



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

September 15, 2010



# ISOAG September 2010 Agenda

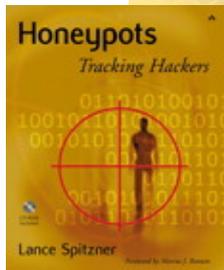
- |      |   |                      |
|------|---|----------------------|
| I.   | Welcome & Opening Remarks                                 | John Green, VITA     |
| II.  | Securing the Human  | Lance Spitzner, SANS |
| III. | Social Engineering: Building Bridges to Confidential Data | Bob Baskette, VITA   |
| IV.  | Scareware: Taking Computers Hostage                       | Eric Taylor, NG      |
| V.   | 2010 COV Security Annual Report                           | John Green, VITA     |
| VI.  | Upcoming Events & Other Business                          | John Green, VITA     |
| VII. | Partnership Update  | Don Kendrick, VITA   |

SANS

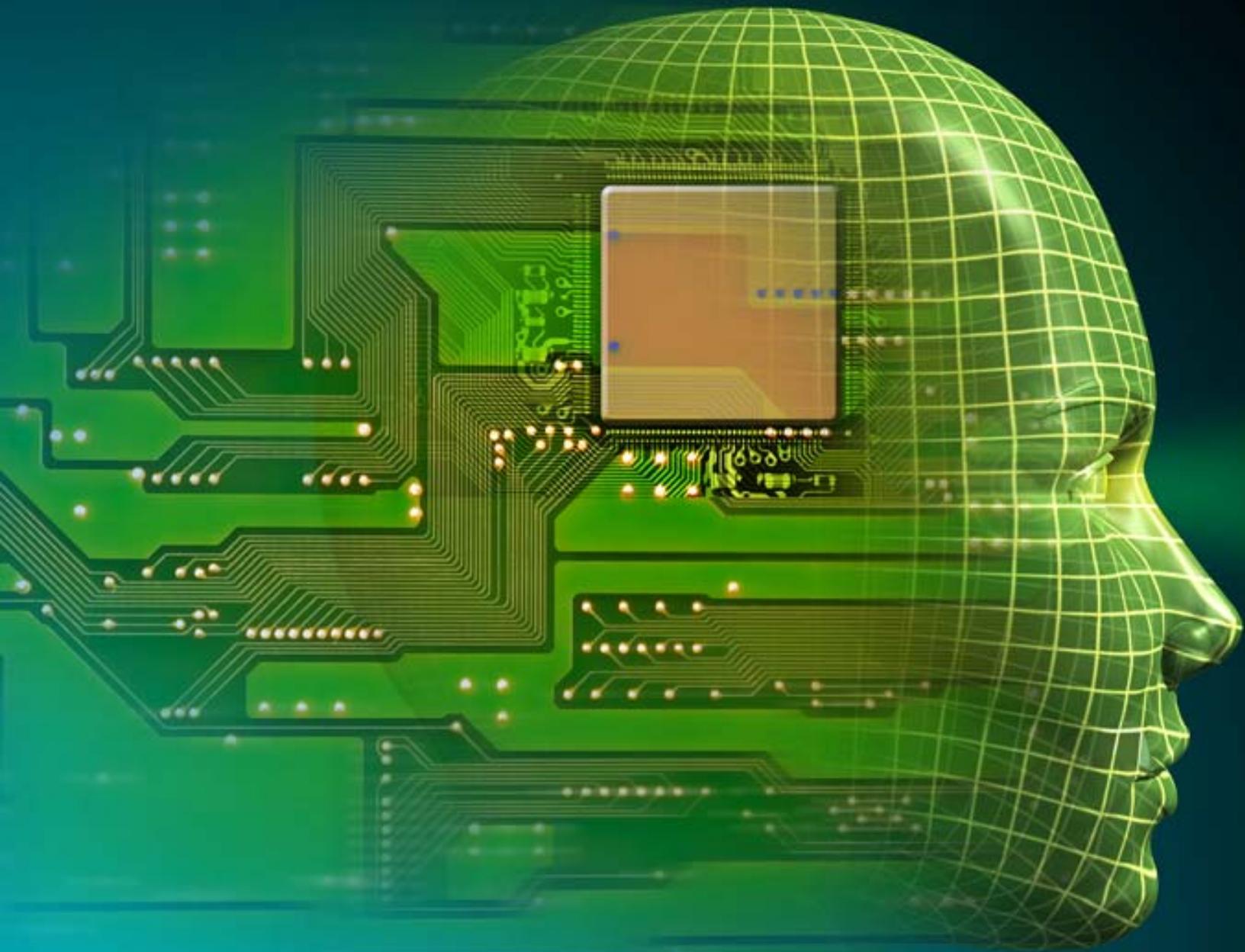


# ***SECURING* THE HUMAN**



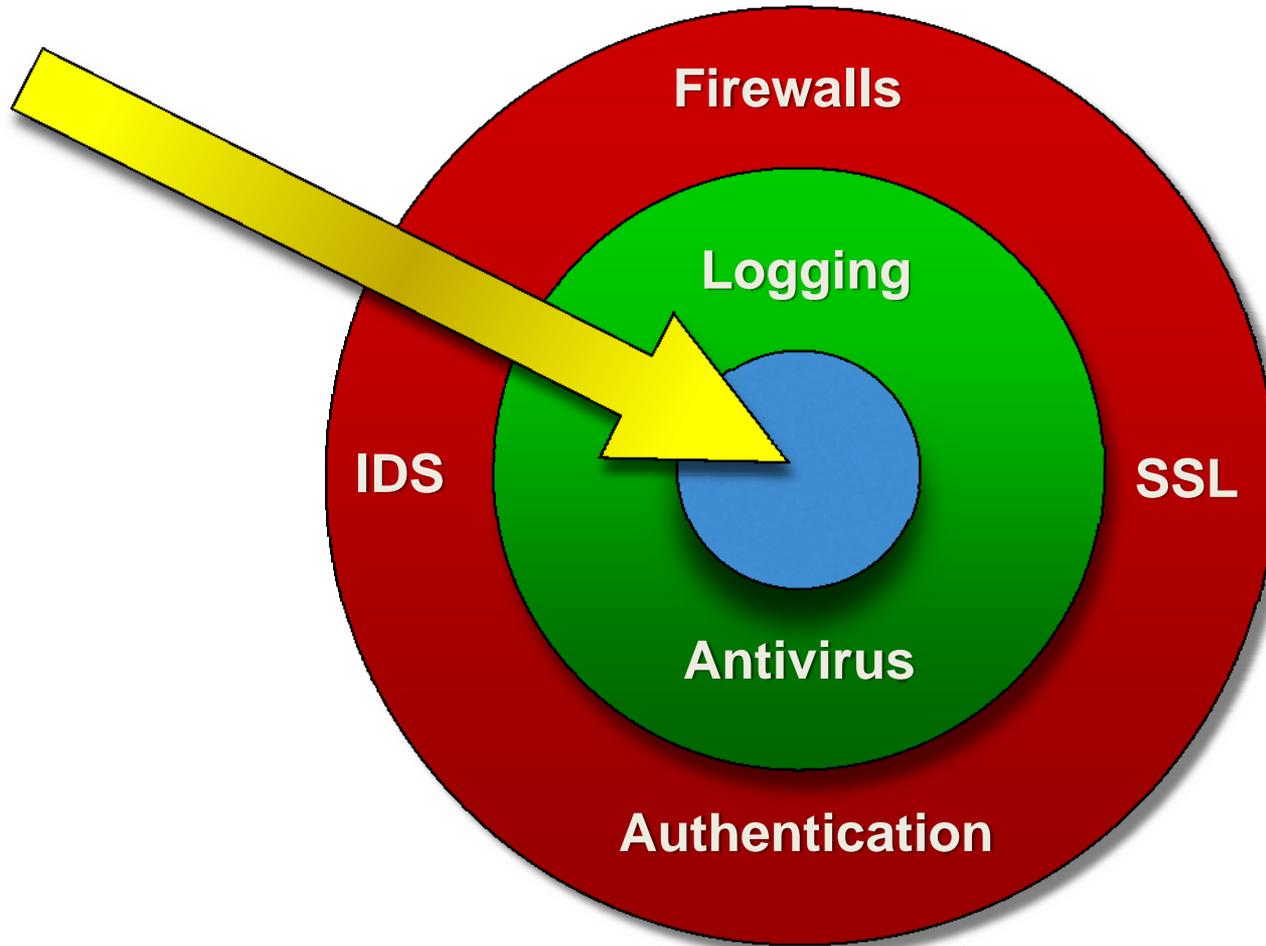






# Numbers

- Symantec – 90% of malware requires human interaction.
- Mandiant – 100% of successful APT attacks compromised the human.



# Bad At Judging Risk

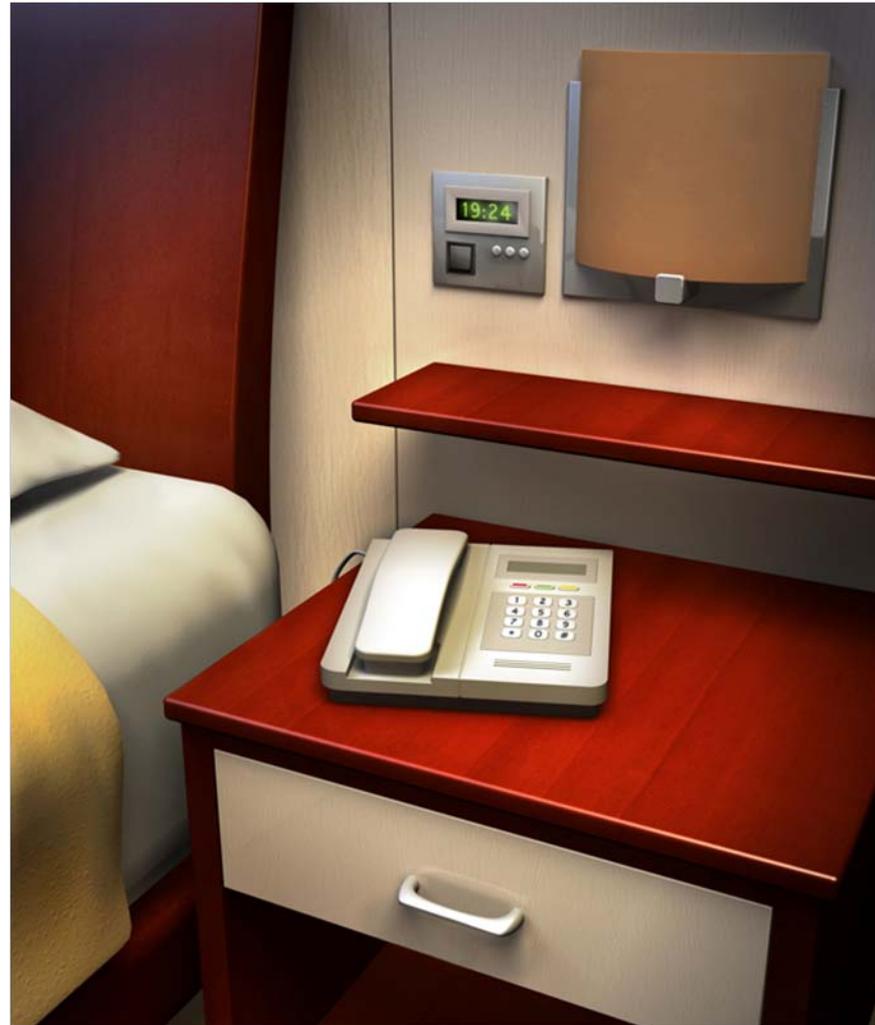
- Humans over estimate visual risks.
- Humans over estimate risk when not in control.



1 in 251,800,000



1 in 112,000,000



\*\*\*\*\*

URGENT SYSTEM SCAN NOTIFICATION ! PLEASE READ CAREFULLY !!

<http://www.systemdetect.net/>

For the link to become active, please click on 'Add to contacts' skype button or type it in manually into your web browser !

FULL DETAILS OF SCAN RESULT BELOW

\*\*\*\*\*

WINDOWS REQUIRES IMMEDIATE ATTENTION

ATTENTION ! Security Center has detected  
malware on your computer !

Affected Software:

- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows Server 2003

Impact of Vulnerability: Remote Code Execution / Virus Infection /  
Unexpected shutdowns

Recommendation: Users running vulnerable version should install a repair utility immediately

