



*Virginia Information Technologies Agency*

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

June 17, 2009

# June



**FLAG DAY**



**FATHER'S DAY**





# ISOAG June 2009 Agenda

- |       |   |  |
|-------|---|--|
| I.    | Welcome & Opening Remarks   | Peggy Ward, VITA                       |
| II.   | Freedom of Information Act (FOIA) –<br>What it is & What it Isn't | Maria Everett, FOI<br>Advisory Council |
| III.  | 2009 COV Security Policy & Standard                               | John Green, VITA                       |
| IV.   | 2009 COV Information Security Report                              | Peggy Ward, VITA                       |
| V.    | Host-Based Intrusion Prevention System                            | Eric Taylor, NG                        |
| VI.   | What is an EISP?<br>Assessing the Self-Assessment—Way Forward     | Leonard Price / Michael Clark, NG      |
| VII.  | SPAM, Phishing, & Other Junk email                                | Bob Baskette, VITA                     |
| VIII. | Upcoming Events   | Peggy Ward, VITA                       |

# **VIRGINIA FREEDOM OF INFORMATION ACT**



**Maria J.K. Everett, Executive Director  
VA Freedom of Information Advisory Council**

# VA Freedom of Information Advisory Council, a state agency

- *Issues advisory opinions*
  - written, oral, email
- *Provides FOIA training*
  - Biennial FOIA Roadshow
  - Specialized training upon request
- *Publishes educational material*

# PURPOSE



- SINGLE BODY OF LAW
- EVERY DAY APPLICATION OF *“GOVERNMENT OF, BY AND FOR THE PEOPLE”*
- PREDICTABLE BEHAVIOR BY GOVERNMENT
- PROCEDURES TO BE FOLLOWED

# FOIA IS A BALANCE



**RIGHT OF ACCESS**

*Versus*

**NEED OF GOVERNMENT  
TO FUNCTION**

# PUBLIC RECORDS

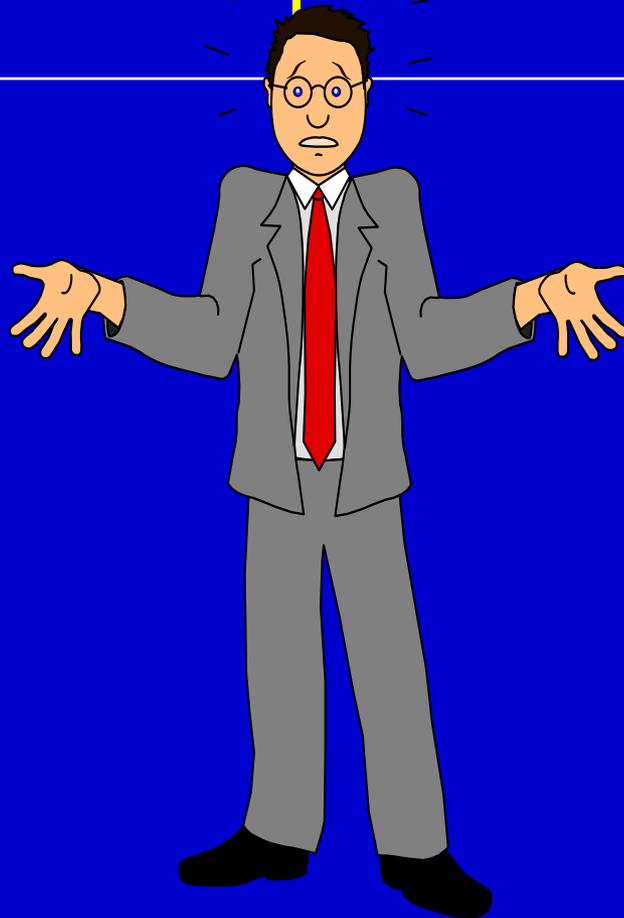
- Regardless of physical form or characteristic;
- However stored;
- **Owned or prepared by or in the possession of a public body or its officers, employees, or agents in the transaction of public business.**

# Debunking FOIA Myths

- **RECORDS not explanations**
- **Inspect or Copy**
- **Not free**
- **FOIA doesn't *prohibit* release**
- **Informal vs. formal requests**

# FOIA REQUESTS

*DON'T HAVE TO:*



BE IN  
WRITING

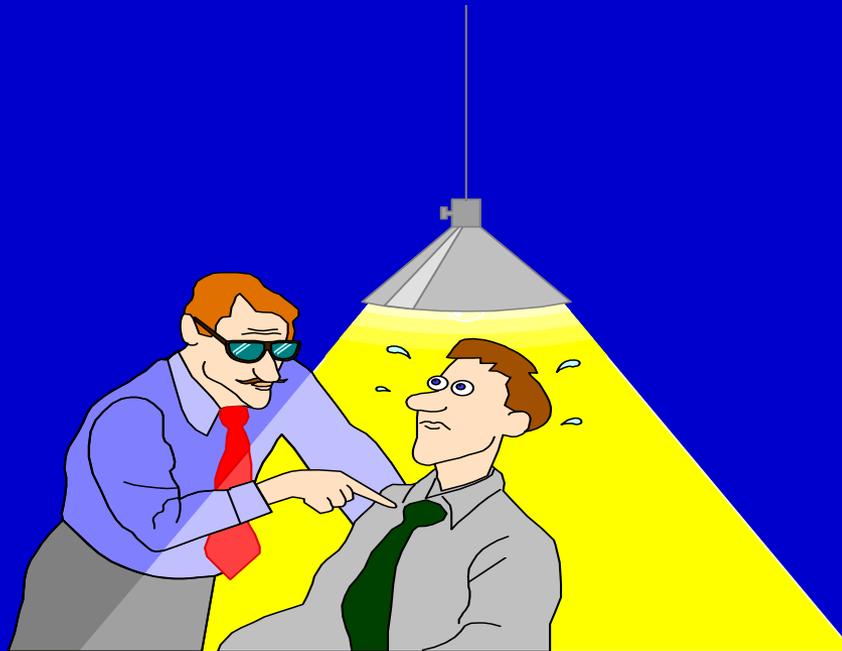
SAY  
“FOIA”

# WHO HAS FOIA RIGHTS

- VIRGINIA  
CITIZENS
- MEDIA



# MOTIVE IMMATERIAL



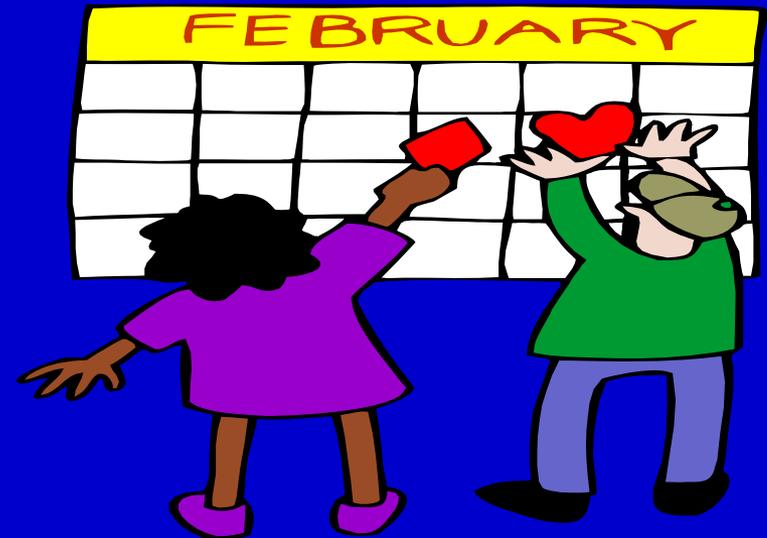
# FOIA REQUIRES

**5 WORKING DAYS**

**TO PRODUCE RECORDS**

**-OR-**

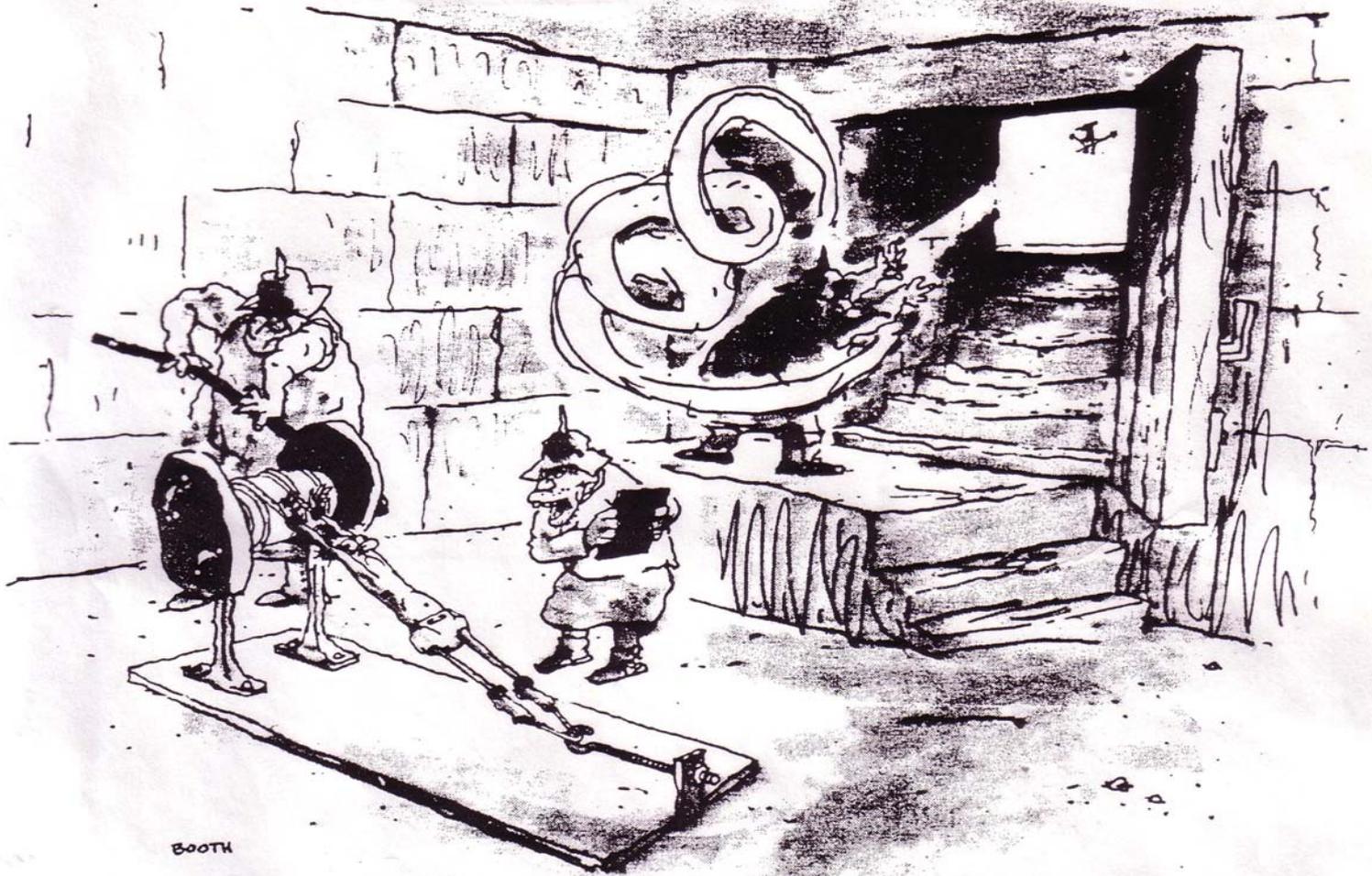
**TO MAKE OTHER  
RESPONSE**



# RESPONSES

- YES, here are the records
- We need more time
- NO, records or portions exempt
- Records don't exist OR can't be located

