



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

May 12, 2010



# ISOAG May 2010 Agenda

- |      |  |   |
|------|--|---|
| I.   | Welcome & Opening Remarks                  | John Green, VITA  |
| II.  | Cyberspace – A Matter of National Security | Marcus Sachs, Verizon                                   |
| III. | Collection of SSN in the Commonwealth      | Lisa Wallmeyer, JCOTS                                   |
| IV.  | Gone Phishing, Be Back at Dark Thirty      | Bob Baskette, VITA<br>Eric Taylor, NG                   |
| V.   | Upcoming Events & Other Business           | John Green, VITA  |
| VI.  | Partnership Update                         | Don Kendrick, VITA<br>Craig Drain, NG<br>Tony Shoot, NG |



## Marcus Sachs, Verizon

- Content Intentionally Omitted



# Collection of SSN in the Commonwealth

Lisa Wallmeyer, Executive Director  
Virginia Joint Commission on Technology & Science

# [ What is JCOTS? ]

- JCOTS is a permanent legislative commission, established by the General Assembly in 1997 to...  
“...study all aspects of technology and science and endeavor to *stimulate, encourage, promote, and assist* in the development of technology and science in the Commonwealth and sound public policies related thereto...”

(§ 30-85 of the Code of Virginia)

# Personally Identifiable Information Subcommittee

- Originally convened during 2007 Interim; continued in 2008 & 2009
- A joint subcommittee of JCOTS and the Freedom of Information Advisory Council
- Develop policy regarding the protection of personally identifiable information
  - Discussion turned to focus on over-collection of Social Security Numbers by government entities

# [ What's been done already? ]

- Federal Privacy Act of 1974
  - No federal, state, or local government agency may deny an individual a right, benefit, or privilege provided by law because the individual refuses to provide his SSN
  - Exceptions:
    - Disclosure is required by federal statute
    - Disclosure was required prior to January 1, 1975 under statute or regulation adopted prior to that date to verify an individual's identity
  - Virginia has adopted similar language – Government Data Collection & Dissemination Practices Act (Va. Code § 2.2-3800 et seq. )

# [ What's been done already? ]

- Over the past decade, Virginia has limited the use of SSN:
  - SSN can no longer be used as driver's license number (not even optional)
  - SSN can't be displayed on student ID cards or agency-issued cards
  - SSN can't be used as Health Insurance ID under state plan

# [ Recent legislation ]

- Legislation adopted during 2009 Session of the General Assembly will prohibit a government agency from releasing more than the last four digits of a SSN in response to a FOIA request
  - Chapter 213 of the 2009 Acts of Assembly

# [ What about collection of SSN? ]

- A lot of focus in this discussion on dissemination of social security numbers...what about looking why and when we collect it in the first place?
- Past few years have drawn attention to database breaches, misuse of information, etc.

# [ Future limitations on collection ]

- Beginning July 1, 2010, no agency shall collect from an individual his social security number (or any portion thereof) unless collection is:
  - Authorized or required by state or federal law; AND
  - Essential for the performance of that agency's duties

# [ Questions? ]

Lisa Wallmeyer, Executive Director  
Virginia Joint Commission on Technology &  
Science

[jcots@dls.virginia.gov](mailto:jcots@dls.virginia.gov)

804.786.3591

<http://jcots.dls.virginia.gov>



# Gone Phishing – Be Back At Dark Thirty

Bob Baskette:  
Commonwealth Security Architect

Eric Taylor:  
Northrop Grumman Security  
Architect



# Phishing Basics

- Phishing campaigns are a form of social engineering, an attack that uses human interaction to obtain or compromise information about an individual or organization. Phishing attacks 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 web sites, auction sites, online payment processors or IT Administrators to entice the unsuspecting public to respond.
- The earliest reports of phishing were associated with AOL. Phishing on AOL was closely associated with the Warez community that used AOL to exchange pirated software and stolen credit card numbers.
- Targeted versions of phishing have been termed spear phishing.
- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft. In 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details.