Your system IS affected, download the patch from the address below !  
Failure to do so may result in severe computer malfunction.

<http://www.systemdetect.net/>

For the link to become active, please click on 'Add to contacts' skype button or type it in manually into your web browser !

**System Tasks**

- View system information
- Add or remove programs
- Change a settings

**Other Places**

- My Network Places
- My Documents
- Shared Documents
- Control Panel

**Details**

**My Computer**  
System Folder

Local Disk (C:) Security threat

Local Disk (D:) Security threat

DVD-RAM Drive (E:)

Shared Documents Security threat

100% files - System scan

Total files 5292

**WARNING! Spyware**

Your Computer is Infected!

- C:\Documents and Settings\use
- C:\Documents and Settings\use
- C:\Documents and Settings\use
- C:\Documents and Settings\use
- C:\WINDOWS\Temp\Temporary

Full system cleanup

**WARNING!!!** Scan results

**WARNING!** Windows has been infected

Name	Type	Alert level
System Soap Pro	Spyware	Avarage
AntiLamer Light	Spyware	Avarage
MC 30 Day	Spyware	Danger
SoftEther	Spyware	High
I-Worm.NetSky.q	Virus	High
I-Worm.Bagle.n	Virus	High
Tofger-A	Virus	Critical
Zinx-A	Spyware	Critical
B-5 Spy 1.90	Spyware	Critical
KrAIMer 1.1	Virus	Critical

**Warning!!! 364 infected files found**

Click the "Erase all threats" button to erase all spyware and viruses from Windows

**Erase all threats**

**Security errors detected**

Click here to view errors list.  
Remove this errors as soon as possible to prevent data lost and privacy information exposure

Repair Registry 2008 - Repair Registry 2008

US \$19.95

1

Instant Download!

US \$19.95

### Why are Digital Downloads Green?

\*After you change any quantities, be sure to click the "Update Cart" button.

update cart

Sub Total

US \$19.95

#### Billing Information

This is the address that your billing information is sent to.