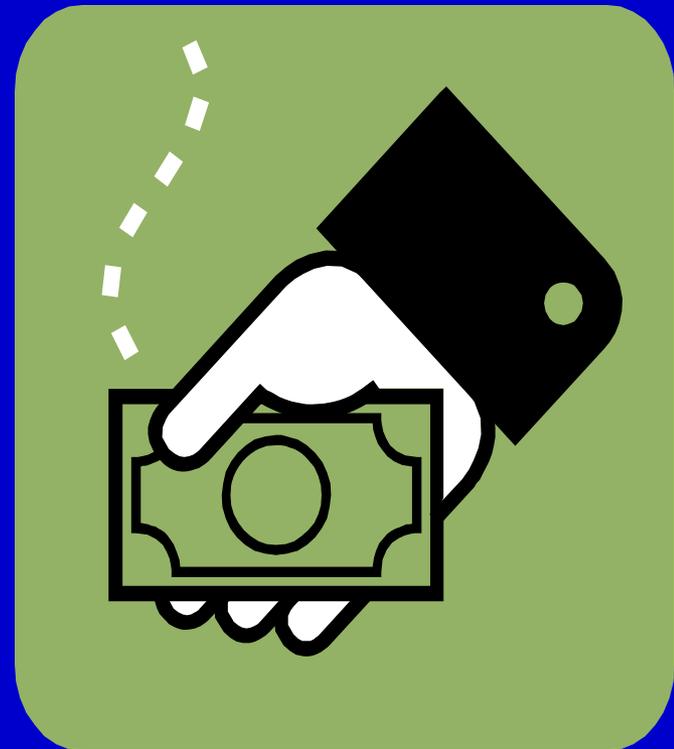
5 DAYS



*"Your FOIA request has been rejected and your dog has been cast out."*

# CHARGES

- **SEARCH COSTS**
- **ACCESSING**
- **SUPPLYING**
- **DUPLICATING**



# ACTUAL COSTS ONLY



- Hourly rate
- NO fringe benefits
- Administrative act
- Reasonable, too.

# CHARGES; ADVANCE DEPOSIT



- More than \$200
- Estimate Required
- Money Up Front

# **ENFORCEMENT**

- **Failure to follow FOIA deemed violation.**
- **FOIA Suit by aggrieved party**
- **Burden of proof on Government**

# PENALTIES



- Pay legal bills of petitioner
- Mandamus or Injunction
- BAD PRESS

# PENALTIES

## “Knowing” and “Willful” Violations



- Up to \$1,000 for 1<sup>st</sup> violation.
- Up to \$2,500 for any subsequent violation.
- Paid by violator, not the agency!

# Advisory Opinions

- VA Freedom of Information Advisory Council
- Attorney General



# Remember

- **Call FOIA Council with ANY questions.**
- **There are NO stupid FOIA questions.**
- **Set “institutional culture” for compliance with FOIA.**
- **FOIA says —How and When to *ACT*; Not how to *FEEL*.**
- **It is NOT our individual sense of fairness, but the collective sense expressed in the law.**



# FOIA COUNCIL

- 1-866-448-4100 (toll free)
- 804-225-3056
- Email:  
foiacouncil@dls.virginia.gov
- Website:  
<http://dls.state.va.us/foiacouncil.htm>



# Policy, Standard & Guidelines

**John Green**

Deputy Chief Information Security Officer



# Policy, Standard & Guidelines Update



1. Collect comments & questions from the IS community during the year
2. Create draft of policy, standard or guideline (PSG) addressing comments...
3. Distribute draft to IS Council for review, input & feedback
4. Collect comments from IS Council, usually giving them a week or so to review
5. Review & address Council comments in the PSG
6. Send draft of PSG to ITIES Directorate for review & comment
7. Aggregate comments from ITIES, usually takes a week or so
8. Comments from ITIES are reviewed with CSRM management & addressed as appropriate
9. Draft of PSG is sent to ITIES for posting to Online Review Comment Application (ORCA)...
10. Gather comments from IS community (ORCA) for at least 30 days
11. Review & address ORCA comments
12. Create responses to comments from ORCA reviewers & distribute through ITIES
13. Send finalized version of PSG to ITIES who sends it to the CIO for approval.
14. If the CIO approves it goes to the ITIB for consideration & approval. If a standard or guideline there is a 5 day comment period & if a policy it must be approved at an ITIB meeting
15. Once approved it is posted to the web

Standard →

Policy →



# Policy and Standard Highlights

- New Policy number SEC519-00
- Online review & comment period for Standard closed June 12
  - 20 individuals commented
  - 350+ comments
    - Approximately 230 recommend content change
    - Grammar fixes deeply appreciated
- Hotspots for comments
  - Roles & Responsibilities
  - Wireless



2009  
Commonwealth Security Annual Report

**Peggy Ward**  
Chief Information Security & Internal Audit Officer





## § 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, 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 and 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 the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



# Explanation

| Agency     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Agency XYZ | Yes            | 10                      | Yes                          | Yes           | Yes               |

**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 |
|------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Agency XYZ | Yes            | 10                      | Yes                          | Yes           | Yes               |

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

**Yes** - submitted a Security Audit Plan for the period of fiscal year 2009 - 2011 for systems classified as sensitive based on confidentiality, integrity or availability

**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 2009 – FY 2011

**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 |
|------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Agency XYZ | Yes            | 10                      | Yes                          | Yes           | Yes               |

**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



# Secretariat: Administration

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



# Secretariat: Agriculture & Forestry

| Agency                         | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Forestry              | Yes            | 1                       | Expired                      | Not Due       | Not Due           |
| Va. Dept. of Ag. & Cons. Serv. | Yes            | 30                      | Yes                          | Yes           | Yes               |



# Secretariat: Commerce & Trade

| Agency  | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|---|----------------|-------------------------|------------------------------|---------------|-------------------|
| Board of Accountancy                            | Yes            | 0                       | Expired                      | Yes           | Not Due           |
| Dept. of Business Assistance                    | Yes            | 2                       | Yes                          | Not Due       | Not Due           |
| Dept. of Housing & Community Development        | Yes            | 1                       | Expired                      | Some          | No                |
| Dept. of Labor & Industry                       | Yes            | 3                       | No                           | N/A           | N/A               |
| Dept. of Mines, Minerals & Energy               | Yes            | 1                       | Expired                      | Yes           | Yes               |
| Dept. of Professional & Occupational Regulation | Yes            | 1                       | Expired                      | No            | N/A               |
| Tobacco Indemnification Commission              | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Economic Development Partnership            | Expired        | 0                       | No                           | N/A           | N/A               |
| Va. Employment Commission                       | Yes            | 2                       | Pending                      | Some          | Yes               |
| Va. Housing Development Authority               | No             | 1                       | No                           | N/A           | N/A               |
| Va. National Defense Industrial Authority       | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Racing Commission                           | Yes            | 1                       | Yes                          | No            | N/A               |
| Va. Resources Authority                         | No             | 0                       | No                           | N/A           | N/A               |



# Secretariat: Education

| Agency                                    | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|---|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Education                        | Yes            | 2                       | Expired                      | No            | N/A               |
| Frontier Culture Museum of Va.            | Yes            | 0                       | No                           | N/A           | N/A               |
| Gunston Hall                              | Yes            | 0                       | No                           | N/A           | N/A               |
| Jamestown - Yorktown Foundation           | Yes            | 1                       | Pending                      | Pending       | N/A               |
| Library of Va.                            | Yes            | 1                       | Expired                      | Not Due       | Not Due           |
| Science Museum of Va.                     | Yes            | 0                       | No                           | N/A           | N/A               |
| State Council of Higher Education for Va. | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Commission for the Arts               | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Museum of Fine Arts                   | Yes            | 2                       | Yes                          | Yes           | No                |



# Secretariat: Education (Cont'd)

| Agency                         | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Christopher Newport University | Yes            | 0                       | Yes                          | No            | N/A               |
| George Mason University        | Yes            | 1                       | Expired                      | Some          | Yes               |
| James Madison University       | Yes            | 0                       | Yes                          | Yes           | Some              |
| Longwood University            | Yes            | 1                       | Expired                      | Yes           | Yes               |
| Norfolk State University       | Yes            | 2                       | Yes                          | No            | N/A               |
| Old Dominion University        | Yes            | 1                       | Expired                      | Yes           | Some              |
| Radford University             | Yes            | 0                       | Yes                          | Yes           | Yes               |
| University of Mary Washington  | Yes            | 1                       | Yes                          | Not Due       | Not Due           |
| Va. Community College System   | Yes            | 43                      | Expired                      | Yes           | Yes               |
| Virginia Military Institute    | Yes            | 0                       | Expired                      | No            | N/A               |
| Virginia State University      | Yes            | 3                       | Yes                          | Not Due       | Not Due           |



# Secretariat: Finance

| Agency                     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|----------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Accounts          | Yes            | 4                       | Yes                          | No            | N/A               |
| Dept. of Planning & Budget | Yes            | 1                       | Yes                          | No            | N/A               |
| Dept. of Taxation          | Yes            | 0                       | Expired                      | Some          | Some              |
| Dept. of the Treasury      | Yes            | 3                       | Yes                          | Yes           | Some              |