# Phishing Techniques

- Social engineering
  - People respond without thinking to things that seem important. Email subjects lines worded to create anxiety 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.
  - Phishing emails also target self-doubt with subject lines such as "Do you trust her/him" or "Is she/he cheating on you".
- URL manipulation
  - Most Phishing methods employ a form of technical deception designed to make the URL in the Phishing e-mail appear to associated to a legitimate company. Misspelled URLs or the use of subdomains are common tactics employed by Phishers.
  - An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password.  
<http://www.amazon.com@members.rbn.com/>

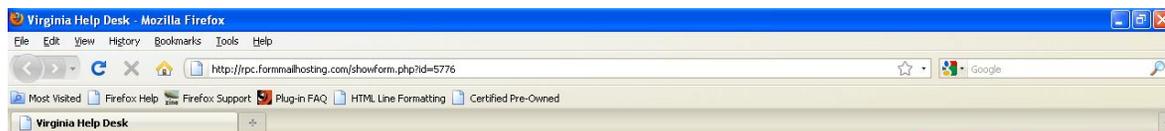


# Phishing Techniques

- Email Filter evasion
  - Phishers will forward the client to a company's legitimate website, then layer a popup window requesting credentials on top of the legitimate website in a way that makes it appear that the company is requesting the information.
  - Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.
  - Once a victim visits the phishing website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.
  - An attacker can even use flaws in a trusted website's own scripts against the victim. These cross-site scripting attacks are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct.



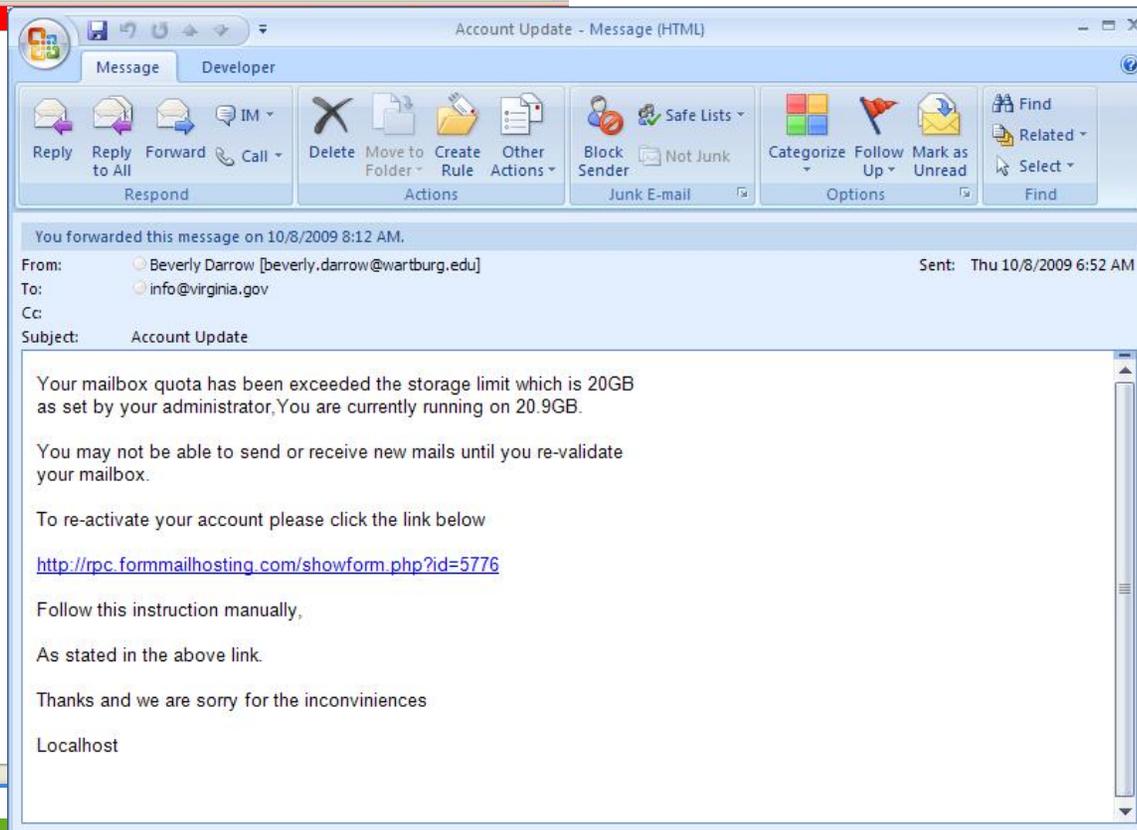
# COV Phishing Examples



## Virginia Help Desk

Verify Your Virginia Webmail Account Details Below

Full Name	<input type="text"/>
Email Address	<input type="text"/>
Email ID	<input type="text"/>
Date of Birth	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>



