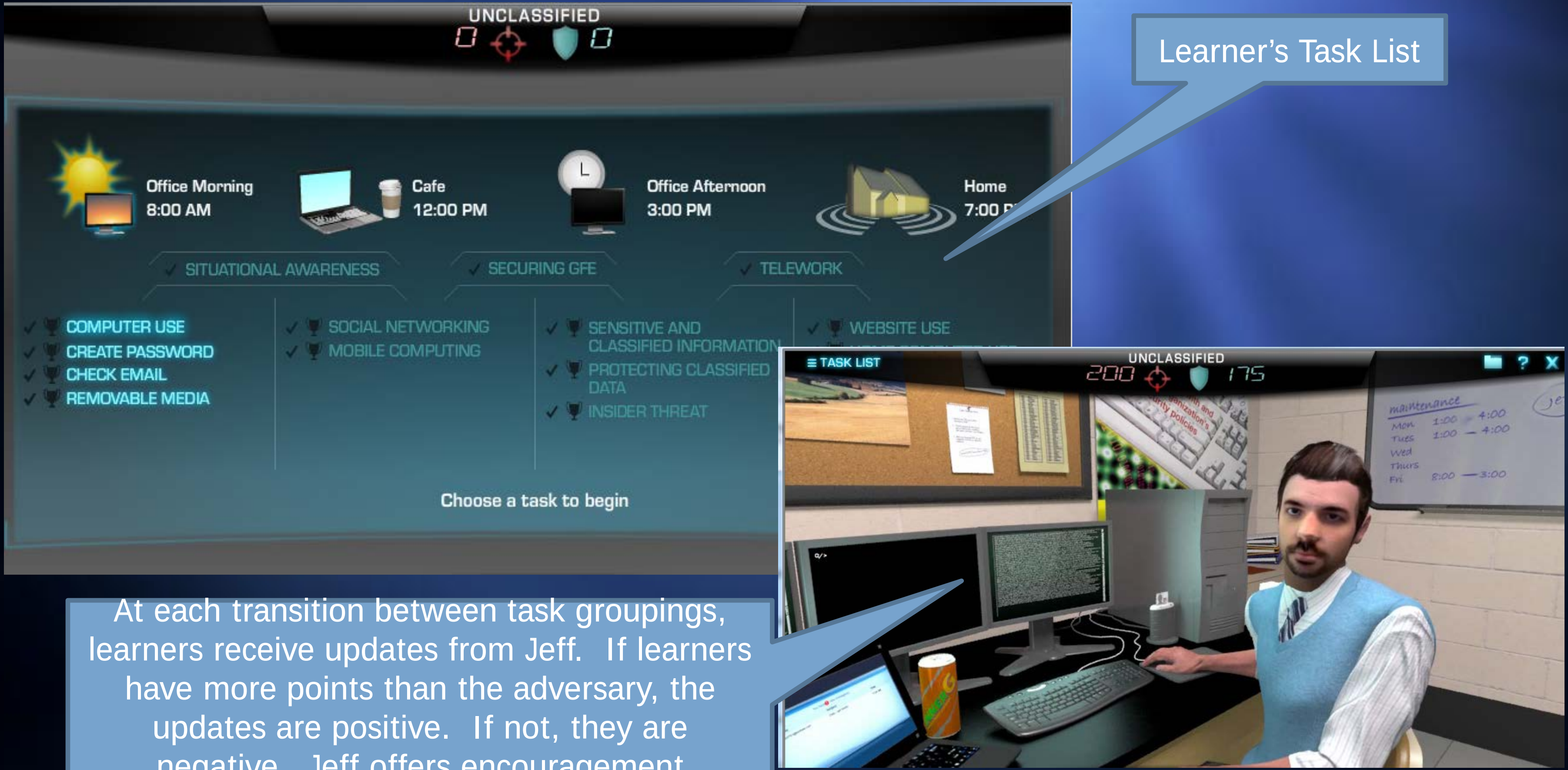
USB Wristband:
Left wrist

Lego USB
(on keychain):
Left hand
pants pocket

DVD:
Right cargo
pants pocket

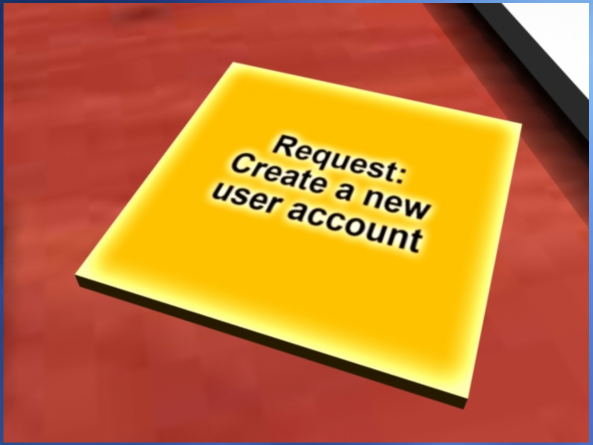
The player's learning is measured through the completion of the series of tasks structured around a "typical workday" that make up the game. These tasks are divided into four groupings by time of day and environment and cover all information assurance content required and approved by DISA.

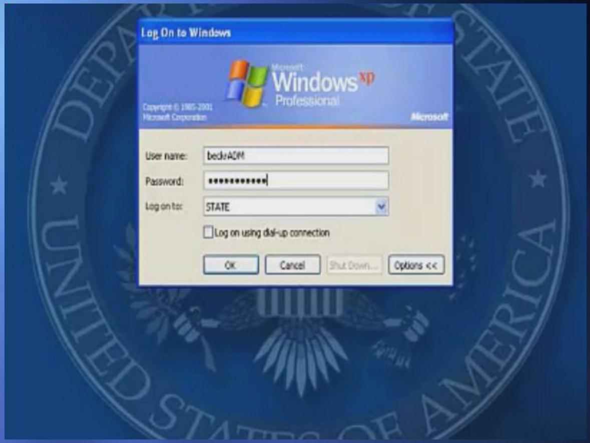
For each task, the learner completes some combination of activities made up of either a simulation or a mini-game. In simulations, the learners are presented with a scenario in which they must select