# Secretariat: Health & Human Resources

| Agency   | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Health Professions  | Yes            | 0                       | Yes                          | Not Due       | Not Due           |
| Dept. of Medical Assistance Services                                   | Yes            | 4                       | Yes                          | Yes           | Yes               |
| Dept. of Mental Health, Mental Retardation, & Substance Abuse Services | Yes            | 20                      | Yes                          | No            | N/A               |
| Dept. of Rehabilitative Services                                       | Yes            | 0                       | Expired                      | No            | N/A               |
| Dept. of Social Services   | Yes            | 2                       | Expired                      | No            | N/A               |
| Tobacco Settlement Foundation  | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Dept. for the Aging  | Yes            | 0                       | Yes                          | Not Due       | Not Due           |
| Va. Dept. of Health  | Yes            | 3                       | Yes                          | Yes           | Yes               |



# Secretariat: Natural Resources

| Agency                             | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Conservation & Recreation | Yes            | 1                       | Expired                      | Some          | No                |
| Dept. of Environmental Quality     | Yes            | 4                       | Expired                      | Some          | Yes               |
| Dept of Game & Inland Fisheries    | Yes            | 2                       | Expired                      | Some          | Some              |
| Dept. of Historic Resources        | Yes            | 2                       | Expired                      | No            | No                |
| Marine Resources Commission        | Yes            | 3                       | Expired                      | Yes           | No                |
| Va. Museum of Natural History      | Expired        | 1                       | No                           | N/A           | N/A               |



# Secretariat: Public Safety

| Agency                                     | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--|----------------|-------------------------|------------------------------|---------------|-------------------|
| Alcoholic Beverage Control                 | Yes            | 4                       | Yes                          | Some          | Some              |
| Commonwealth's Attorneys' Services Council | Yes            | 0                       | No                           | N/A           | N/A               |
| Dept. of Correctional Education            | Yes            | 1                       | Yes                          | Not Due       | Not Due           |
| Dept. of Corrections                       | Yes            | 2                       | Expired                      | Some          | No                |
| Dept. of Criminal Justice Services         | Yes            | 2                       | Expired                      | Yes           | Not Due           |
| Dept. of Fire Programs                     | Yes            | 2                       | Yes                          | Not Due       | Not Due           |
| Dept. of Forensic Science                  | Yes            | 1                       | Expired                      | No            | N/A               |
| Dept. of Juvenile Justice                  | Yes            | 3                       | Expired                      | No            | N/A               |
| Dept. of Military Affairs                  | Expired        | 1                       | No                           | N/A           | N/A               |
| Dept. of Veterans Services                 | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Dept. of Emergency Management          | Yes            | 2                       | No                           | N/A           | N/A               |
| Va. State Police                           | Yes            | 3                       | Yes                          | Not Due       | Not Due           |



# Secretariat: Technology

| Agency                        | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|-------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| The Ctr for Innovative Tech.  | Yes            | 1                       | Expired                      | No            | N/A               |
| Va. Info. Technologies Agency | Yes            | 29                      | Yes                          | Not Due       | Not Due           |



# Secretariat: Transportation

| Agency                        | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|-------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Dept. of Aviation             | Yes            | 3                       | No                           | N/A           | N/A               |
| Dept. of Motor Vehicles       | Yes            | 2                       | Yes                          | Not Due       | Not Due           |
| Dept. of Rail & Public Trans. | Yes            | 0                       | Expired                      | Not Due       | Not Due           |
| Motor Vehicle Dealer Board    | Yes            | 0                       | No                           | N/A           | N/A               |
| Va. Dept. Of Transportation   | Yes            | 5                       | Yes                          | Yes           | Yes               |



# Independent Branch Agencies

| Agency                               | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--------------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Indigent Defense Commission          | Yes            | 5                       | Expired                      | No            | N/A               |
| State Corporation Commission         | Yes            | 2                       | Yes                          | Not Due       | Not Due           |
| State Lottery Dept.                  | Yes            | 2                       | No                           | N/A           | N/A               |
| Va. College Savings Plan             | Yes            | 3                       | Yes                          | No            | N/A               |
| Va. Office for Protection & Advocacy | Yes            | 1                       | Exception                    | Exception     | Not Due           |
| Va. Retirement System                | Yes            | 2                       | Yes                          | No            | N/A               |
| Va. Workers' Compensation Commission | Yes            | 3                       | Exception                    | Exception     | Not Due           |



# Others

| Agency                         | ISO Designated | Attended IS Orientation | Security Audit Plan Received | CAPs Received | Quarterly Updates |
|--------------------------------|----------------|-------------------------|------------------------------|---------------|-------------------|
| Office of the Attorney General | Yes            | 0                       | Yes                          | Not Due       | Not Due           |
| Office of the Governor         | Yes            | 1                       | Exception                    | Exception     | Not Due           |



# Host-based Intrusion Prevention System (HIPS)

*Eric Taylor*  
*IT Infrastructure Partnership Team*



# Agenda

- What is *Host-based Intrusion Prevention System (HIPS)*
- Benefits
- Server HIPS
  - Recommendations for deployment
  - System Requirements
  - Installation
  - Baseline Configuration
  - Questions

## What is *Host-based Intrusion Prevention System*?

- HIPS is a security software package that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.
- HIPS technology is designed to protect Servers against external & internal exploits, and has traditionally been deployed on critical assets such as e-Commerce servers, dynamic Web servers, Mail servers, DNS servers, Database servers, File & Print servers, ERP Systems, and so on.
- HIPS prevents the following from being used to attack a system:
  - known exploits
  - unknown exploits against known vulnerabilities
  - unknown exploits that attempt to exploit a system by abusing a specific protocol

## Benefits

- HIPS can help Agencies achieve and maintain compliance with regulations that require security against malicious threats which may compromise servers and sensitive data
- HIPS can handle encrypted and unencrypted traffic equally, because it can analyze the data after it has been decrypted on the host.
- “Virtual patch” protection: Protects servers before traditional definitions are posted, voiding emergency patch rollouts.
- Data security and integrity controls: File Integrity, OS Audit Log and Registry Integrity Monitoring
- HIPS complements traditional finger-print-based and heuristic antivirus detection methods, since it does not need continuous updates to stay ahead of new malware.

## The Business Case for Host-based Intrusion Prevention

- *“Security flaws and errors found in software are responsible for the exploits that lead to identity theft, unauthorized funds transfer and fraud, costing the U.S. economy \$59.5 billion per year.”*
  - *National Institute of Standards and Technology.*
- *The most common methods used to defend against worms today are reactive, e.g., virus- scanning, or software-patching. These mechanisms have no hope of preventing fast spreading worms, or worms that use zero-day exploits to carry out their attacks.*
  - *The Case for Using Layered Defenses to Stop Worms(NSA)*
- The Benefit of a Patch Without the Downtime

# ***Server Host-based Intrusion Prevention System (HIPS)***

# Recommendations for deployment

- Internet / public web server and database servers
- Internet / public application servers
- Application, File and Database Servers that contain
  - HIPPA or Electronic Protected Health Information (EPHI)
  - Personally Identifiable Information (PII)
  - PCI cardholder data
  - TAX Data
  - Sensitive Data
- Enterprise Infrastructure Servers
  - NGC will assume costs for enterprise infrastructure servers

# Recommendations for deployment

- Defining the servers will require Agency support
  - The partnership will request Agency support for defining the HIPS candidate servers
- ITP is developing a cost unit per server for this service
- If desired, Agencies will purchase this service from ITP for additional servers
  - Help ensure compliancy with Sec 501. If encrypted in-transit end to end, network intrusion detection and prevention can not interrogate the data stream.
    - Encryption 6.2.2 - 3 - Require encryption during transmission of data that is sensitive relative to confidentiality and integrity.
    - Threat Detection 9.2 - Threat Detection requirements identify the practices for implementing intrusion detection and prevention

# System Requirements

| Windows  | Unix/Linux  |
|--|---|
| <p><u>Windows Server 2003 (EM64T, AMD64)</u></p> <ul style="list-style-type: none"> <li>• Windows Server 2003 SP2 Standard Edition</li> <li>• Windows Server 2003 SP2 Enterprise Edition</li> <li>• Windows Server 2003 R2 Standard Edition</li> <li>• Windows Server 2003 R2 Enterprise Edition</li> </ul> <p><u>Windows Server 2003 (32-bit)</u></p> <ul style="list-style-type: none"> <li>• Windows Server 2003 SP2 Standard Edition</li> <li>• Windows Server 2003 SP2 Enterprise Edition</li> <li>• Windows Server 2003 R2 Standard Edition</li> <li>• Windows Server 2003 R2 Enterprise Edition</li> <li>• Windows Server 2003 SP1 Standard Edition</li> <li>• Windows Server 2003 SP1 Web Edition</li> <li>• Windows Server 2003 SP1 Enterprise Edition</li> </ul> <p><u>Windows 2000 Server</u></p> <ul style="list-style-type: none"> <li>• Windows 2000 Server SP4</li> <li>• Windows 2000 Advanced Server SP4</li> </ul> | <p>Red Hat Enterprise Linux (RHEL) 5.0 BS/AS<br/>                     Red Hat Enterprise Linux (RHEL) 4.0 AS/ES<br/>                     Red Hat Enterprise Linux (RHEL) 3.0 AS/ES (32-bit only)<br/>                     SuSE Linux Enterprise Server (SLES) 9 SP3<br/>                     SuSE Linux Enterprise Server (SLES) 10 SP1<br/>                     SuSE Linux Enterprise Server (SLES) 10 SP2</p> <p>NOTE: SSL inspection is NOT available for 64-bit versions of Apache<br/>                     Red Hat Enterprise Linux with SELinux enabled is NOT supported.</p> |

Supports the stated operating systems and kernel versions running in virtual machines on the following VMware platforms: ESX 3.0.x & ESX 3.5.x

# Installation

- Agency must be on the transformed network
  - Network Communications over port 3995 HTTP (SSL)
- Installation is done by the server team or local service delivery
- Special considerations needed for deployment over RDP
- Installation is documented in Installation Procedures & Baseline Policy
  - This will be delivered with the Agent software
- The installation of the HIPS application may take a noticeably longer time on some systems than others. During the installation of the Agent, the Buffer Overflow Exploit Prevention (BOEP) module needs to analyze certain Windows components.
- Security Engineer will be available for installation and troubleshooting

# Baseline Configuration

- **Firewall**
  - Trusting - All ports remain open and unblocked allowing all inbound traffic.
- **Security Events (IPS)**
  - Alert only (IDS) - Sends an alert to the management console but does not block the intrusion
- **Buffer Overflow Exploit Prevention (BOEP)**
  - Alert only (IDS) - Sends an alert to the management console but does not block the intrusion
- **Bypass Filters**
  - Security Expressions Compliancy Scanners
  - ISS Enterprise Vulnerability Assessment Scanners
- **File Integrity Monitoring**
- **System Integrity Monitoring**

# Baseline Configuration

- How do we get to IPS mode on servers ???
  - When can we get to blocking mode?
    - Once we gather enough events (at least month), then these events will be analyzed to exclude trusted traffic, this will be in conjunction with the system admin. Then we'll follow to next stage UAT prior to deployment.
  - Is the Agency expected to help?
    - During UAT phases, Agencies will be expected to work with Security Engineers to ensure the applied policy don't cause a major application outage.
  - Part of change control, correct?
    - Each location must follow the change control method(s) as normal. For policy changes we will be following change control after UAT is completed.