Shipping Address is same as Billing Address

E-mail Address:

First Name:

Last Name:

Company:

Street 1:

Street 2:

City:

State/Province:

Zip/Postal code:

Country:

Phone:

#### Payment Information



CREDIT CARD online now

CREDIT CARD by FAX CREDIT CARD by PHONE PAYPAL Electronic Funds Transfer with Proforma Invoice\* Wire Transfer with Proforma Invoice\* CHECK with Proforma Invoice\*

Card Number:

Expiration Date:

Card Security Code:

Issue Number:

 (Maestro only)

Start Date:

 (Maestro only)

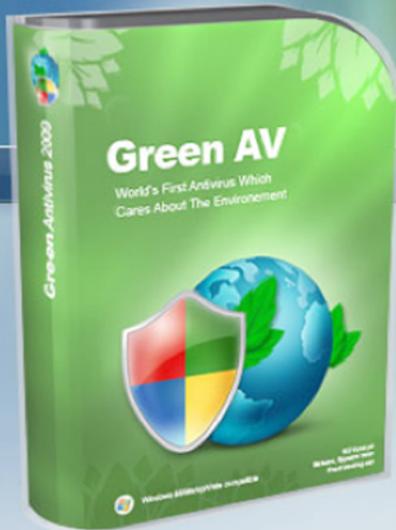
SWREG and the publisher of this product would like to keep you



Highest level of shopping safety!

Shop with confidence knowing that you are totally protected when you order through any SWReg network member.





## Green AV Professional License



Secure SSL Connection  
100% Privacy Guarantee

Protect your PC and join our green movement

5 345 users worldwide trust us. Their stories are...

Buy Green AV today and make your contribution to Environmental care program. We have already raised:



**\$ 12 789, 1234**  
and counting... Join!



Protect your PC with innovative technology and prevent further infection.



100% remove of malicious software, viruses, spyware, malware etc.



Removes suspicious files, Facebook and MySpace account stealers.



Protect personal information from phishing.



Protect E-mail correspondence, addressbook stealing, spam abuse.



Environment care program.  
\$2 from every sale we make will be sent on saving green forests in Amazonia.



Denis Kelmerin

26 years  
web-developer  
NY

“ I can trust Green AV to protect my PC. I know that creating really good antivirus - is a tough a challenge, and Green AV Team did it. ”



Anne Tartari

34 years  
teacher, housewife  
LA

“ I think the Environmental program was maybe the strongest reason. There are many antiviruses, and they all are great i suppose. But I share the idea of environmental care and try to support it whatever it is. It looks simple - just 2 dollars, but it's a good new start! ”



Fully Secure & Encrypted Ordering -  
Even Safer Than Over the Phone.



TRUSTe

Your Email Address and Personal  
Information are private  
and NEVER resold.



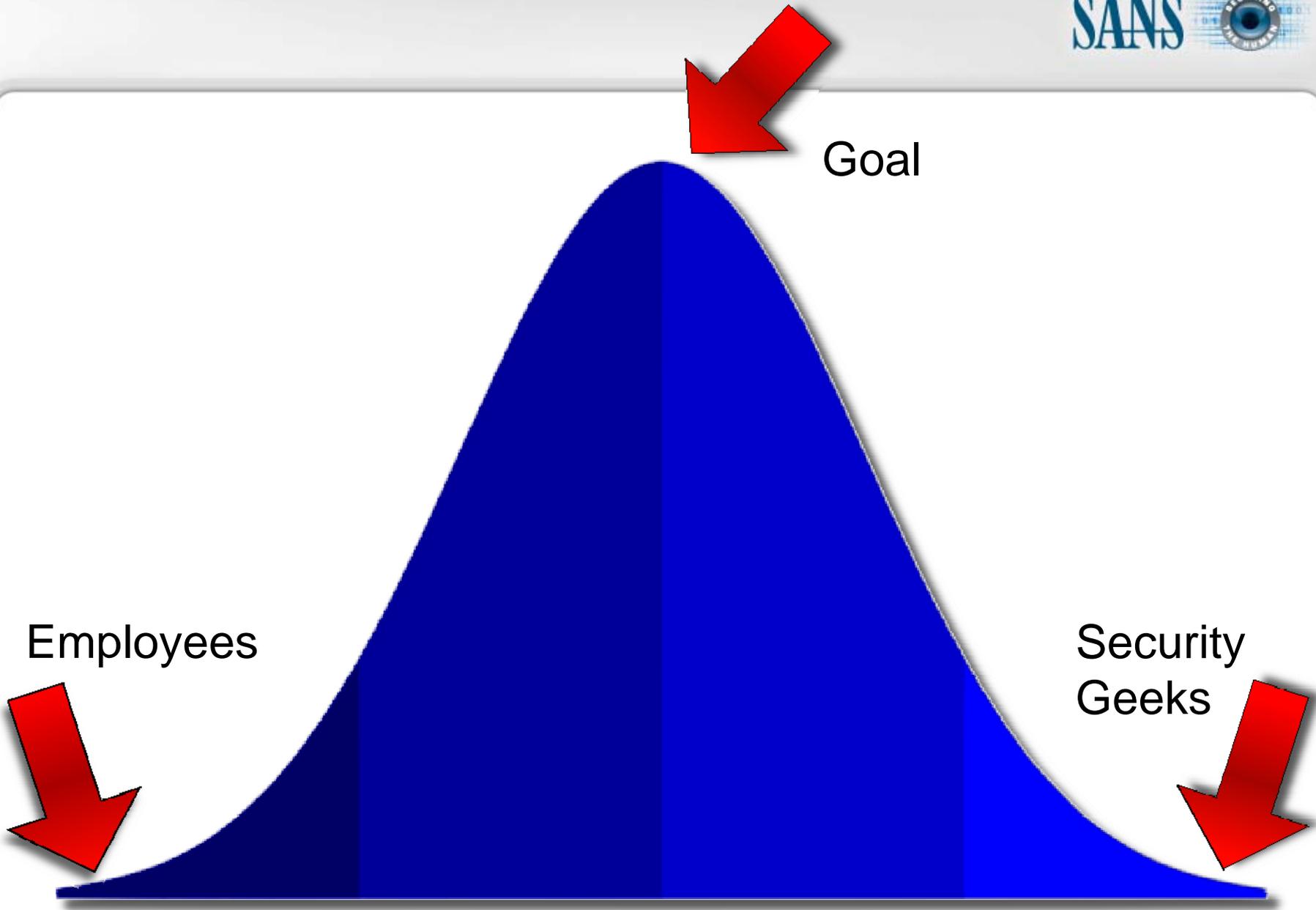
Retail price

**\$99,99**

**Buy now**

100% money back guarantee

# ***WHAT WORKS ...*** **AND WHAT DOESN'T**



Employees

Goal

Security Geeks

# Before You Start

- Why?
- Who is in charge?

# The Plan

- WHO
- WHAT
- HOW

# Who

- Employees
- Management
- IT Staff
- Customers

# WHAT

- Prioritize – fewest topics with greatest ROI.

# HOW

- Often hardest part.
- Think like marketing, not security.

[NEWS](#)
[SEARCH CARDS](#)
[SUPPORT TICKETS](#)
[PAYMENTS](#)
[EXIT](#)
**satu96**

 Shopping cart:  
 0 item(s).  
 0 rubles

 Account balance:  
 5 rubles

 Account status:  
 USER

**Your account**
[Your cards \(0\)](#)
[Payments](#)
[Personal info](#)
**Information**
[FAQ / Help](#)
[BIN List](#)
[Flags of the World](#)
[World Country](#)
[Information](#)
[ISO 3166 Country](#)
[Code List](#)
**CARDS**

Searching by BINs: , CVV2: , City: atlanta, State: , Zip: , Country: .