the best course of action to protect information systems and sensitive information. In mini-games, learners apply information assurance concepts in a fun and interactive context.



Learner's Task List

At each transition between task groupings, learners receive updates from Jeff. If learners have more points than the adversary, the updates are positive. If not, they are negative. Jeff offers encouragement throughout to keep learners motivated and engaged.



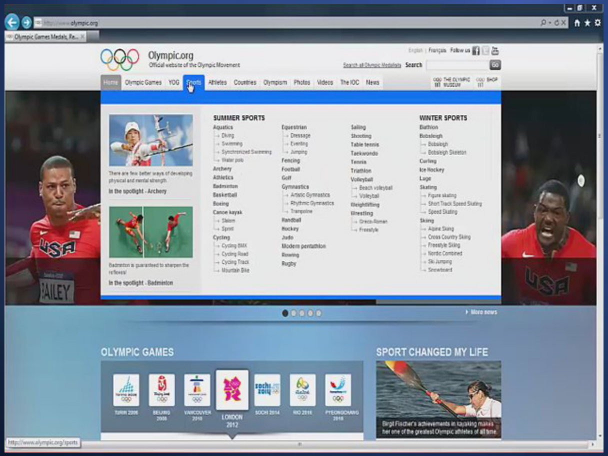


User name: beckrADM

Password: ●●●●●●●●●●●

Log on to: STATE

□ Log on using dial-up connection



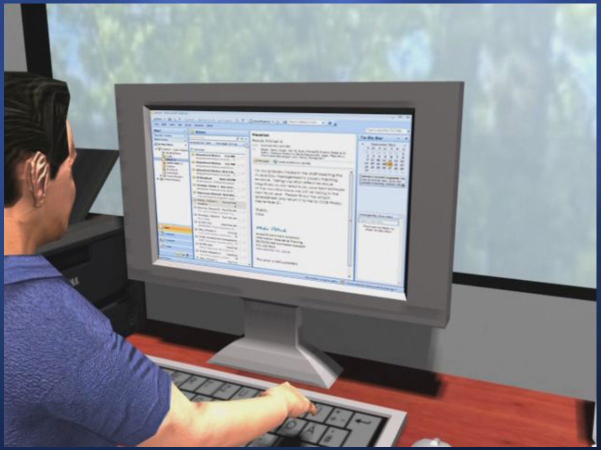
There are few better ways of developing physical and mental strength.