# What is an EISP?

## Assessing the Self-Assessment—Way Forward

*Leonard Price / Michael Clark  
PSO Planning & Compliance Office*



**NORTHROP GRUMMAN**

# Current Version – 2.1

- Enterprise Infrastructure Security Practices
  - Purpose of document
    - Provide security “best” practices regarding SEC501
      - Guidance to NG management and administration
- Scope of Document
  - SEC 501 used for direction in content of EISP
  - Assisted with compliance to VITA Standards and Policies
  - Applied to all NG employees, partners, contractors, vendors
    - Agencies
    - CESC

# Future of EISP

- New Version 3 Scope
  - Rewrite of current version to coincide with:
    - SEC501
    - VITA Policies and Standards
    - Northrop Grumman Procedures Manuals
  - Give detail of “How To” comply
    - Steps to performing different functions required
  - Provide links to appropriate NG Procedures Manual for greater detail
  - Stay updated with changes in SEC501 and other standards/policies

# Communication of Release

- New version approval
- Place on Program Security Office page
  - <https://vitaweb.virginia.gov/sites/ngpsso/default.aspx>
- AOM's to receive hard and soft copy
- Email sent out announcing new version of EISP

# Past Self-Assessments

- Purpose
  - Assess Agency/NG compliance with COV ITRM Standard SEC501-01.
- Analysis indicates
  - 2007 and 2008 Self-Assessments (SA) results did not return an optimal reflection of the status of NG managed security services.
  - SA Responses
    - ITP retains documented procedures and processes...but...
      - What are they and how do they relate to managed services?
    - Transformation – Although a sound business decision, how are security services actualized until completion of transformation.
    - VITA Exceptions – Annotated as submitted, but no synopsis of what the exception requested or remediation strategy.
    - Some SAs were not returned with all areas annotated, should have stated non-applicable and provide justification.

## Past Self-Assessments

- Process lacked guidance to the personnel conducting the SA.
- Personnel conducting SAs were not the subject matter experts (SME) concerning all areas reviewed related to SEC501-01.
- Quarterly Updates
  - Non-remediated items from 2008 SA related to managed services become part of 2009 SA.
  - Transformation of top 20 agencies and third-party audit season impacted resource availability.
  - 2009 SA to utilize different more manageable approach.
- Recent discussions within the Partnership identified
  - SAs need to reflect the security posture for NG Managed Services based against the NG document, Enterprise Infrastructure Security Practices (EISP).
  - SA focus entails NG managed security services provided to all agencies.
  - The process requires a robust reporting structure to agencies and NG Towers.

# Way Forward - 2009 Self-Assessment

- New process – parsing the process
  - Enhancing Security Control framework to improve process results.
  - Utilize the new NG Managed Services organizations such as...
    - Back-up Tower for back-ups
    - Server Tower for servers
    - Security Operations for firewalls
  - Delivers the assessment to the SMEs who best know the applicable processes and procedures and can supply comprehensive responses.
  - 2009 SA begins in first half of July 09.
  - The SMEs provide responses in 6 weeks.
  - The Planning and Compliance team conducts correlation and analysis of responses; then, provides first reports beginning at the end of September 09.
  - The sharelink VITAwab Program Security Office (PSO) site identified as a repository for the reports using Access Control List for each agency.

# Way Forward - 2009 Self-Assessment

- New Process continued
  - Develop a two-way communication structure with Agencies.
  - Reports
    - Assessment: Overall responses by SME for an agency
    - Remediation plan:
      - Planning and Compliance recommended remediation actions.
      - NG Managed Service agency personnel solidify remediation plan.
      - Remediation efforts scheduled for 1 Oct with target completion date of 11 Dec 09.
  - Planning and Compliance team correlates process efforts and post remediation status reports on PSO VITAweb sharelink site on monthly basis.
  - Planning and Compliance team conducts trend analysis and re-testing based on analysis results and/or Agency concerns.

**QUESTIONS?**



## SPAM, Phishing, & other Junk email

Bob Baskette: CISSP, CCNP  
Commonwealth Security  
Incident Management Engineer



# SPAM and the Flying Circus

- Spam is the intentional abuse or misuse of electronic messaging systems to send unsolicited bulk messages.
- 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.



# SPAM, SPAM, SPAM, SPAM, SPAM

- In November 2008, the McColo ISP, which was providing service to botnet operators, was shutdown and SPAM dropped 50%-75% Internet-wide.
- Instant Messaging SPAM, AKA SPIM makes use of instant messaging systems since instant messaging is not usually blocked by firewalls.
- Mobile phone SPAM is directed at the mobile text messaging service. Mobile phone SPAM can have a dual economic impact since most mobile phone users have a limited number of free text messages per month and many financial institutions are now using text messages to relay financial information.
- Spamdexing refers to the practice of modifying HTML pages of public web servers to increase the chances of those web servers being placed high on search engine relevancy lists. These websites use search engine optimization techniques to unfairly increase their rank in search engines.
- Video sharing sites, such as YouTube, are now being frequently targeted by spammers. The most common technique uses people or compromised computers to post links to sites, most likely illicit or online dating, on the comments section of random videos or people's profiles.



# 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.



# SPAM verses Phishing

- SPAM is intended to advertise products, services, or ideologies.
- SPAM servers as the modern version of the bulk mail from the United States Postal Service.
- Phishing is intended to steal information from the recipient.
- Phishing is directed at a service or product that you already have while SPAM is intended to sell you something new.



# IRS-related Phish

**From:** Internal Revenue Service [mailto:urgent@irs.gov]  
**Sent:** Saturday, January 03, 2009 10:16 AM  
**To:** undisclosed-recipients  
**Subject:** Refund Taxes of 2008 Urgent Note

Dear Applicant:

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund under section 501(c) (3) of the Internal Revenue Code. Tax refund value is \$402.50.

Please submit the tax refund request and allow us 3-6 days in order to IWP the data received.

If you are customer of : E\*Trade

Mazuma C.U.

COUNTY OF HENRICO F.C.U.

1ST CITY C.U.

NORTHERN STAR C.U.

MONEY ACCESS SERVICE

ZIP NETWORK ,

you will receive an additional \$172.00 after last annual calculations of your bank activity.

To access the form for your tax refund, please click here (or please copy/paste the link below in your browser) :

<http://www.IRS.gov/refunds/tax.php>

This notification has been sent by the Internal Revenue Service, a bureau of the Department of the Treasury.

---

Note:

- If you received this message in your SPAM/BULK folder, that is because of the restrictions implemented by your ISP
- For security reasons, we will record your ip address, the date and time.
- Deliberate wrong inputs are criminally pursued and indicted.

© Copyright 2008, Internal Revenue Service U.S.A.

Tax ID :



# IRS Phish Headers

Microsoft Mail Internet Headers Version 2.0

Received: from covmsgces-ebh02.cov.virginia.gov ([10.192.3.45]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Sat, 3 Jan 2009 10:15:43 -0500

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh02.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Sat, 3 Jan 2009 10:15:43 -0500

X-SBRS: 5.3

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.36,322,1228107600";  
d="scan'208,217";a="186547145"

**Received: from mail108c26.carrierzone.com ([64.29.152.118])**

by CMailA.vita.virginia.gov with ESMTTP/TLS/DHE-RSA-AES256-SHA; 03 Jan 2009  
10:15:43 -0500

X-Authenticated-User: jessie.jaxnet.net

**Received: from User ([91.140.231.98])**

(authenticated bits=0)

by mail108c26.carrierzone.com (8.13.6.20060614/8.13.1) with ESMTTP id  
n03FFSDM009493;

Sat, 3 Jan 2009 15:15:32 GMT

Message-Id: <[200901031515.n03FFSDM009493@mail108c26.carrierzone.com](mailto:200901031515.n03FFSDM009493@mail108c26.carrierzone.com)>

**Reply-To: <[Internal.Revenue.Service@mail108c26.carrierzone.com](mailto:Internal.Revenue.Service@mail108c26.carrierzone.com)>**



## IRS Phish Headers

**From: "Internal Revenue Service" <[urgent@irs.gov](mailto:urgent@irs.gov)>**

Subject: Refund Taxes of 2008 Urgent Note

Date: Sat, 3 Jan 2009 18:15:39 +0300

MIME-Version: 1.0

Content-Type: text/html;  
charset="Windows-1251"

Content-Transfer-Encoding: 7bit

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2600.0000

X-MimeOLE: Produced By Microsoft MimeOLE

V6.00.2600.0000

To: undisclosed-recipients:;

**Return-Path: [urgent@irs.gov](mailto:urgent@irs.gov)**

X-OriginalArrivalTime: 03 Jan 2009 15:15:43.0542 (UTC)

FILETIME=[2561ED60:01C96DB6]



## IRS Phish Domain Information

**Date of receipt:** 2009-01-03

**Subject of Phishing:** Refund Taxes of 2008  
Urgent Note

**Fake URL:** <http://www.IRS.gov/refunds/tax.php>

**Actual URL:**

<http://75.150.62.234/internal/revenue/service/index.html>

**Sender name:** Internal Revenue Service  
[mailto:urgent@irs.gov]

**Sender IP-address:** 91.140.231.98 (Kuwait,  
Gulfnet)



## Additional Fake IRS Domains

**Date of receipt:** 2009-03-08

**Subject of Phishing:** Tax Refund from  
Department of the Treasury

**Fake URL:** <http://www.IRS.gov/refunds/tax.php>

**Actual URL:**

<http://58.181.36.135/internal/revenue/service/index.html>

**Sender name:** "Internal Revenue  
Service" [tax@irs.gov](mailto:tax@irs.gov)

**Sender IP-address:** 77.104.228.1 (Czech  
Republic, Pardubicky Kraj, Chrudim)

**URL IP-Address:** 58.181.36.135 (Korea, Republic  
of, Seoul-t'ukpyolsi, Seoul)



# Email Account Phish

-----Original Message-----

From: Login Webmail [mailto:jkeller@brocku.ca]

Sent: Saturday, January 31, 2009 9:27 AM

To: undisclosed-recipients

Subject: Your Account Expires in 2 Day(s)

The Helpdesk Program that periodically checks the size of your e-mail space is sending you this information. The program runs weekly to ensure your inbox does not grow too large, thus preventing you from receiving or sending new e-mail. As this message is being sent, you have 18 megabytes (MB) or more stored in your inbox. To help us reset your space in our database, please enter your current user name

( \_\_\_\_\_ ) password ( \_\_\_\_\_ )

You will receive a periodic alert if your inbox size is between 18 and 20 MB. If your inbox size is 20 MB, a program on your Webmail will move your oldest e-mails to a folder in your home directory to ensure you can continue receiving incoming e-mail. You will be notified this has taken place.