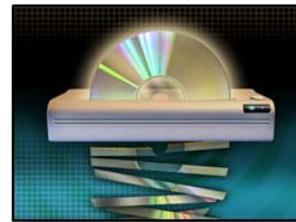
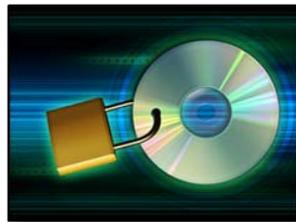
[REFINE SEARCH](#)

NN	PAN	CVV2	EXP/DATE	NAME	ADDRESS	CITY	STATE	ZIP	COUNTRY	PHONE	PRICE	<input type="checkbox"/>
1	4356190#####	###	07/10		#### Greencrest Dr. NE	Atlanta	GA	30345	US	6785#####	35.00	<input type="checkbox"/>
2	3715653#####	####	05/10		### Peachtree Street NE ####	Atlanta	GA	30303	US	4048#####	35.00	<input type="checkbox"/>
3	4465610#####	###	11/10		#### Wieuca RD NE	Atlanta	GA	30342	US	4042#####	35.00	<input type="checkbox"/>
4	4357970#####	###	09/11		#### Dresden Dr.	Atlanta	GA	30319	US	4045#####	35.00	<input type="checkbox"/>
5	3728136#####	####	10/08		#### Cedar Canyon Dr., NE	Atlanta	GA	30345	US	4046#####	35.00	<input type="checkbox"/>
6	3712871#####	####	04/09		P.O. Box #####	Atlanta	GA	30356	US	6783#####	35.00	<input type="checkbox"/>
7	5446792#####	###	05/10		#### paul ave. nw	atlanta	GA	30318	US	4047#####	35.00	<input type="checkbox"/>
8	4356190#####	###	04/10		#### Boulder Rd. SE	Atlanta	GA	30316	US	404-54#-####	35.00	<input type="checkbox"/>





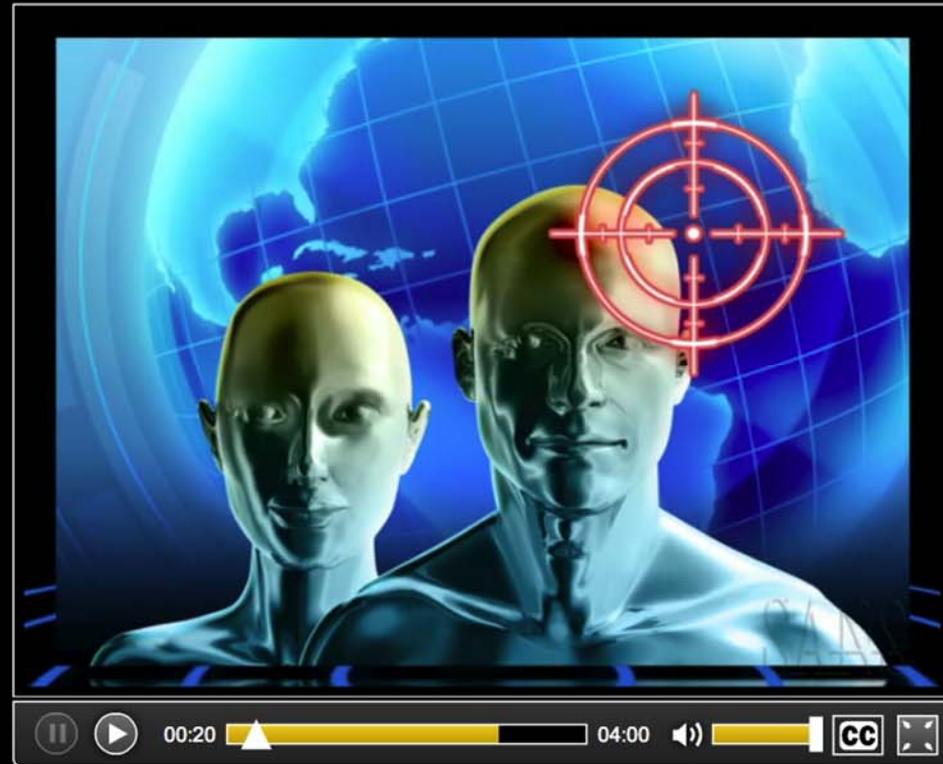




## Security Awareness For Employees



1 - YOU ARE THE TARGET



# YOU ARE THE TARGET

Your information and your computer have tremendous value to cyber criminals. The first step to protecting yourself is understanding that you are the target.



**YOU ARE THE CYBER CRIMINAL'S TARGET**



## CYBER SECURITY

newsletter



### You Are The Target

Many people mistakenly believe that cyber criminals do not target them, that their computer or information has no value. In reality individuals like you are the cyber criminals' primary target—you and your computer are under attack every day. The first step to protecting yourself is understanding that you are a valuable target.



This newsletter is published by The SANS Institute, the world's leader in information security training. Learn how we can help secure your organization at:

[www.securingthehuman.org](http://www.securingthehuman.org)

# Customize

- Organization colors, logo & contact information
- Language
- Culture

# Summary

- Humans are another operating system.
- Employees least protected, as a result greatest risk.
- A small investment can make a huge difference.



---

[info@securingthehuman.org](mailto:info@securingthehuman.org)

<http://www.securingthehuman.org>





*Virginia Information Technologies Agency*

# Social Engineering: Building Bridges to Confidential Data

Bob Baskette

CISSP-ISSAP, CCNP/CCDP

Commonwealth Security Architect



# Social Engineering

- The use of influence and persuasion to deceive people for the purpose of obtaining information or persuading a victim to perform some action
- Based on the building of inappropriate trust relationships
- Targets Help Desk personnel, onsite employees, and contractors
- One of the most potentially dangerous attacks since it does not directly target technology



# Factors in Social Engineering

- Desire to be helpful
- Tendency to trust people
- Fear of getting in trouble
- Art of Manipulation (the ability to blend-in)



# Social Engineering Behavioral Types

- Scarcity
  - Belief that an item is in short supply
  - Commonly used by marketing
- Authority
  - Based on premise of power
- Liking
  - Based on the fact that people tend to help people they like



# Social Engineering Behavioral Types

- Consistency
  - Based on the fact that people like to be consistent
- Social Validation
  - If one person does it, others will follow
- Reciprocation
  - One good turn deserves another



# Social Engineering Attack Types

- Human-based (Person-to-Person)
- Computer-Based (Automated)



## Human-based (Person-to-Person)

- Uses the following techniques:
  - Shoulder surfing
  - Dumpster diving
  - Impersonation
  - Intimidation
  - Using third-party approval



## Human-based (Person-to-Person)

- Impersonation (Masquerading)
  - Attacker pretends to be someone else
  - Can impersonate an new employee, valid user, business client, janitor, delivery person, or mail room person
  - Attack carries a higher risk since the attacker is inside the facility perimeter

## Human-based (Person-to-Person)

- Intimidation (Posing as an important user)
  - Attacker pretends to be an important user
  - Works on the belief that it is not good to question authority
- Using third person authorization
  - Attacker convinces the victim that the attacker has approval from a third party that is an authoritative source
  - Works on the belief that most people are good and truthful



# Human-based (Person-to-Person)

- Reverse Social Engineering
  - Considered to be the most difficult type of Social Engineering attack
  - Requires a tremendous amount of preparation and skill
  - Act as help-desk or admin staff to request information
  - Can involve sabotaging the victim's equipment and then offering to fix the problem
  - Can be difficult to execute since the first step requires the sabotage of a system
  - Target could be an external utility such as a phone line
  - Deliver defective equipment and then offer to repair
    - Attach business card to toner box or laptop case