In the spotlight - Archery

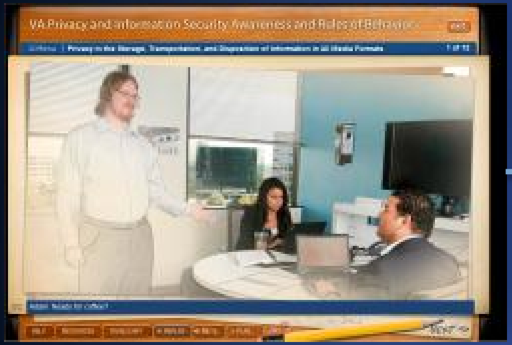
Badminton is guaranteed to sharpen the reflexes!

In the spotlight - Badminton

Birgit Fischer's achievements in kayaking makes her one of the greatest Olympic athletes of all time.

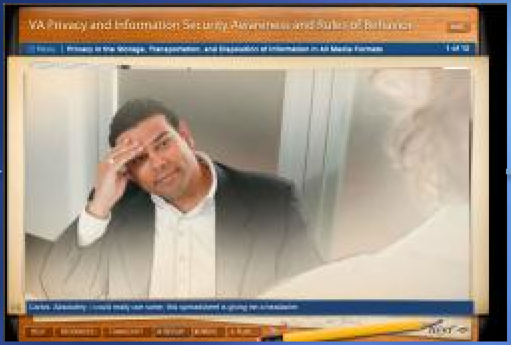


Storytelling and Scenario-based Examples


VA Privacy and Information Security Awareness and Rules of Behavior

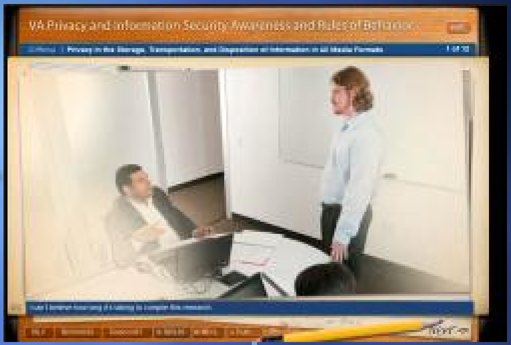
Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Adam: Ready for coffee?


VA Privacy and Information Security Awareness and Rules of Behavior

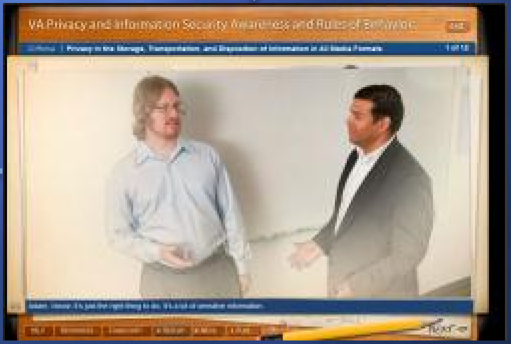
Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Carlos: Absolutely. I could really use some, this spreadsheet is giving me a headache.


VA Privacy and Information Security Awareness and Rules of Behavior

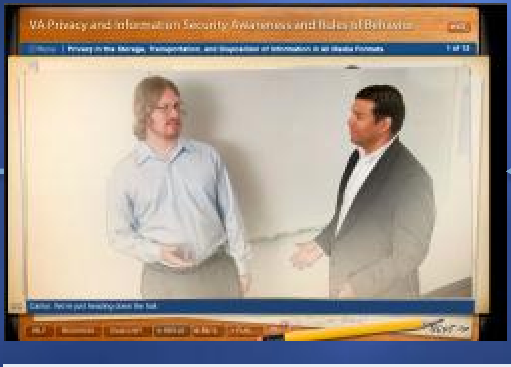
Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

I can't believe how long it's taking to compile this research.


VA Privacy and Information Security Awareness and Rules of Behavior

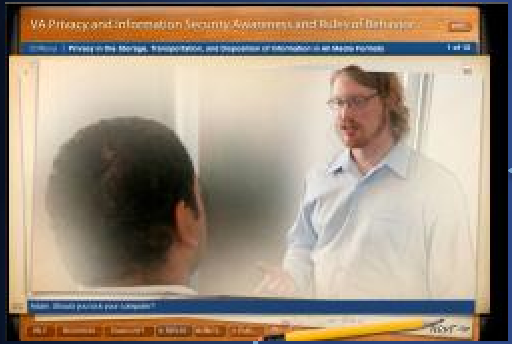
Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Adam: I know, it's just the right thing to do. It's a lot of sensitive information.