If your inbox grows to 25 MB, you will be unable to receive new e-mail and it will be returned to sender. All this is programmed to ensure your e-mail continues to function well.

Thank you for your cooperation.

Help Desk



# Email Account Phish Headers

Received: from covmsgces-ebh01.cov.virginia.gov ([10.192.3.25]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);  
Sat, 31 Jan 2009 09:26:53 -0500

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh01.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);  
Sat, 31 Jan 2009 09:26:53 -0500

X-SBRS: 5.3

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.37,355,1231131600";  
d="scan'208";a="194323924"

Received: from outpostal.ac.brocku.ca ([139.57.65.198])  
by CMailA.vita.virginia.gov with ESMTP; 31 Jan 2009 09:26:52 -0500

**Received: from newwebmail.ac.brocku.ca (newwebmail.ac.brocku.ca [139.57.65.70])**  
by outpostal.ac.brocku.ca (8.13.8/8.13.8) with ESMTP id n0VEQbXN002442;  
Sat, 31 Jan 2009 09:26:37 -0500

Received: from newwebmail.ac.brocku.ca (newwebmail.ac.brocku.ca [127.0.0.1])  
by newwebmail.ac.brocku.ca (8.13.1/8.13.1) with ESMTP id n0VEQiJS028604;  
Sat, 31 Jan 2009 09:26:45 -0500

Received: (from apache@localhost)  
by newwebmail.ac.brocku.ca (8.13.1/8.13.1/Submit) id n0VEQh1e028603;  
Sat, 31 Jan 2009 09:26:43 -0500

X-Authentication-Warning: newwebmail.ac.brocku.ca: apache set sender to jkeller@brocku.ca using -f

**Received: from 80.255.59.243 ([80.255.59.243]) by webmail.brocku.ca (Horde**  
MIME library) with HTTP; Sat, 31 Jan 2009 09:26:39 -0500

Message-ID: <20090131092639.as7gb1opic0wwwcs@webmail.brocku.ca>



# Email Account Phish Headers

Date: Sat, 31 Jan 2009 09:26:39 -0500

**From: Login Webmail <jkeller@brocku.ca>**

**Reply-to: helpweb11@yahoo.com.hk**

To: undisclosed-recipients;

Subject: Your Account Expires in 2 Day(s)

MIME-Version: 1.0

Content-Type: text/plain;

charset=ISO-8859-1;

DelSp="Yes";

format="flowed"

Content-Disposition: inline

Content-Transfer-Encoding: quoted-printable

User-Agent: Internet Messaging Program (IMP) H3 (4.1.2)

X-Virus-Scanned-By: outpostal.ac.brocku.ca, using ClamAV 0.88.4

X-Scanned-By: MIMEDefang 2.58 on 139.57.65.198

**Return-Path: jkeller@brocku.ca**

X-OriginalArrivalTime: 31 Jan 2009 14:26:53.0517 (UTC)

FILETIME=[F68497D0:01C983AF]



# Email Phish Domain Information

**Date of receipt:** 2009-01-31

**Subject of Phishing:** Your Account Expires in 2 Day(s)

**Fake URL:** N/A

**Actual URL:** N/A

**Sender name:** Login Webmail [mailto:jkeller@brocku.ca]

**Sender IP-address:** 80.255.59.243 (Nigeria)

**Domain information:** brocku.ca

Approval date: 2000/10/19

Renewal date: 2017/08/15

Registrar:

Name: Canadian Domain Name Services Inc.

Number: 140

Registrant:

Name: Brock University

Number: 26519

Description: Brock University is a degree granting academic organization.



## Financial Phish

-----Original Message-----

From: MARKADAMS [<mailto:markadams@host63.hrwebservices.net>]

Sent: Wednesday, March 04, 2009 2:54 AM

To: Removed-by-CSR

Subject: INVESTMENT

Dear Sir/Madam

It is with heartfelt hope that I write to seek your co-operation and assistance in my desire to invest into Estate properties in your country.

Briefly, I am Mark Adams, I am an Administrative Staff of Department Of Petroleum Resources(DPR).

I represent a group that is interested in engaging your services for investment and humanitarian purposes of a large volume of fund.

Please if you are ready to render the needed assistant get back to me, so that we can work out the procedure for the execution of this transaction.

Please reach me via my private e-mail address: [drm45adams@yahoo.com](mailto:drm45adams@yahoo.com) together with your private telephone number for easy reach.

Thanks for your co-operation.

Best Regards

Mark Adams



# Financial Phish Headers

Received: from covmsgces-ebh01.cov.virginia.gov ([10.192.3.25]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Wed, 4 Mar 2009 02:54:29 -0500

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh01.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Wed, 4 Mar 2009 02:54:29 -0500

X-SBRS: 5.3

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.38,299,1233550800";  
d="scan'208";a="204320452"

Received: from relay1.hrnoc.net ([216.120.226.254])

by CMailA.vita.virginia.gov with ESMTP/TLS/DHE-RSA-AES256-SHA; 04 Mar 2009  
02:54:29 -0500

**Received: from host63.hrwebservices.net ([216.120.241.16])**

by relay1.hrnoc.net with esmtp (Exim 4.63)

(envelope-from <nobody@host63.hrwebservices.net>)

id 1LelVe-0004MA-RA

for billy.shelton@vdfp.virginia.gov; Wed, 04 Mar 2009 02:54:10 -0500

Received: from nobody by host63.hrwebservices.net with local (Exim 4.69)

(envelope-from <nobody@host63.hrwebservices.net>)

id 1LelvP-00059Q-Jz

for Removed-by-CSR; Wed, 04 Mar 2009 02:53:55 -0500



# Financial Phish Headers

To: Removed-by-CSR

Subject: INVESTMENT

**From: MARKADAMS <markadams@host63.hrwebservices.net>**

**Reply-To: mark25adams@uku.co.uk**

MIME-Version: 1.0

Content-Type: text/plain

Content-Transfer-Encoding: 8bit

Message-Id: <E1LelVP-00059Q-Jz@host63.hrwebservices.net>

Date: Wed, 04 Mar 2009 02:53:55 -0500

X-AntiAbuse: This header was added to track abuse, please include it with any abuse report

X-AntiAbuse: Primary Hostname - host63.hrwebservices.net

X-AntiAbuse: Original Domain - vdfp.virginia.gov

X-AntiAbuse: Originator/Caller UID/GID - [99 99] / [47 12]

X-AntiAbuse: Sender Address Domain - host63.hrwebservices.net

X-HR-Scan-Signature: 06d900a217027daee363edd08c15fb37

X-HR-ClamAV-Scan: Clear

X-HR-SA-Score: 5.7 (+++++)

X-HR-Status: Normal-(nobody@host63.hrwebservices.net/216.120.241.16)

Return-Path: nobody@host63.hrwebservices.net

X-OriginalArrivalTime: 04 Mar 2009 07:54:29.0267 (UTC)



## Financial Phish Domain Information

**Date of receipt:** 2009-03-04

**Subject of Phishing:** INVESTMENT

**Fake URL:** N/A

**Actual URL:** N/A

**Sender name:**

[markadams@host63.hrwebservices.net](mailto:markadams@host63.hrwebservices.net)

**Sender IP-address:** 216.120.241.16 (United States, New York, Clifton Park)

**Domain information:**

uku.co.uk ISP located in UK.



## SPAM – Potential Phish

**From:** Rob Atkins [mailto:a19@oneaxisng.co.cc]

**Sent:** Wednesday, March 04, 2009 1:55 PM

**Subject:** Get paid to shop. Get paid to spend money

We are accepting applications from qualified individuals to become Secret Surveyors. We have an assignment in your area and we would like you to participate.

Survey Profits is an internet based customer experience management agency. Our clientele includes businesses in many countries. We serve clients in every region and have a growing membership of about 100,000 members worldwide.

We provide customer experience management services to our clients and businesses worldwide. By so doing our clients are able to serve their own end customers better. One of our tasks is to evaluate the quality of businesses and financial services in your area, businesses like WAL-MART, WESTERN UNION, BANKS, MONEYGRAM, HOSPITALS, RESTAURANTS, HOTELS and other business franchise or financial services etc.

This is done through your assistance as a Secret Surveyor. As a Secret Surveyor you get paid to conduct a Simple Survey and provide valuable Customer Service Feedback to us. Your feed back is used to prepare our evaluation which is then presented to our clients that is all. You will be required to visit businesses and franchise locations like stores, restaurants, banks, movie theaters, hotels and other businesses in your area as an 'undercover customer'. Your job is just to act like any regular customer and perform a normal business transaction while you conduct a simple survey and gather information about the quality of service by staff, behavior of staff and other issues at such locations.



## SPAM – Potential Phish

You will be given an assignment to perform which will deal with reported issues about businesses in your area and you will be asked to go as a undercover customer to such locations. During the assignment you will visit the locations and make several observations as regards the customer service. You will be required to interact with the shop clerk or staff. Please note; you are not spending your own money for any assignment. All funds required will be provided by our clients and sent to you to complete your assignment. You only need to perform your task successfully and give us feed back.

Registration is FREE. You will also be paid in full in advance to perform your assignment. In your case you will be paid 200 dollars for each survey assignment you undertake. Also on top of being paid you are also allowed to keep purchases made if any purchase was done by you during any assignment.