# Computer-Based (Automated)

- Phishing and Spam
- Email attachments
- Fake websites
- Pop-up messages
- Drive-by downloads
- DNS Cache poisoning
- Spoofed SSL-certificates



# SPAM

- SPAM is normally associated with e-mail spam, can be used with other electronic transmission types such as instant messaging, Usenet newsgroups, Web search engines, blogs, mobile phone messaging, Internet forums, and fax transmissions
- SPAM remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings
- Today, SPAM is increasingly sourced from “bot networks”. Many modern worms install a backdoor which allows the spammer access to the computer and use it for malicious purposes
- SPAM email-chains are still very popular promising good fortune if the chain is not broken



# Phishing Basics

- Phishing campaigns use either email or malicious web sites to solicit personal information from targeted individuals
- Attackers attempt to replicate the look and format of emails from reputable companies, government agencies, or financial institutions
- The Phishing messages appear to come from popular social networking sites, auction sites, online payment processors or IT Administrators to entice the unsuspecting public to respond
- Phishing campaigns that target specific categories or groups of users are known as Spear Phishing Campaigns



# Phishing Basics

- People respond without thinking to things that seem important
- Email subjects lines worded to create anxiety or self-doubt with subject lines such as “Do you trust her/him” or “Is she/he cheating on you” usually entice immediate action
- Email with the subjects such as “Your bank account has been suspended” or “There is a problem with your bank account” will usually get instant attention and prompt most people to click on the listed URL to determine what has happened



# Pop-up messages

- Can prompt victim for numerous types of information
- Can be very successful since the message appears to be a system message referencing loss of access or malicious software detection
- Has been used successfully to install malicious software under the pretense of removing malicious software



# Drive-By Downloads

- Uses legitimate websites to infect end users
- The legitimate website is compromised by a malicious individual to add hidden frames, malicious URLs, or malicious scripts to the legitimate website
- The user's browser retrieves the information associated with the malicious URL or script and becomes infected with malicious software
- ClickJacking = Use of hidden frames on web pages to entice the user into clicking on malicious URLs



# DNS Cache Poisoning

- Uses DNS responses to redirect users to malicious websites
- Uses multiple techniques to load malicious IP-address information into legitimate DNS servers
- Removes the need to trick a user into visiting a malicious website since the malicious IP-address is provided by a legitimate DNS server

# SSL Certificate Spoofing

- MD5 Hash Collision/Digital Signature transfer
  - A vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure websites has been identified
  - Utilizes a weakness in the MD5 cryptographic hash function to allow the construction of different messages with the same MD5 hash
  - This vulnerability can be used to create a rogue Certification Authority (CA) certificate trusted by all common web browsers
  - This rogue certificate can be used to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol

# SSL Certificate Spoofing/Piggybacking

- “Piggybacking” SSL Certificates
  - Allows multiple phishing attacks on a single certificate
  - A single compromised Web server with a valid SSL certificate can be used to host multiple phishing sites since visitors to the phishing sites erroneously believe that they have a secure connection with original website
  - Visitors could only detect the fake SSL certificate if they reviewed the certificate or had access to other visual indicators (secured with an extended validation SSL certificate)

# SSL Certificate Spoofing/URL Obfuscation

- NULL character attack
  - Convinces the end-user that a certificate has been issued to a different domain than the one to which it was actually issued
  - The use of NULL characters provides the ability to put up a certificate on what appears to be the exact same domain name as the targeted site
  - This technique utilizes a Man-in-the-Middle attack and uses the null-character certificate to create its false certificates as needed
- Leading zero attack
  - Similar to the NULL Character attack
  - The certificate will attach an invisible zero to the first hex character in the certificate



# Social Engineering Mitigation Methods

- User Security Awareness and Training
- Policies
- Procedures



# Security Awareness Training

- Increases the understanding of security and the threat of Social Engineering
- Training should occur during employee enrollment and at regular intervals
- Training could be outsourced to a third-party since many employees consider third-party input to be more important



# Email Security Awareness Training

- The best mitigation mechanism for SPAM and Phishing emails is the delete button
- To mitigate the potential threat presented by a spam email campaign, it is recommended that you remind your users to never open attachments or click links contained in unsolicited email messages
- Advise them, if possible, to check with the person who supposedly sent the email to make sure that it is legitimate prior to opening any attachments
- Scan any attachments at the network perimeter as well as the desktop with anti-virus software before opening the attachment
- Never use the contact information provided on a web site connected directly to the email request



# Email Security Awareness Training

- Also advise users not to reveal personal or financial information in an email, and not to respond to email solicitations for this information
- Always examine the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain extension such as .com vs. .net
- An additional step to help mitigate the risk of a phishing campaign is to limit the administrative rights of the local users through the implementation of the Least-Privileged best practice
- Only display functional/group email addresses on public websites to limit the amount of SPAM/Phishing emails sent to individuals



# Physical Security Awareness Training

- Ensure all visitors are always escorted
  - Remind employees not to allow “Piggy-Back” access
  - Remind employees not to allow an unknown person to wander the facility
- Never allow a visitor, client, or other persons to simply connect a computer to the internal network without prior approval



# Credential Security Awareness Training

- Protection of account credentials
  - Never give out or share passwords
  - Use strong passwords for any application requiring a login
  - Use unique passwords for every application and avoid using the same password for similar applications
  - Carefully consider the questions used to verify the user for automated password resets
  - Most automated systems use a common set of questions for password reset and the answers to these questions can be found in public records or on-line
    - Place of birth, mother's maiden name, and school information are available in public records
    - Friends, color preference, hobbies, and pet information often found on Social Network sites
    - Make of first car can be guessed based on purchasing trends



# Identity Security Awareness Training

- Protection of Personal Identifiable Information within Social Networks
  - Select your screen name carefully – do not include any information such as your name, age, sex, city, or employer
  - Never post anything you would not want to have distributed publicly
  - Never post personally identifying information such as: SSN, first and last name, address, driver's license, telephone number and e-mail address
  - When establishing your account, adjust your profile until you are comfortable with the amount of protection provided to maximize your security



## Policies

- Must clarify information access controls
- Detail rules for setting up accounts
- Define access approval
- Define process for changing passwords



## Policies

- Define policy for physical destruction of devices and media
  - Hard Drives
  - CD/DVDs
- Define physical control selection and implementation
  - Locks
  - Access controls
  - How visitors are authorized and escorted



# Employee Hiring / Termination Policies

- Hiring should include background checks, verifying educational records, and Non-Disclosure Agreements
- Termination should include exit interviews, review of NDA, suspension of network access, and checklist for equipment return



## Help Desk Procedures

- Used to make sure that there is a standard procedure for employee verification
- Caller-ID or employee call-back can be used to verify caller
- Can also use Cognitive Passwords
  - Arcane information that only the user should know



# Password Change Policy

- Require strong passwords
  - Must not contain any part of account name
  - Must be at least 8-characters long
  - Must contain at least three or four:
    - Numbers
    - Uppercase letters
    - Lowercase letters
    - Non-alphanumeric symbols
- Require password aging
- Prohibit password reuse



# Employee Identification

- ID badges give a clear indication of authorized personnel
- Guests should also wear temporary ID badges
- Guests should be required to sign-in and sign-out
- Anyone without a badge should be questioned and escorted to the proper facility personnel



## Privacy Policies

- Employees and customers have a certain expectation with regard to privacy
- The privacy policy should be posted on the public website