VA Privacy and Information Security Awareness and Rules of Behavior

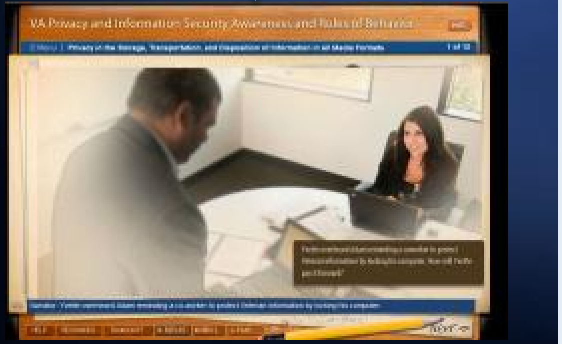
Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Carlos: We're just heading down the hall.


VA Privacy and Information Security Awareness and Rules of Behavior

Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Adam: Should you lock your computer?


VA Privacy and Information Security Awareness and Rules of Behavior

Privacy in the Storage, Transportation, and Disposition of Information in All Media Formats

Yvette overheard Adam reminding a coworker to protect Veteran information by locking his computer. How will Yvette pay it forward?

Narrator: Yvette overheard Adam reminding a co-worker to protect Veteran information by locking his computer.

Transcript

Adam: Ready for coffee?

Carlos: Absolutely. I could really use some, this spreadsheet is giving me a headache. I can't believe how long it's taking to compile this research.

Adam: Should you lock your computer?

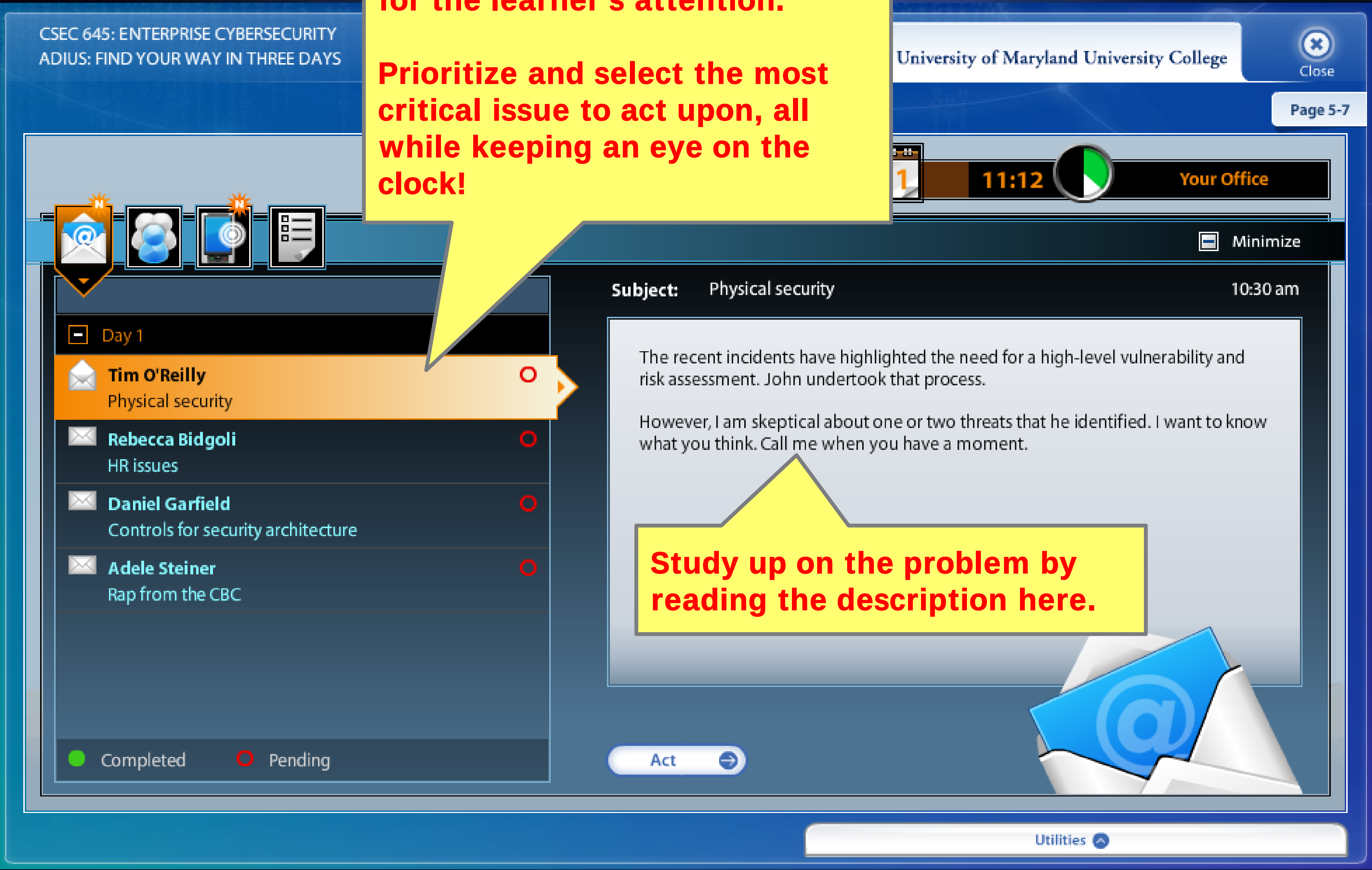
Carlos: We're just heading down the hall.