If you are interested then kindly send the required information below for registration and membership and join a growing network of about 100,000 members in the US, Canada, China, Asia, Europe, Middle East and Africa. I assure you that we will respect your privacy and your information is very well protected with the very best and robust encryption technology in the market place and very safe with us. Note; we reserve the right to decline any application for membership.



# SPAM – Potential Phish

Kindly send us an email with ALL the details requested below. Incomplete information will not be accepted. We will get back to you shortly with an assignment in your area.

**PERSONAL INFORMATION:**

- First Name;
- Last Name;
- Age;
- Street Address;
- City;
- State;
- Zip Code;
- Country;
- Cell Phone Number;
- Home Phone Number;
- Current Occupation (If employed);
- Preferred Email Address (if any);

**AVAILABILITY:**

- Days and Hours You Are Always Available
- Monday .....
- Tuesday .....
- Wednesday .....
- Thursday .....
- Friday .....
- Saturday .....
- Sunday .....
- Hours Available: from \_\_\_\_\_ to \_\_\_\_\_

NOTE: IF this message is in your bulk/spam folder transfer to your in-box before you reply..

Thank you for your time. We look forward to working with you.  
 Sincerely,  
 Rob Atkins  
 Survey Profits



# SPAM Headers

Received: from covmsgces-ebh01.cov.virginia.gov ([10.192.3.25]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);  
Wed, 4 Mar 2009 13:55:37 -0500  
Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh01.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);  
Wed, 4 Mar 2009 13:55:37 -0500  
X-SBRS: 4.5  
X-HAT: Group: None, Policy: \$ACCEPTED  
X-IronPort-Anti-Spam-Filtered: true  
X-IronPort-Anti-Spam-Result:  
AvrLABddrknRVdugkWdsb2JhbAASggwziCOBb4Z0A2k/AQEBAQkJDAcPMZ1SmDeMeYJ  
JAYE+BoZs  
X-SUSPECT-SPAM: ID'ed as SUSPECTED SPAM by Ironport!  
X-IronPort-AV: E=Sophos;i="4.38,302,1233550800";  
d="scan'208";a="204485379"  
**Received: from mail-ew0-f160.google.com ([209.85.219.160])**  
by CMailA.vita.virginia.gov with ESMTP; 04 Mar 2009 13:55:37 -0500  
Received: by ewy4 with SMTP id 4so1520239ewy.8  
for <Removed-by-CSRMS>; Wed, 04 Mar 2009 10:55:36 -0800 (PST)  
MIME-Version: 1.0  
Received: by 10.216.11.84 with HTTP; Wed, 4 Mar 2009 10:54:53 -0800 (PST)  
**Reply-To: [applications@axistwong.co.cc](mailto:applications@axistwong.co.cc)**  
Date: Wed, 4 Mar 2009 19:54:53 +0100  
Message-ID: <[c6cf84bd0903041054j2ffa77a5xfa532cebb808cee0@mail.gmail.com](mailto:c6cf84bd0903041054j2ffa77a5xfa532cebb808cee0@mail.gmail.com)>  
Subject: Get paid to shop. Get paid to spend money  
**From: Rob Atkins <[a19@oneaxisng.co.cc](mailto:a19@oneaxisng.co.cc)>**



## SPAM – Potential Phish

**Date of receipt:** 2009-03-04

**Subject of Phishing:** Get paid to shop. Get paid to spend money

**Fake URL:** N/A

**Actual URL:** N/A

**Sender name:** Rob Atkins <[a19@oneaxisng.co.cc](mailto:a19@oneaxisng.co.cc)>

**Sender IP-address:** 209.85.219.16 (United States, California, Mountain View)

**Sender IP-address:** 118.219.232.248 (KOREA REPUBLIC OF, KYONGGI-DO)



## Traditional Phish

-----Original Message-----

From: Solomon Ngige [<mailto:office1199@handbag.com>]

Sent: Wednesday, March 11, 2009 5:46 PM

Subject: Very Important !!!!

Hello Friend.

I am Solomon Ngige A family friend to a wife of a late farmer on her intention to invest the sum of US\$42M in a more developed country being money left for her family by her late husband who is dead. I advised her to have patience as I will source for a reliable and trust-worthy investor who can receive, invest and manage the money very well for her.

Intrested please get back to me.

Solomon Ngige

---

Tiscali Broadband from 14.99 with free setup!  
<http://www.tiscali.co.uk/products/broadband/>



## Traditional Phish Header

Received: from DITOWA.ditlan.dit.state.va.us ([172.22.254.22]) by DITEXCHANGE3-CL.ditlan.dit.state.va.us with Microsoft SMTPSVC(6.0.3790.3959);

Wed, 11 Mar 2009 17:46:19 -0400

Received: from CMailA.vita.virginia.gov ([166.67.65.181]) by DITOWA.ditlan.dit.state.va.us with Microsoft SMTPSVC(6.0.3790.1830);

Wed, 11 Mar 2009 17:46:19 -0400

X-SBRS: 5.6

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.38,345,1233550800";  
d="scan'208";a="206232572"

**Received: from mk-filter-1-a-2.mail.uk.tiscali.com ([212.74.100.48])**

by CMailA.vita.virginia.gov with ESMTMP; 11 Mar 2009 17:46:18 -0400

X-Trace: 165644108/mk-filter-1.mail.uk.tiscali.com/WEBB2C/\$webb2c-  
ALLOWED\_RELAY/webb2c-ALLOWED-B2C-  
WEBMAIL/212.74.100.141/None/office1199@handbag.com

X-SBRS: None

X-RemoteIP: 212.74.100.141

**X-IP-MAIL-FROM: office1199@handbag.com**



## Traditional Phish Header

**Received: from mail-1.uk.tiscali.com ([212.74.100.141])**

by websmtp.tiscali.co.uk with ESMTP; 11 Mar 2009 21:46:17 +0000

**Received: from [41.222.192.69] by mail-1.uk.tiscali.com with HTTP;**

Wed, 11 Mar 2009 22:46:14 +0100

Date: Wed, 11 Mar 2009 09:46:14 -1200

Message-ID: <499EFA2A00001E84@mail-1-uk.mail.tiscali.sys>

From: "Solomon Ngige" <office1199@handbag.com>

Subject: Very Important !!!!

Reply-To: office1999@handbag.com

MIME-Version: 1.0

Content-Type: text/plain; charset="US-ASCII"

Content-Transfer-Encoding: 7bit

Bcc:

Return-Path: office1199@handbag.com

X-OriginalArrivalTime: 11 Mar 2009 21:46:19.0276 (UTC)

FILETIME=[CFD864C0:01C9A292]



# Traditional Phish Domain Information

**Date of receipt:** 2009-03-11

**Subject of Phishing:** Very Important !!!!

**Fake URL:** N/A

**Actual URL:** N/A

**Sender name:** "Solomon Ngige" [office1199@handbag.com](mailto:office1199@handbag.com)

**Sender IP-address:** 41.222.192.69 (BEN, Benin)

**Domain information:** handbag.com

Domain Name..... handbag.com

Creation Date..... 1999-02-27

Registration Date.... 2007-05-16

Expiry Date..... 2009-09-24

Organisation Name.... Handbag.com Limited

Organisation Address. 72 Broadwick Street

Organisation Address.

Organisation Address. London

Organisation Address. W1F 9EP

Organisation Address. London

Organisation Address. GREAT BRITAIN (UK)



## Job Offer Phish

From: colin.peters@homecall.co.uk [<mailto:colin.peters@homecall.co.uk>]  
Sent: Sunday, March 15, 2009 9:05 AM  
Subject: Orlen Vera-----Job Position( Opportunity Knocks! )

VACANCY ! VACANCY!! VACANCY!!!

Dear Sir/Madam,

No one is immune from the economic crisis. Don't wait until you're one of the millions of unemployed. You can make your life recession-proof, with our PKN ORLEN VERVA Companies. You and your family can survive this terrible recession by working on a part time basis as a finance manager for this company.

You will be entitled to certain percentage on any payment you received and processed successfully.

Reply: shop1vervafuels@hotmail.com



## Job Offer Phish

BELOW ARE THE INFORMATION REQUIRED FROM YOU:

- \* Full Name.
- \* Residential Address (In Full, Not P.O.BOX).
- \* Zip Code
- \* City
- \* State
- \* Contact Phone number(S).
- \* Email.
- \* Age.
- \* Occupation.
- \* Financial Institution.

Kindly get back at with the required information if you are interested,we will provide detail information on the job description to you.

Warm Regards

Torsten Rieger,

PKN ORLEN ,

+447024076586

Web site: [www.verva.pl](http://www.verva.pl)

Email: [shop1vervafuels@gmail.com](mailto:shop1vervafuels@gmail.com)

NOTE: IGNORE THIS EMAIL IF YOU ARE THE BUSY TYPE THAT WILL NOT BE ABLE TO CHECK YOUR EMAIL DAILY.



## Job Offer Phish Headers

Received: from covmsgces-ebh01.cov.virginia.gov ([10.192.3.25]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Sun, 15 Mar 2009 09:05:02 -0400

Received: from CMailB.vita.virginia.gov ([10.193.13.182]) by covmsgces-ebh01.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Sun, 15 Mar 2009 09:05:01 -0400

X-SBRS: 4.5

X-HAT: Group: None, Policy: \$ACCEPTED

X-IronPort-Anti-Spam-Filtered: true

X-IronPort-Anti-Spam-Result:

ApU0AFOavEnUSmQ0kWdsb2JhbABOXIscKgg0g0KDMx+BAQEBAQEJCwoH  
EQMshWaII5Ng38GYyQi

X-IronPort-AV: E=Sophos;i="4.38,366,1233550800";  
d="scan'208";a="178802490"

**Received: from mk-filter-1-a-1.mail.uk.tiscali.com ([212.74.100.52])**

by CMailB.vita.virginia.gov with ESMTP; 15 Mar 2009 09:04:58 -0400

X-Trace: 167525939/mk-filter-1.mail.uk.tiscali.com/B2C/\$b2c-  
ALLOWED\_RELAY/b2c-SMARTHOST-  
RELAY/212.74.112.92/None/colin.peters@homecall.co.uk



# Job Offer Phish Headers

**Received: from mk-webmail-2.b2b.uk.tiscali.com ([212.74.112.92])**

by smtp.tiscali.co.uk with ESMTP; 15 Mar 2009 13:04:55 +0000

Received: from exim by mk-webmail-2.b2b.uk.tiscali.com with local (Exim 4.69)

(envelope-from <colin.peters@homecall.co.uk>)

id 1Liq1N-000BhH-2r; Sun, 15 Mar 2009 13:04:53 +0000

From: colin.peters@homecall.co.uk

Reply-To: shop1vervafuels@hotmail.com

Subject: Orlen Vera-----Job Position( Opportunity Knocks! )

Date: Sun, 15 Mar 2009 13:04:51 +0000

Mime-Version: 1.0

Content-Type: text/plain; charset="utf-8"; format=flowed

Content-Transfer-Encoding: 7bit

Message-Id: <E1Liq1N-000BhH-2r@mk-webmail-2.b2b.uk.tiscali.com>

Bcc:

Return-Path: colin.peters@homecall.co.uk

X-OriginalArrivalTime: 15 Mar 2009 13:05:01.0807 (UTC)

FILETIME=[A6AC5FF0:01C9A56E]



## Job Offer Phish Domain Information

**Date of receipt:** 2009-03-15

**Subject of Phishing:** Orlen Vera-----Job  
Position( Opportunity Knocks! )

**Fake URL:** N/A

**Actual URL:** [www.verva.pl](http://www.verva.pl)

**Sender name:** [colin.peters@homecall.co.uk](mailto:colin.peters@homecall.co.uk)

**Sender IP-address:** 212.74.112.92  
(United Kingdom, Hertford, Stevenage)

**Domain information:** [verva.pl](http://verva.pl)



# Credit Union Security Warning Phish

-----Original Message-----

**From:** Chesterfield Federal Credit Union  
[mailto:notification@chesterfieldfcu.net]  
**Sent:** Monday, March 09, 2009 6:50 AM  
**To:** Removed-by-CSRM  
**Subject:** You have 1 New Security Notification!