# Data Classification Systems

- Can help prevent Social Engineering
- Can be used to define what information is most critical
- Can be used to gain end-user compliance
- Governmental Information Classification System
  - Designed to protect confidentiality of information
- Commercial Information Classification System
  - Focused on the integrity of information



# Governmental Info Classification System

- Unclassified
  - Information is not sensitive and does not need to be protected
  - The loss of information would not cause damage
- Confidential
  - Information is sensitive and the disclosure could result in some damage
  - Will require a safeguard against disclosure
- Secret
  - Information that is classified as secret has a greater important than confidential data
  - Disclosure would result in serious damage
  - May result in loss of significant scientific or technical development
- Top-Secret
  - Information that requires the most protection
  - Disclosure would be catastrophic



# Commercial Info Classification System

- Public
  - Similar to unclassified information
  - Disclosure would not result in damage
- Sensitive
  - Information requires controls to prevent the release to unauthorized parties
  - Disclosure would result in some damage
- Private
  - Information is primary personal in nature
  - Can include employee or medical records
- Confidential
  - Information has the most sensitive rating
  - Information is required to keep the company competitive
  - The information should never be released



# Questions???



For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!



# *Scareware: Taking Computers Hostage*

*Eric Taylor*

*Northrop Grumman Enterprise Security Architect*

September 2010



***NORTHROP GRUMMAN***

# Rogue or Fake Security Software

- Rogue security software (a.k.a RougeAV, FakeAV) which is software that poses as legitimate Internet security software but is actually malware.
- Rogue security software mainly relies on social engineering (fraud) in order to defeat the security built into operating system and browser software and install itself onto victims' computers.
- The assertive tactics of the scareware has caused significant losses to users. The FBI is aware of an estimated loss to victims in excess of **\$150 million**. [1]

[1] <http://www.ic3.gov/media/2009/091211.aspx>

# Top malware distribution vectors

- **Search Index Poisoning:** Google is a frequent target of online threats. Attackers employ sophisticated search engine optimizations to manipulate search engine rankings and poison users' search result, which sends people to compromised Web sites and leads to malware infections.
- **Social Networks/Web 2.0:** Popular online communities, blogs and social media sites such as YouTube, MySpace, Facebook and Twitter are targets
- **Compromised Websites:** Mass infection of legitimate websites, infecting them with malicious JavaScript.

# Top malware distribution vectors

- Cybersquatting and typosquatting: Malicious Web sites that look like a legitimate website deceive users into believing their transactions and activities are taking place at reputable sites.
- Rich Media and Content format: Attacker misuse known trusted file format to serve malware, these are Image files like GIF and JPEG; Adobe PDF and Flash (SWF), and Media file such as ASF and MP3. Adobe PDF is the most popular exploited Rich Internet Application and it is often used for Drive-by download attacks.
- Malicious Email Spam: Emails containing malicious URL and/or attachments. This type of threat usually uses social engineering techniques to entice users in executing files or clicking URLs.

# SEO Poisoning: A Growing Trend

- **Search engine optimization (SEO)** is the process of improving the visibility of a web site or a web page in search engines via the "natural" or un-paid ("organic" or "algorithmic") search results
- SEO poisoning is a method by which hackers can get a malicious link or URL, indexed by a search engine.
  - The first step in this attack involves an attacker compromising a legitimate website.
  - Hackers are injecting malicious URLs into compromised websites to latch onto Google trends
- SEO poisoning attacks are primarily attacks on popular websites using XSS or cross server scripting.
- Most common SEO poisoning attack today is the the Iframe attack.



- Can you spot the Fake Security Center?



## • Can you spot the Fake Security Center?



Windows Security Center

Security Center  
Help protect your PC

**Resources**

- Get the latest security and virus information from Microsoft
- Check for the latest updates from Windows Update
- Get support for security-related issues
- Get help about Security Center
- Change the way Security Center alerts me

**Security essentials**

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.  
[What's new in Windows to help protect my computer?](#)

**Firewall** ON

**Automatic Updates** ON

**Virus Protection** NOT FOUND

Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. [How does antivirus software help protect my computer?](#)

Note: Windows does not detect all antivirus programs.

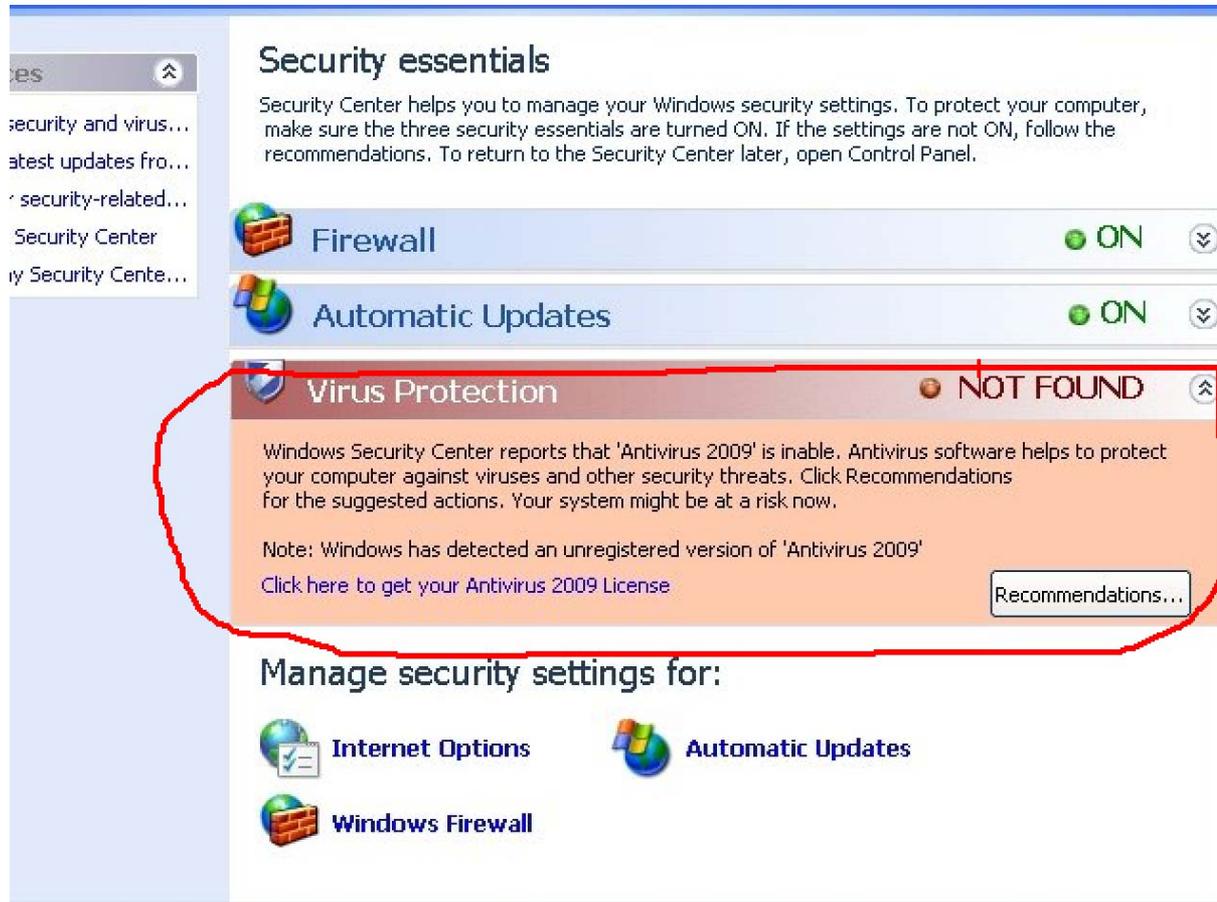
Recommendations...