Done



# COV Phishing Examples



## ADMINISTRATIVE INTRANET

Question # 1  
\*First Name:

Question # 2  
\*Last Name:

Question # 3  
\*Email Address:

Question # 4  
\*DomainUsername:

Question # 5  
\*Password:

Question # 6  
\*Confirm Password:

Powered by [Sureforms FREE Survey, Payment Form and Basic Form Builder](#)



Subject: Re: Your Webmail Quota Has Exceeded??

Attachments: image001.gif (4 KB)

---

**From:** Mayo, Charles [mailto:Charles.Mayo@umassmemorial.org]  
**Sent:** Thursday, January 14, 2010 10:51 AM  
**To:** admin@helpdesk.org  
**Subject:** Your Webmail Quota Has Exceeded??

Your Webmail Quota Has Exceeded The Set Quota/Limit Which Is 20GB.  
 You Are Currently Running On 23GB Due To Hidden Files And Folder On Your Mailbox.  
 Please Click the Link Below To Validate Your Mailbox And Increase Your Quota.

[Click here:](#)

Failure To Click This Link And Validate Your Quota May Result In Loss Of Important Information In Your Mailbox/Or Cause Limited Access To It.

Thanks  
 HELP DESK

*The information transmitted is intended only for the person or entity to which it is addressed and may be confidential, privileged or otherwise subject to legal protection. If you have received this in error, please contact the sender and delete the material from any computer.*



## Phishing Analysis

- 8 accounts compromised = **2,096,786** SPAM messages
- Over 10,000 abuse messages have been received
- Internet Service Provider blacklisting Commonwealth



## How it's done

- Simple Demo
  - Social Engineering
    - Something you want or need
    - Trust
  - Account Harvesting
  - Account Compromise
    - OWA
    - Delete all rule
    - SPAM



## The Power of a Signature

- The signature of John Hancock on the Declaration of Independence is one of the most recognizable in Western history.
- Hancock was the first to sign and he did so in an entirely blank space.
- Hancock commented, "The British ministry can read that name without spectacles; let them double their reward."



# Asymmetric Algorithms / Public Key

- Two keys linked mathematically, but would be mutually exclusive
- One key will encrypt/the other key would decrypt
- User generates two keys
  - Private Key that is kept secret and used to by receiver to decrypt messages
  - Public Key that can be sent to anyone and is used by sender to encrypt messages
- Important key properties:
  - Public key cannot decrypt message it encrypted
  - Private key cannot be derived from the public key
  - Message encrypted by one key can be decrypted by the other key
  - Private key must be kept secret
- Asymmetric algorithms are one-way functions



# Asymmetric-related terms

- **Confidentiality**
  - Sender encrypts message with the receiver's public key
  - Only the receiver can decrypt the message
- **Non-repudiation**
  - Security service by which evidence is maintained so that the sender and the recipient of the data cannot deny having participated in the communications
  - Supported via public-key encryption and digital signatures
  - Sender encrypts the message with the sender's private key
  - The receiver opens with the sender's public key

# Asymmetric Message Formats

- **Secure Message Format**
  - Encrypting a message with receiver's public key
  - Will provide confidentiality but not authentication or non-repudiation
- **Open Message Format**
  - Encrypting a message with the sender's private key
  - Will provide authentication and non-repudiation but not confidentiality



## Digital Signature

- A digital signature is simply a mathematical algorithm used to demonstrate the authenticity of a digital message or document.
- A valid digital signature provides the recipient a basis to believe that the message was created by a known sender and that the message was not altered in transit.
- Digital signatures are equivalent to traditional handwritten signatures and can provide non-repudiation as well as authentication.