Adam: I know, it's just the right thing to do. It's a lot of sensitive information.

Narrator: Yvette overheard Adam reminding a coworker to protect Veteran information by locking his computer. How will Yvette pay it forward?

There are multiple events vying for the learner's attention.

Prioritize and select the most critical issue to act upon, all while keeping an eye on the clock!



CSEC 645: ENTERPRISE CYBERSECURITY
ADIUS: FIND YOUR WAY IN THREE DAYS

University of Maryland University College

Day 1

Tim O'Reilly Physical security	○	
Rebecca Bidgoli HR issues	○	
Daniel Garfield Controls for security architecture	○	
Adele Steiner Rap from the CBC	○	

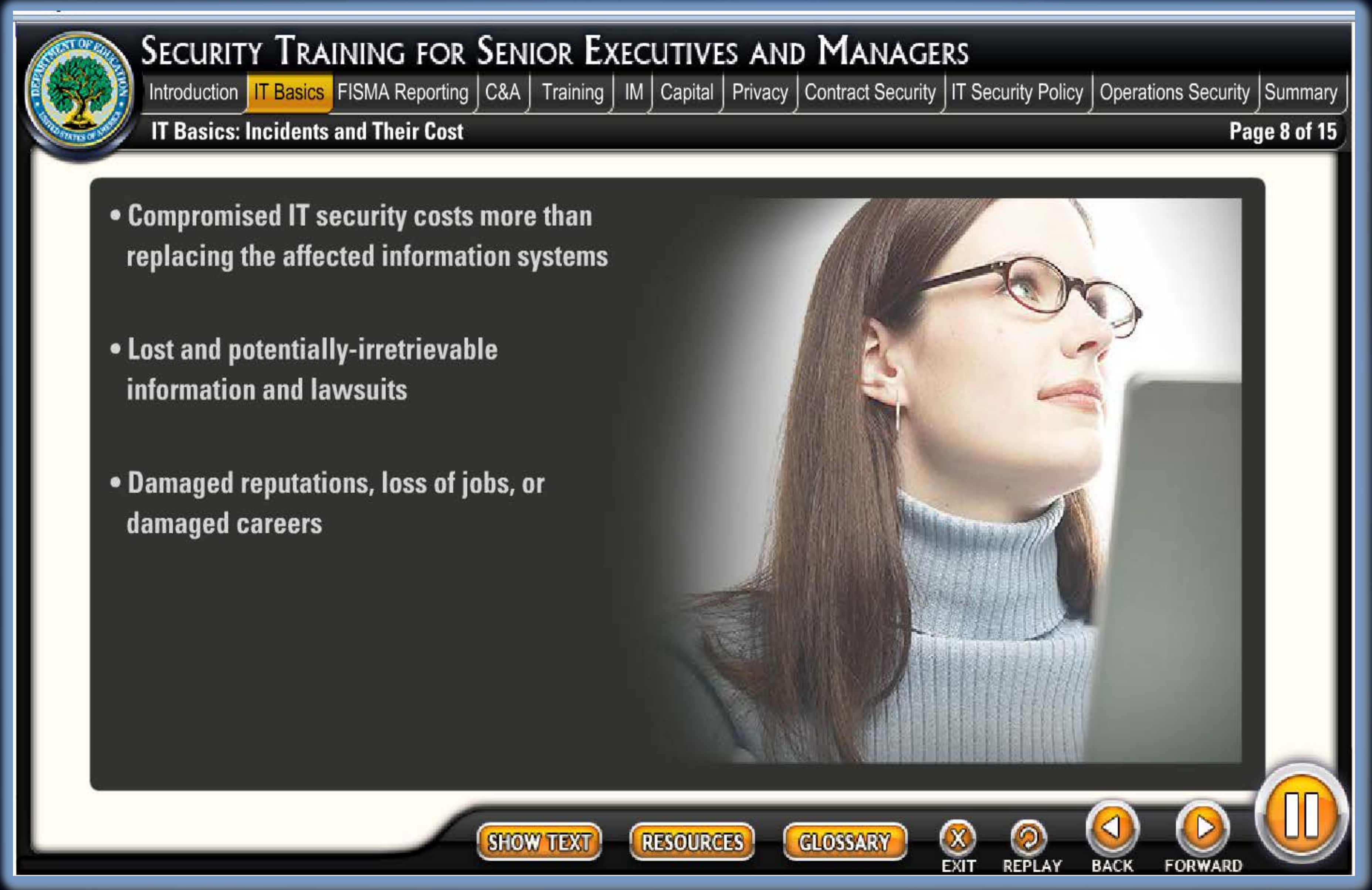
● Completed ○ Pending

Subject: Physical security 10:30 am

The recent incidents have highlighted the need for a high-level vulnerability and risk assessment. John undertook that process.

However, I am skeptical about one or two threats that he identified. I want to know what you think. Call me when you have a moment.

Study up on the problem by reading the description here.



Security Training for Senior Executives and Managers

IT Basics: Incidents and Their Cost

Page 8 of 15

- Compromised IT security costs more than replacing the affected information systems
- Lost and potentially-irretrievable information and lawsuits
- Damaged reputations, loss of jobs, or damaged careers

Upon completion of this course, Senior Executives and Managers should be able to: explain the importance of IT security; identify the possible impact of a security breach; list their responsibilities as a senior executive or manager; recognize key security acts and legislation that affect the Department's IA processes; recall crucial federal security standards; identify the purpose and importance of the Authorization & Accreditation (C&A) process; and recount key IT security Department policies, procedures, and training initiatives.