Manage security settings for:

- Internet Options
- Automatic Updates
- Windows Firewall

At Microsoft, we care about your privacy. Please read our [privacy statement](#).

- Can you spot the Fake Security Center?



# Rogue or Fake Security Software

- Wrap up ...
  - Profitable for scammers
  - Social Engineering
  - Becoming more sophisticated

# References

- <http://www.ic3.gov/media/2009/091211.aspx>
- [http://en.wikipedia.org/wiki/Rogue\\_security\\_software](http://en.wikipedia.org/wiki/Rogue_security_software)
- <http://community.ca.com/blogs/securityadvisor/archive/2010/01/18/black-hat-seo-campaign-using-latest-trend-keywords-demystified.aspx>
- <http://www.stopthehacker.com/2010/04/05/google-trends-for-seo-poisoning/>



Virginia Information Technologies Agency

# 2010 Commonwealth Security Annual Report

John Green  
Chief Information Security Officer



## § 2.2-2009

§ 2.2-2009. (Effective until July 1, 2010) Additional duties of the CIO relating to security of government information.

C. The CIO shall annually report to the Governor, the Secretary, and General Assembly those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the public body's information technology projects pursuant to § 2.2-2015, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.



# Explanation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

**Acronyms:**

- ISO:** Information Security Officer
- IS:** Information Security
- CAP:** Corrective Action Plan
- CISO:** Chief Information Security Officer of the Commonwealth

**ISO Designated: The Agency Head has**

**Yes** - designated an ISO with the agency within the past two years

**No** – not designated an ISO for the agency since 2006

**Expired** –designated an ISO more than 2 years ago or the designated ISO is no longer with the agency

**Attended IS Orientation:**

The number indicates agency personnel that have attended the optional Information Security Orientation sessions within the last 2 years. Their attendance indicates they are taking additional, voluntary action to improve security at their agency akin to “Extra Credit!”



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

**Security Audit Plan Received: The Agency Head has**

**Yes** - submitted a Security Audit Plan for the period of fiscal year (FY) [2010-2012 or 2011-2013](#) for systems classified as sensitive based on confidentiality, integrity or availability (Note: after July 1, 2010, Audit Plans submitted shall reflect FY 2011-2013)

**No** - not submitted a Security Audit Plan since 2006

**Exception** – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved

**Expired** –submitted a Security Audit Plan on file that does not contain the current three year period FY [FY 2010-2012 or FY 2011-2013](#)

**Pending** –submitted a Security Audit Plan that is currently under review

**Corrective Action Plans Received: The Agency Head or designee has**

**Yes** - submitted an adequate Corrective Action Plan or notification of no findings for Security Audits scheduled to have been completed

**Some** - submitted an adequate Corrective Action Plan or notification of no findings for some, but NOT all Security Audits scheduled to have been completed

**No** – not submitted any adequate Corrective Action Plans or notification of no findings for Security Audits scheduled to have been completed

**Not Due** - not had Security Audits scheduled to be completed

**N/A** - not submitted a Security Audit Plan so not applicable

**Pending** –submitted a Corrective Action Plan that is currently under review



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

**Quarterly Updates: The Agency Head or designee has**

**Yes** - submitted adequate quarterly status updates for all corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Some** - submitted adequate quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**No** - not submitted ANY quarterly status updates for some corrective actions resulting from Security Audits previously conducted by or on behalf of the agency

**Not Due** - no open Security Audit findings

**N/A** - not submitted a Security Audit Plan or a Corrective Action Plan that was due

**Pending** - submitted quarterly status update that is currently under review



# Explanation – Continued

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
XYZ	Yes	5	Yes	Yes	Yes	100%

### Percentage of Audit Obligation Completed:

Percent of sensitive systems reported in 2007 (according to IT Security Audit Plans) that have been audited to date. This datapoint is based on the IT Security Audit Standard requirement: *“At a minimum, databases that contain sensitive data, or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years.”*

Agencies that did not submit an IT Security Audit Plan in 2007 were not in compliance and therefore there is no data to report on for 2010.

Systems that have been removed from audit plans within the three year period due to retirement of the system or reclassification to non-sensitive are not counted.

**N/C** – agency not in compliance in 2007, agency did not submit an IT Security Audit Plan in 2007

**N/R** – agency not required to submit an IT Security Audit Plan until 2008

**Pending** – currently under review

**Exception** – submitted an exception on file with VITA to allow time for developing the Security Audit Plan & the CISO has approved



## FAQ!

### **What should an agency do if they conduct a Security Audit that results in no findings?**

In the event that a Security Audit was performed and there were no findings and, therefore, no Corrective Action Plan is due, the Agency Head should notify Commonwealth Security via email or letter stating what audit was conducted and that there were no findings.

### **What is the cutoff date to submit documentation for the Commonwealth Security Annual Report?**

October 31, 2010



# Secretariat: Administration

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Compensation Board	Yes	1	Yes	No	N/A	0%
Dept. of General Services	Yes	3	Yes	Not Due	Not Due	0%
Dept. of Human Res. Mgmt	Yes	1	Yes	No	N/A	0%
Dept. Min. Bus. Enterprise	Yes	0	Yes	Not Due	Not Due	N/C
Employee Dispute Resolution	Yes	0	Exception	Exception	Exception	0%
Human Rights Council	Yes	0	Yes	Not Due	Not Due	N/C
State Board of Elections	Yes	0	Expired	Some	No	50%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Agriculture & Forestry

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Forestry	Yes	0	Yes	Not Due	Not Due	0%
Va. Dept. of Ag. & Cons. Serv.	Yes	0	Yes	Yes	Yes	66%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Commerce & Trade

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Board of Accountancy	Yes	0	Yes	Yes	Not Due	100%
Dept of Business Assistance	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Housing & Community Development	Yes	1	Yes	Yes	Yes	14%
Dept. of Labor & Industry	Yes	0	Yes	No	N/A	N/C
Dept. of Mines, Minerals & Energy	Yes	0	Yes	Yes	Yes	80%
Dept. of Professional & Occupational Regulation	Yes	1	Yes	Yes	Not Due	100%
Tobacco Indemnification Commission	Yes	1	Yes	No	N/A	N/C
Va. Economic Development Partnership	Yes	1	Yes	Not Due	Not Due	N/C
Va. Employment Commission	Yes	1	Yes	Yes	Yes	Exception
Va. National Defense Industrial Authority	Yes	0	Yes	Not Due	Not Due	N/C
Va. Racing Commission	Yes	1	Yes	Yes	Not Due	N/C
Va. Resources Authority	No	0	No	N/A	N/A	N/C

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Education

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Christopher Newport University	Yes	0	Yes	Not Due	Not Due	0%
Dept. of Education	Yes	1	Yes	Not Due	Not Due	0%
Frontier Culture Museum of Va.	Yes	0	Yes	Not Due	Not Due	N/C
Gunston Hall	Yes	1	Yes	Not Due	Not Due	N/C
Jamestown - Yorktown Foundation	Yes	2	Yes	Yes	Not Due	100%
Library of Va.	Yes	0	Yes	Not Due	Not Due	100%
Norfolk State University	Yes	0	Yes	No	N/A	N/C
Richard Bland College	Yes	0	Yes	Not Due	Not Due	100%
Science Museum of Va.	Yes	1	Yes	Not Due	Not Due	N/C
State Council of Higher Education for Va.	Yes	0	Yes	Not Due	Not Due	N/C
University of Mary Washington	Yes	1	Yes	Yes	Yes	67%
Va. Commission for the Arts	Yes	0	Yes	Not Due	Not Due	N/C
Va. Museum of Fine Arts	Yes	0	Yes	Yes	Some	Exception
Va. School for the Deaf and Blind	Yes	2	Yes	Not Due	Not Due	N/R
Virginia State University	Yes	1	Yes	Yes	Yes	Exception