# Digital Signature

- Message's Hash value that has been encrypted with the sender's private key
- Act of signing is the act of encryption
- Legally binding and enforceable in most courts
- Used to detect unauthorized modification of data and to authenticate the identity of the signatories and non-repudiation
- Accomplished by generating a block of data that is usually smaller than the size of the original data (bound to the original data and the identity of the sender)
- Will include a date and time of signature as well as a method for a third-party to verify
- Hashing will provide message integrity
- Encrypting Hash will provide authentication and non-repudiation



# Digital Certificates

- A digital certificate, as defined within the field of cryptography, is an electronic document which utilizes a digital signature to bind a publicly-accessible encryption key to the identity of the encryption key owner.
- This identity is compromised from information such as the name of the person or organization that owns the encryption key, the postal address of the entity, and the contact information for more information about the owner of the encryption key.
- The certificate is normally used to verify that the publicly-accessible encryption key belongs to the stated owner. A digital certificate can be used to receive encrypted email or digitally sign an electronic document.



## Digital Certificates Provide

- Confidentiality
- Access control
- Integrity
- Authentication
- Non-repudiation



## Digital Certificate (identity certificate)

- Uses a digital signature to bind a public key with a user's identity to produce a public certificate
- Contains information:
  - Certificate validity period
  - Peer identity information
  - Encryption keys used for secure communications
  - Signature of the issuing Certificate Authority



## Self-Signed Digital Certificate

- A self-signed digital certificate is used strictly as an identity certificate.
- The self-signed digital certificate is signed solely by its creator and does not provide an independent verification for the identity of the certificate owner.
- Such certificates are also termed root certificates.



## VITA Self-Sign Root Digital Certificate

- The VITA self-signed root digital certificate has been made available to the public to allow any entity to verify the digital signature of an electronic message signed using a digital certificate based on the VITA self-signed root digital certificate. The VITA self-signed root digital certificate can be found at the following URL:  
<https://webmail.vita.virginia.gov/vita/vitaintadcapath.p7b>
- The Thumbprint to validate the integrity of the VITA self-signed root digital certificate is: 5E69B1C0 7E851889 C9B2E13B 731EF1AF D4719E0A (sha1)



## Importing a Certificate

- To import a certificate into Microsoft Outlook (contact list)
  - In Contacts, open the contact form for the individual whose certificate you want to import
  - On the Contact tab, in the Show group, click Certificates, and then click Import
  - Locate and select the certificate file that you want, and then click Open.



## Importing a Certificate cont.

- To add a contact and certificate received in an e-mail message to your contact list
  - Open the digitally signed message from the recipient.
  - Right-click the name in the 'From Field', and then click 'Add to Contacts' on the shortcut menu.
  - If a contact entry already exists for this person, select 'Update new information'

## Sending a message with a digital signature

1. Hash algorithm used to generate the message digest from the message
2. Message digest is fed into the digital signature algorithm that generates the signature of the message
3. Sign the message by encrypting the message digest with the sender's private key and attach to the message

# Digital Signature Example

**Message Security Properties** ✕

 Subject: YOUR PASSWORD IS EXPIRING IN 15 DAYS on 5/12/2010

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

**Security Layers**  
 Select a layer below to view its description.

- ✓ Subject: YOUR PASSWORD IS EXPIRING IN 15 DAYS on 5/12/2010
  - ✓ Digital Signature Layer
    - ✓ Signer: EnterpriseMessagingOperations@cov.virginia.gov