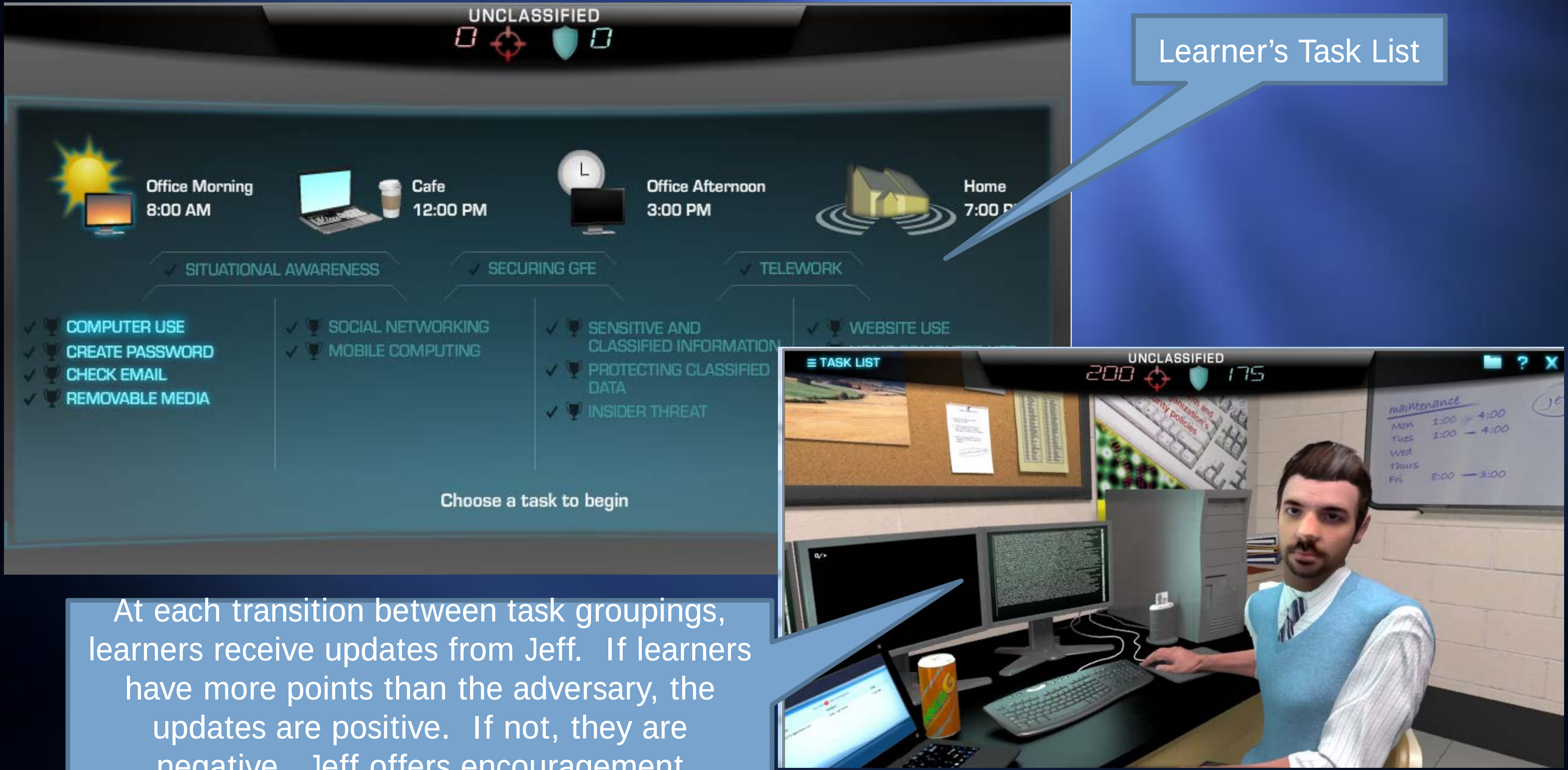
Training Winner!

DISA, SAIC, and Carney, Inc.

Name of submitter:
Carmen Carper

The player's learning is measured through the completion of the series of tasks structured around a "typical workday" that make up the game. These tasks are divided into four groupings by time of day and environment and cover all information assurance content required and approved by DISA.

For each task, the learner completes some combination of activities made up of either a simulation or a mini-game. In simulations, the learners are presented with a scenario in which they must select the best course of action to protect information systems and sensitive information. In mini-games, learners apply information assurance concepts in a fun and interactive context.



UNCLASSIFIED

0 0

Office Morning
8:00 AM

Cafe
12:00 PM

Office Afternoon
3:00 PM

Home
7:00 P

✓ SITUATIONAL AWARENESS

✓ SECURING GFE

✓ TELEWORK

✓ COMPUTER USE
✓ CREATE PASSWORD
✓ CHECK EMAIL
✓ REMOVABLE MEDIA

✓ SOCIAL NETWORKING
✓ MOBILE COMPUTING

✓ SENSITIVE AND CLASSIFIED INFORMATION
✓ PROTECTING CLASSIFIED DATA
✓ INSIDER THREAT

✓ WEBSITE USE

Choose a task to begin

≡ TASK LIST

UNCLASSIFIED

200 175

Learner's Task List

At each transition between task groupings, learners receive updates from Jeff. If learners have more points than the adversary, the updates are positive. If not, they are negative. Jeff offers encouragement throughout to keep learners motivated and engaged.

Peer's Choice Awards

- Part of the Poster Session on Thursday
  - Stop by and see all the entries and descriptions up close
  - Vote for your favorites (1 from each category)
  - Winners will be announced during the closing session Thursday
  - 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!