Dear Member,

You have 1 New Security Notification!

**In order to read, please [Log-in](#) to your PCU Home Banking account and follow the steps.**

Sincerely,

Chesterfield Federal Credit Union Member Services

Copyright © 2009 Chesterfield Federal Credit Union. All Rights Reserved.



## Credit Union Security Warning Headers

Received: from covmsgces-ebh02.cov.virginia.gov ([10.192.3.45]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Mon, 9 Mar 2009 06:50:29 -0400

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh02.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Mon, 9 Mar 2009 06:50:28 -0400

X-SBRS: None

X-HAT: Group: RELAYLIST, Policy: \$RELAYED

Received: from smtp.dhcd.virginia.gov ([165.176.17.132])

by CRelayA.vita.virginia.gov with ESMTP; 09 Mar 2009 06:50:29 -0400

Received: from CMailB.vita.virginia.gov ([166.67.65.182]) by smtp.dhcd.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Mon, 9 Mar 2009 06:50:28 -0400

X-SBRS: 4.8

X-HAT: Group: None, Policy: \$ACCEPTED

X-IronPort-Anti-Spam-Result:

Ap1FAHORtEIQSo84X2dsb2JhbACBTIYeAwwBhRCFMAGGdAOBGB8lrSogSwi  
EFIhcgkMEBgiBMAaFFg

X-IronPort-AV: E=Sophos;i="4.38,328,1233550800";  
d="scan'208";a="177417093"

**Received: from outbound.icp-qv1-irony-out4.iinet.net.au  
([203.59.1.150])**



## Credit Union Security Warning Headers

**Received: from unknown (HELO chesterfieldfcu.net)  
([65.40.132.32])  
by outbound.icp-qv1-irony-out4.iinet.net.au with ESMTP;  
09 Mar 2009 19:50:22 +0900**  
From: Chesterfield Federal Credit  
Union <[notification@chesterfieldfcu.net](mailto:notification@chesterfieldfcu.net)>  
To: Removed-by-CSRM  
Subject: You have 1 New Security Notification!  
Date: 09 Mar 2009 06:50:22 -0400  
Message-ID:  
<[20090309065022.6145B422F6B0CF31@chesterfieldfcu.net](mailto:20090309065022.6145B422F6B0CF31@chesterfieldfcu.net)>  
MIME-Version: 1.0  
Content-Type: text/html;  
charset="iso-8859-1"  
Content-Transfer-Encoding: quoted-printable  
Return-Path: [notification@chesterfieldfcu.net](mailto:notification@chesterfieldfcu.net)  
X-OriginalArrivalTime: 09 Mar 2009 10:50:28.0581 (UTC)  
FILETIME=[DC2D5950:01C9A0A4]



## Credit Union Security Domain Information

**Date of receipt:** 2009-03-09

**Subject of Phishing:** You have 1 New Security Notification!

**Fake URL:** [Log-in](#)

**Actual URL:**

<http://ginalele.net/chf.useronlnet.com/asp/USERS/Common/Login/NetLogin.asp/>

**Sender name:** Chesterfield Federal Credit Union <[notification@chesterfieldfcu.net](mailto:notification@chesterfieldfcu.net)>

**Sender IP-address:** 65.40.132.32 (United States, Ohio, Jefferson)

**Domain information:** ginalele.net

Creation Date..... 2009-03-09

Registration Date.... 2009-03-09

Expiry Date..... 2010-03-09

Organisation Name.... Carlos Briseno

Organisation Address. P O Box 99800

Organisation Address. Emeryville, CA, 94662

**Domain information:** useronlnet.com

Users Incorporated

1250 Drummers Lane

Valley Forge, PA 19482-0897

US



# Survey – Gift Card Phish

**From:** Wal-Mart Stores, Inc. [mailto:online@walmart.com]  
**Sent:** Monday, March 02, 2009 1:37 PM  
**Subject:** Official Notification  
**Importance:** High

**Congratulations!**

Dear Customer,

You've been selected to take part in our quick and easy **9** questions survey  
In return we will credit **\$90.00** to your account - **Just for your time!**  
**This survey is for the customers of Credit Union and Federal Credit Union ONLY!**

This survey has been sent only to a **few** people from our random generator !  
Please spare two minutes of your time and take part in our online survey  
so we can improve our services.  
Don't miss this chance to change something.  
To access the form please click the link below :

<http://www.survey.walmart.com/customers/fcu&cu/form>

With the information collected we can decide to direct a number of changes to improve and expand our online services.

Copyright © 2009 **Wal-Mart Stores, Inc.** All Rights Reserved.

**Note:**

- \* If you received this message in your SPAM/BULK folder, that is because of the restrictions implemented by your ISP
- \* For security reasons, we will record your ip address, the date and time.
- \* Deliberate wrong inputs are criminally pursued and indicted.

Survey ID : **WAL493029884729XXC**



## Survey – Gift Card Phish Headers

Received: from covmsgces-ebh02.cov.virginia.gov ([10.192.3.45])  
by COVMSGCES-EMB05.cov.virginia.gov with Microsoft  
SMTPSVC(6.0.3790.3959);

Mon, 2 Mar 2009 14:12:05 -0500

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by  
covmsgces-ebh02.cov.virginia.gov with Microsoft  
SMTPSVC(6.0.3790.3959);

Mon, 2 Mar 2009 14:12:05 -0500

X-SBRS: 5.3

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.38,290,1233550800";  
d="scan'208,217";a="203872317"

**Received: from ihs.ktro.com (HELO mail.knight-  
trosoft.com) ([216.12.177.21])**

by CMailA.vita.virginia.gov with ESMTTP/TLS/DHE-RSA-AES256-  
SHA; 02 Mar 2009 14:12:05 -0500

Received: (qmail 20159 invoked from network); 2 Mar 2009  
12:43:31 -0600

**Received: from unknown (HELO User) (77.104.228.1)  
by 216.12.177.118 with SMTP; 2 Mar 2009 12:43:31 -0600**



# Survey – Gift Card Phish Headers

Reply-To: <[no-reply@walmart.com](mailto:no-reply@walmart.com)>  
From: "Wal-Mart Stores, Inc." <[online@walmart.com](mailto:online@walmart.com)>  
Subject: Official Notification  
Date: Mon, 2 Mar 2009 19:36:46 +0100  
MIME-Version: 1.0  
Content-Type: text/html;  
charset="Windows-1251"  
Content-Transfer-Encoding: 7bit  
X-Priority: 1  
X-MSMail-Priority: High  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE  
V6.00.2600.0000  
Bcc:  
Return-Path: [online@walmart.com](mailto:online@walmart.com)  
Message-ID: <[COVMSGCES-  
EBH02hzwV00017e1a@covmsgces-ebh02.cov.virginia.gov](mailto:COVMSGCES-EBH02hzwV00017e1a@covmsgces-ebh02.cov.virginia.gov)>  
X-OriginalArrivalTime: 02 Mar 2009 19:12:05.0576 (UTC)



## Survey – Gift Card Domain Information

**Date of receipt:** 2009-03-02

**Subject of Phishing:** Official Notification

**Fake URL:**

<http://www.survey.walmart.com/customers/fcu&cu/form>

**Actual URL:**

<http://58.181.36.135/walmart/online.survey/index.html>

**Sender name:** "Wal-Mart Stores, Inc." [online@walmart.com](mailto:online@walmart.com)

**Sender IP-address:** 77.104.228.1 (Czech Republic, Chrudim, Wifi network)

**Sender IP-address:** 58.181.36.135 (Korea, Republic of, Seoul) NexG



# Credit Union Survey Phish

**From:** Northern Star Credit Union [mailto:nstarcu@survey.org]  
**Sent:** Thursday, February 26, 2009 6:12 AM  
**To:** Removed-by-CSR  
**Subject:** You have been selected!

Dear Member,

Due to the rumors of financial crisis, Northern Star Credit Union has decided to make a Member Satisfaction Survey. The information collected will be used to improve and expand our services. For the completion of this survey, we will credit your account with \$100.00.

To take part, please [click here](#)

Note - The information we gather from this survey will not be handed down to any third party.

© 2009 Northern Star Credit Union. All rights reserved.



# Credit Union Survey Phish Headers

Received: from covmsgces-ebh02.cov.virginia.gov ([10.192.3.45]) by COVMSGCES-EMB03.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Thu, 26 Feb 2009 06:12:39 -0500

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh02.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Thu, 26 Feb 2009 06:12:39 -0500

X-SBRS: 2.9

X-HAT: Group: None, Policy: \$ACCEPTED

X-IronPort-Anti-Spam-Filtered: true

X-IronPort-Anti-Spam-Result:

Apo4AAwIpknaIMrngWdsb2JhbACCQTEBhQqFQIYRA4EqAQEWIqdWiIEfOBII  
hyyIWIJVBaiBMAaERg

X-IronPort-AV: E=Sophos;i="4.38,270,1233550800";  
d="scan'208";a="202828629"

**Received: from mail.myvu.com ([74.8.196.60])**

by CMailA.vita.virginia.gov with ESMTP; 26 Feb 2009 06:12:39 -0500

**Received: from survey.org ([65.40.132.32]) by mail.myvu.com with Microsoft SMTPSVC(6.0.3790.3959);**



# Credit Union Survey Phish Headers

Thu, 26 Feb 2009 06:10:03 -0500

From: Northern Star Credit Union<nstarcu@survey.org>

To: Removed-by-CSR

Subject: You have been selected!