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Finance

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Accounts	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Planning & Budget	Yes	0	Yes	Yes	Not Due	N/C
Dept. of Taxation	Yes	1	Yes	Yes	Not Due	50%
Dept. of Treasury	Yes	1	Yes	No	N/A	0%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Health & Human Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Health Professions	Yes	4	Yes	Not Due	Not Due	0%
Dept. of Medical Assistance Services	Yes	4	Yes	Yes	Yes	100%
Department of Behavioral Health and Developmental Services	Yes	13	Yes	Yes	Yes	100%
Dept. of Rehabilitative Services	Yes	0	Yes	Yes	Not Due	19%
Dept. of Social Services	Yes	0	Yes	Not due	Not Due	0%
Virginia Foundation for Healthy Youth <del>FSF</del>	Yes	1	Yes	Not due	Not Due	N/C
Va. Dept. for the Aging	Yes	0	Yes	Yes	Not Due	Exception
Va. Dept. of Health	Yes	2	Yes	Some	Some	20%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Natural Resources

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Conservation & Recreation	Yes	1	Yes	Some	Yes	0%
Dept. of Environmental Quality	Yes	2	Yes	Some	Some	60%
Dept of Game & Inland Fisheries	Yes	3	Expired	Some	No	N/C
Dept. of Historic Resources	Yes	1	Expired	No	No	0%
Marine Resources Commission	Yes	1	Yes	Yes	Yes	100%
Va. Museum of Natural History	Yes	1	Yes	Not Due	Not Due	N/C

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Public Safety

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Alcoholic Beverage Control	Yes	5	Yes	Yes	Yes	100%
Commonwealth's Attorney's Services Council	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Correctional Education	Yes	0	Yes	Yes	Yes	N/C
Dept. of Corrections	Yes	3	Yes	Yes	Yes	50%
Dept. of Criminal Justice Services	Yes	2	Pending	Pending	Pending	20%
Dept. of Fire Programs	Yes	2	Yes	Yes	Yes	N/C
Dept. of Forensic Science	Yes	0	Yes	Not Due	Not Due	N/C
Dept. of Juvenile Justice	Yes	0	Yes	Yes	Not Due	33%
Dept. of Military Affairs	Expired	1	No	N/A	N/A	N/C
Dept. of Veterans Services	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. of Emergency Management	Yes	1	No	N/A	N/A	N/C
Va. State Police	Yes	1	Yes	Some	Yes	67%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Technology

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
The Ctr for Innovative Tech.	Yes	0	Yes	Not Due	Not Due	N/C
Va. Info. Technologies Agency	Yes	14	Yes	Yes	Yes	70%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Secretariat: Transportation

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Dept. of Motor Vehicles	Yes	1	Yes	Yes	No	N/C
Dept. of Aviation	Yes	1	Yes	Not Due	Not Due	N/C
Dept. of Rail & Public Trans.	Yes	0	Yes	Not Due	Not Due	0%
Motor Vehicle Dealers Board	Yes	0	Yes	Not Due	Not Due	N/C
Va. Dept. Of Transportation	Yes	5	Yes	Yes	Yes	66%

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Independent Branch Agencies

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Indigent Defense Commission	Yes	1	Yes	Yes	Not Due	N/R
State Lottery Dept.	Yes	2	Yes	Not Due	Not Due	N/R
State Corporation Commission	Yes	3	Yes	No	No	N/R
Va. College Savings Plan	Yes	0	Yes	Yes	Not Due	N/R
Va. Office for Protection & Advocacy	Yes	1	Exception	Exception	Exception	N/R
Va. Retirement System	Yes	1	Yes	Some	Some	N/R
Va. Workers' Compensation Commission	Yes	3	Exception	Exception	Exception	N/R

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# Others

Agency	ISO Designated	Attended IS Orientation	Security Audit Plan Received	CAPs Received	Quarterly Updates	Percentage of Audit Obligation Completed
Office of the Governor	No	0	No	N/A	N/A	N/C
Office of the Attorney General	Yes	0	Yes	Not Due	Not Due	N/C

**NOTE:** Information in this slide represents what Commonwealth Security is currently tracking for these agencies. The data in these slides will change month to month as agencies submit their documentation. If any of the information seems erroneous please contact [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



*Virginia Information Technologies Agency*

# Upcoming Events





## Future ISOAG's

**From 1:00 – 4:00 pm at CESC**

**Thursday - October 14, 2010**

**Tuesday - November 9, 2010**

**Thursday - December 9, 2010**

***ISOAG will be held the 1<sup>st</sup> Wednesday of each month in 2011***



# Future IS Orientation Sessions

**Monday - November 1, 2010 1:00 – 3:30**  
**(CESC)**

**Tuesday - January 11, 2011 9:00 – 11:30**  
**(CESC)**

**IS Orientation is now available via webinar!**



# InfraGard Quarterly Meeting

The Richmond Chapter of InfraGard will hold its quarterly meeting

**Date:** Wednesday, October 6, 2010,

**When:** 10:00am-12:00pm,

**Where:** Henrico Training Center,

7701 E. Parham Road, Henrico, VA, 23294.

**Topic:** Cyber Security

**Speaker:** Randy Marchany, Chief Information Technology Security Officer, Virginia Tech will present, "*The More It Changes, The More It Stays the Same*" discussing how the same cyber attack techniques used 10 years ago, still work today. The second hour will have 4 government attorneys who specialize in cyber prosecutions discuss what they are seeing at the federal, state & local levels; how they are addressing these issues; what role the private sector can play in fighting cyber crime.

**RSVP by September 30 to: [paul.messing@leo.gov](mailto:paul.messing@leo.gov)**

This meeting will be open to non-members, so please respond early to reserve your place.



# AITR Meeting

## AITR Meeting:

**Wednesday, October 20th**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** CESC



# Information Security System Association

ISSA meets on the second Wednesday of every month

**DATE: Wednesday, October 13, 2010**

**LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,  
#2204, Richmond/Short Pump Mall**

**TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &  
Lunch served at 12.**

**COST: ISSA Members: \$10 & Non-Members: \$20**

**SPEAKER: Randy Sabett (topic to be finalized)**



## MS-ISAC Webcast

# National Webcast!

Thursday, October 14, 2010, 2:00 to 3:00 p.m.

**Topic: In Collaboration of National Cyber Security Month**

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



## Identity Theft Red Flags Rules Extended Until December 31, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until December 31, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Virginia Information Technologies Agency

Any Other Business ???????





# ISOAG-Partnership Update

*Don Kendrick*

*IT Infrastructure Partnership Team*

September 15, 2010



**NORTHROP GRUMMAN**

# Section Agenda

- Windows Patching Effort
- BlueCoat Splash Screen – Dean Weiner
- BlueCoat Reporter – Brandi Lucas
- Partnership Q & A

**ADJOURN**

**THANK YOU FOR ATTENDING**