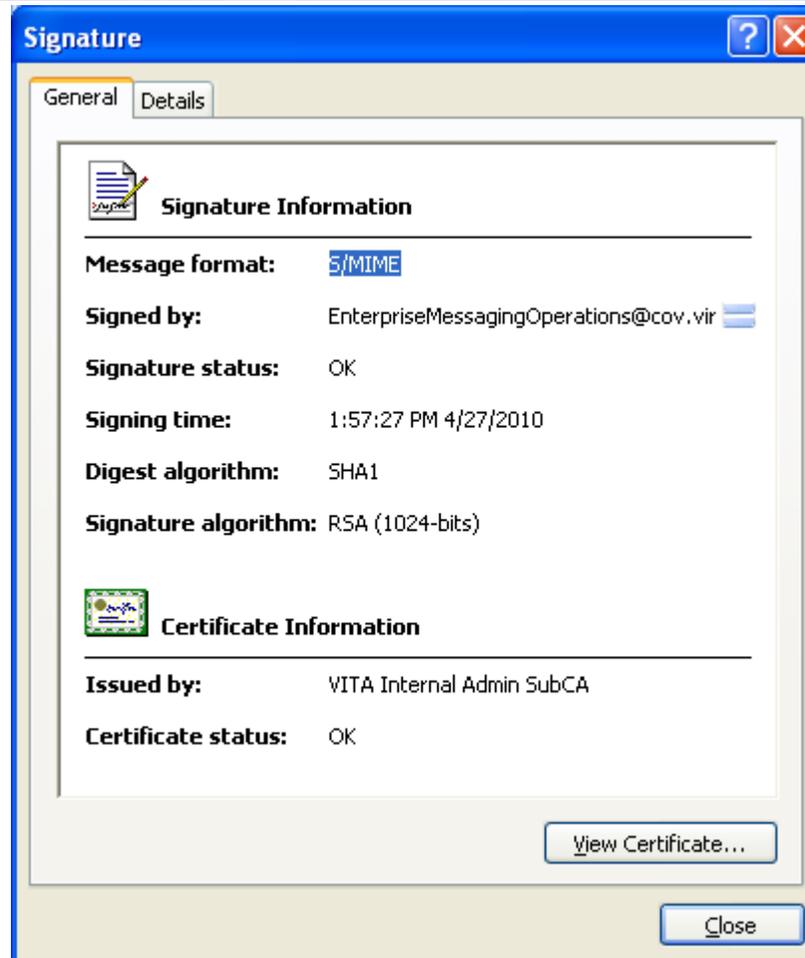
Description:

OK: Signed by EnterpriseMessagingOperations@cov.virginia.gov using RSA/SHA1 at 1:57:27 PM 4/27/2010.

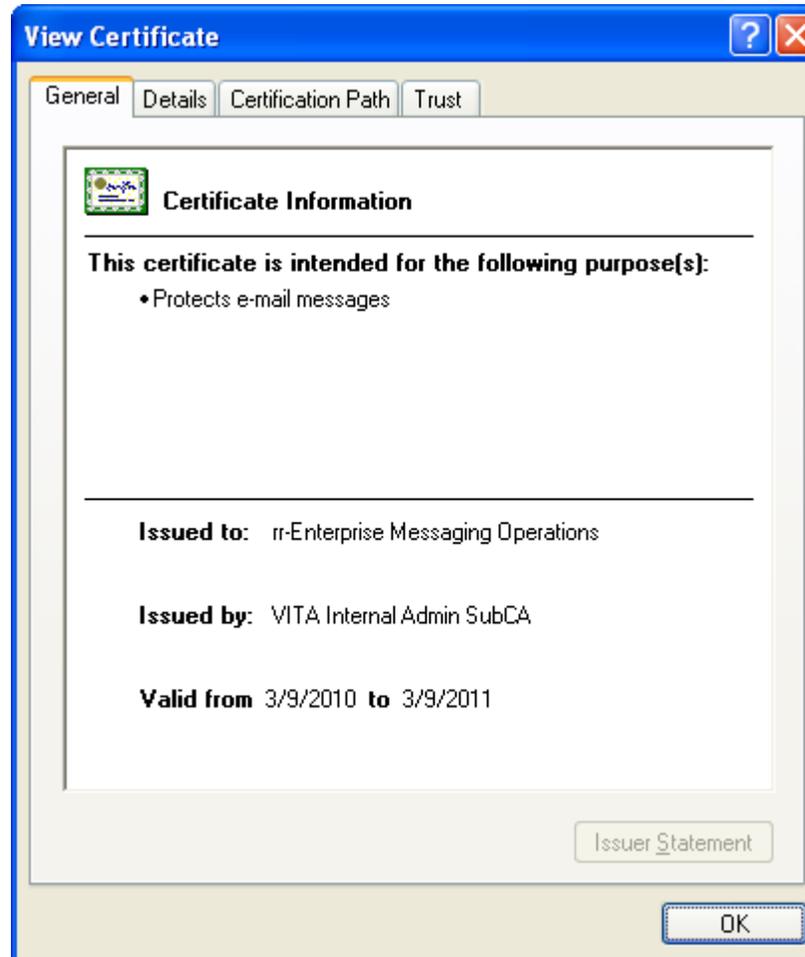
Click any of the following buttons to view more information about or make changes to the selected layer:

Warn me about errors in digitally signed e-mail.

# Digital Signature Example cont.



# Digital Signature Example cont.





## Final Thoughts

- The best mitigation mechanism for Phishing emails is the delete button.
- To mitigate the potential threat presented by a Phishing 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.
- If the legitimacy of an email request needs to be verified, try to verify the origin of the email by contacting the company directly. Never use the contact information provided on a web site connected directly to the email request.



## Final Thoughts

- 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. Granting each local user only those system access rights required to perform the duties assigned to each local user will reduce the impact of any exploit successfully downloaded to the local user's computer.
- Finally, carefully consider the email addresses listed on public websites. Only display functional/group email addresses to limit the amount of SPAM/Phishing emails sent to individuals.



## Questions???

For more information, please contact:  
[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

Thank You!



Virginia Information Technologies Agency

# Upcoming Events





## Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday - June 16, 2010 - **@ DMV!**  
*(Thank you Norm Hill for coordinating this!)*

Thursday - July 22, 2010

Thursday - August 12, 2010



# Future IS Orientation Sessions

- |           |                   |                     |
|-----------|-------------------|---------------------|
| Tuesday - | July 6, 2010      | 1:00 – 3:30 (CESC)  |
| Tuesday - | September 7, 2010 | 9:00 – 11:30 (CESC) |
| Monday -  | November 1, 2010  | 1:00 – 3:30 (CESC)  |

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



# DHS/FEMA State Cyber Security Training Program

The Adaptive Cyber-Security Training Online (ACT-Online) courses are now available on the TEEEX Domestic Preparedness Campus. This training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

Cost is Free!! Students earn a DHS/FEMA Certificate of Completion along with Continuing Education Units (CEU) at the completion of each course.

No-Charge registration is available at the host site:

<http://www.teexwmdcampus.com>

*Thanks to Cameron Caffee, VDOT, for this information!*



# Information Security System Association

ISSA meets on the second Wednesday of every month

**DATE: Wednesday, June 9, 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.**

**PRESENTATION: Encryption Trends & Best Practices  
by IBM**

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



# SANS

Host: Virginia Tech

Ed Skoudis' Class - SEC 560 Network Pen Test & Ethical Hacking

Date: May 17-22, 2010

Cost: \$800 per person (regular price \$3550) for state and local government employees including LEO

Visit: [www.cpe.vt.edu/isect](http://www.cpe.vt.edu/isect)



## MS-ISAC Webcast

### National Webcast!

Wednesday, June 23, 2010, 2:00 to 3:00 p.m.

Topic: Incident Response

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 June 1, 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 June 1, 2010. Read the FAQ at:  
<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



## Security Awareness Tools

For those of you here in Chester, we have Security Awareness Tools available for you!

Security Bookmarks!  
Security Brochures!  
Security Posters!  
*Duh's of Security* DVD!

- All of these tools and many more can be downloaded from the toolkit website

<http://www.vita.virginia.gov/security/default.aspx?id=5146>



Virginia Information Technologies Agency

Any Other Business ???????





# ISOAG-Partnership Update

*Don Kendrick*

*IT Infrastructure Partnership Team*

May 12, 2010



***NORTHROP GRUMMAN***

# Content Intentionally Omitted



**ADJOURN**

**THANK YOU FOR ATTENDING**