Date: 26 Feb 2009 06:12:25 -0500

Message-ID:

<20090226061225.68CC8D485E6A43A3@survey.org>

MIME-Version: 1.0

Content-Type: text/html;

charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

Return-Path: nstarcu@survey.org

X-OriginalArrivalTime: 26 Feb 2009 11:10:03.0700 (UTC)

FILETIME=[C60F0740:01C99802]



# Credit Union Survey Domain Information

**Date of receipt:** 2009-02-26

**Subject of Phishing:** You have been selected!

**Fake URL:** <http://hungis.net/www.nstarcu.org/MemberServices/>

**Actual URL:** N/A

**Sender name:** Northern Star Credit Union [mailto:nstarcu@survey.org]

**Sender IP-address:** 74.8.196.60 (US, Rhode Island, Johnston)  
65.40.132.32 (US, Ohio, Bellville)

**Domain information:** HUNGIS.NET

Domain Name..... hungis.net  
Creation Date..... 2009-02-26  
Registration Date.... 2009-02-26  
Expiry Date..... 2010-02-26  
Organisation Name.... Carlos Briseno  
Organisation Address. P O Box 99800  
Organisation Address.  
Organisation Address. EmeryVille  
Organisation Address. 94662  
Organisation Address. CA  
Organisation Address. US



# On-line Banking Phish

**From:** Bank of America [mailto:bankofamerica@securespot.net]  
**Sent:** Wednesday, May 13, 2009 11:52 AM  
**To:** Removed-by-CSR  
**Subject:** IMPORTANT - Customer Service Message

Dear Bank of America customer,

We recently have determined that different computers have logged into your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us.

If this is not completed by May 18, 2009, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:  
<https://sitekey.bankofamerica.com/sas/signon.do/Login/>

Thank you for your patience in this matter,  
Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered. © 2009 Bank of America Corporation. All rights reserved .



# On-line Banking Phish Headers

Received: from covmsgces-ebh01.cov.virginia.gov ([10.192.3.25]) by COVMSGCES-EMB05.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Wed, 13 May 2009 11:52:25 -0400

Received: from CMailA.vita.virginia.gov ([10.193.13.181]) by covmsgces-ebh01.cov.virginia.gov with Microsoft SMTPSVC(6.0.3790.3959);

Wed, 13 May 2009 11:52:25 -0400

X-SBRS: 5.3

X-HAT: Group: WHITELIST, Policy: \$TRUSTED

X-IronPort-AV: E=Sophos;i="4.41,188,1241409600";  
d="scan'208,217";a="220981851"

Received: from relay0.lixxus.net (HELO s1.l1.lixxus.net) ([82.112.104.162])

by CMailA.vita.virginia.gov with ESMTP; 13 May 2009 11:52:24 -0400

**Received: from rjmittens.co.uk (host-83-231-129-4.xdsl.lixxus.net [83.231.129.4])**

by s1.l1.lixxus.net (8.12.11/8.12.11) with ESMTP id n4DFqHc8029073 for <[division2@vdfp.virginia.gov](mailto:division2@vdfp.virginia.gov)>; Wed, 13 May 2009 16:52:18 +0100 (BST)

**Received: from securespot.net ([216.31.181.25]) by rjmittens.co.uk with Microsoft**



# On-line Banking Phish Headers

SMTPSVC(6.0.3790.3959);

Wed, 13 May 2009 16:52:12 +0100

From: Bank of America <[bankofamerica@securspot.net](mailto:bankofamerica@securspot.net)>

To: Removed-by-CSR

Subject: IMPORTANT - Customer Service Message

Date: 13 May 2009 08:52:10 -0700

Message-ID:

<[20090513085210.9C27CBAE34D83EB2@securspot.net](mailto:20090513085210.9C27CBAE34D83EB2@securspot.net)>

MIME-Version: 1.0

Content-Type: text/html;

charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

X-OriginalArrivalTime: 13 May 2009 15:52:12.0719 (UTC)

FILETIME=[C7EF53F0:01C9D3E2]

Return-Path: [bankofamerica@securspot.net](mailto:bankofamerica@securspot.net)



## On-Line Banking Phish Domain Information

**Date of receipt:** 2009-05-13

**Subject of Phishing:** IMPORTANT - Customer Service Message

**Fake URL:** <https://sitekey.bankofamerica.com/sas/signon.do/Login/>

**Actual URL:** <http://www.h43.pl/webapps/>

**Sender name:** Login Webmail [mailto:jkeller@brocku.ca]

**Sender IP-address:** 216.35.181.25 (USA Walnut CA.)

**Domain information:** h43.pl

registrant's handle: nta200372 (CORPORATE)

created: 2008.02.03 14:54:25

last modified: 2009.03.21 23:08:22

REGISTRANT:

company: GF Marek Mucha

street: Wita Stwosza 16

city: 33-100 Tranów

location: pl

phone: +48.508388966



## The Bait

- Both SPAM and Phishing can be used to gather additional emails (Bait).
  - Responding to a SPAM or Phishing email, even to asked to be removed from the sender's list, only validates the responder's email address.
  - Address Harvesting can occur through compromised Social Network sites, Websites that sell registration information without permission (although some websites have fine print of agreements allowing this action), and websites that publish a directory or contact information for individual users.
  - Some Phishing emails include URLs that link to malicious software that can harvest the recipient's electronic address book.
  - The Recipient's email address can now be used as the source address for the next round of malicious emails, thereby adding legitimacy to the email.



## Waledac Spam terms and objectives

- Joe Job = A spam attack using spoofed sender data that is intended to tarnishing the reputation of the spoofed sender and/or induce the recipients of the spoofed email to take action against the spoofed sender. The spam attack will simply advertise the victim's product, business or website or it may also claim that the spoofed sender is selling illegal or offensive items such as illegal drugs, automatic weapons or child pornography to increase the likelihood that the recipient will take action against the victim. The spam attack can also lead to a temporary Denial-of-Service condition for the spoofed sender's website.
- Joe Jobs are acts of revenge and are one of the few spam-related activities that do not have an economic goal.



# Security Measures

- Delete the SPAM or Phishing email. Do not read or reply to the message
- To protect the Operating System:
  - Enable the “Automatic Software Update” feature.
  - Remove software that is no longer needed.
  - Remove trial software once the trial has ended.
  - Do not install unsolicited software from any source.
- Employ the Least Privilege concept
  - Create a separate account for system administration on the computer system.
  - Do not use the name Admin, Superuser, Root, or any other term that would suggest that the account is the Administrator account. The “Administrative” account should only be used to install software and make system modifications.
- Create separate accounts for each user on the computer system. The user accounts should be used for the day to day activities. Limiting access to the system privileges associated with the Administrator account will prevent some of the malicious content spreading across the Internet from getting installed on the computer system.



# Additional Security Measures

- Every computer system on the network needs an up-to-date version of anti-virus, anti-spyware, anti-spam, and anti-phishing software.
- Configure the Anti-X software to check for product updates on a daily basis.
- Configure the Anti-X software to scan the entire contents of the hard drive at least once a week.
- Configure the Anti-X software to scan ALL removable media each time the removable media is attached to the computer system.
- Monitor the computer system:
  - Monitor hard disk space to determine if the available space decreases for an unknown reason – This may indicate a backdoor has been installed on the computer system and the system is storing information for a malicious individual.
  - Monitor the log files and Event Viewer logs for unexpected error messages
- Renew the software update license each year or purchase a new copy of the software at the end of each year. Do not let the Anti-X software expire.



# Security Research URLs

- American Registry of Internet Numbers
  - Provides ownership information of IP-addresses
  - [www.arin.net](http://www.arin.net)
- Whois / Network Solutions
  - Provides information on domain name ownership
  - [www.networksolutions.com/whois](http://www.networksolutions.com/whois)
- Websense Security
  - Provide hundreds of organizations around the world with the latest security warnings on malicious Internet events and compromised Web sites.
  - <http://securitylabs.websense.com/content/alerts.aspx>
- Anti-Phishing Working Group
  - The Anti-Phishing Working Group (APWG) is the global association focused on eliminating the fraud and identity theft from email spoofing of all types.
  - [http://www.antiphishing.org/phishing\\_archive.html](http://www.antiphishing.org/phishing_archive.html)
- PhishTank
  - PhishTank is a collaborative clearing house for data and information about phishing on the Internet.
  - <http://www.phishtank.com/>



# Additional Security Research URLs

- Shadow Server
  - <http://www.shadowserver.org/wiki/>
- Internet Storm Center
  - <http://isc.sans.org/>
- SANS Reading Room
  - [https://www.sans.org/reading\\_room/](https://www.sans.org/reading_room/)
- US-CERT
  - <http://www.us-cert.gov>
  - [http://www.us-cert.gov/reading\\_room/emailscams\\_0905.pdf](http://www.us-cert.gov/reading_room/emailscams_0905.pdf)
  - <http://www.us-cert.gov/cas/tips/ST04-014.html>
- Security Focus
  - <http://www.securityfocus.com/>
- Commonwealth of Virginia Security Information Resource Center
  - <http://www.csirc.vita.virginia.gov>



## Final Thoughts

- 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.
- 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!



# Upcoming Events





## UPCOMING EVENTS! Future 2009 ISOAG's

**All currently from 1:00 – 4:00 pm at CESC  
though working with the Science Museum (thanks!)  
(please let us know if you want to host in the Richmond area!)**

**Tuesday, July 14**

**Wednesday, August 12**

**Wednesday, September 9**



# Upcoming Events – ISOAG July 14

## Draft Agenda

E-Discovery

Julie Whitlock, Office of the  
Attorney General

Electronic Records

Siri Berdahl, Library of Va.

Information Security Awareness ToolKit

Nakita Albritton, VITA



# Information Security System Association

ISSA meets on the second Wednesday of every month

- **DATE:** Wednesday July 15<sup>th</sup>
- **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.
- **Shirley Teague, Supervisory Special Agent, FBI will provide an overview on "FBI-sponsored Regional Computer Forensics Laboratory (RCFL) program."**
- **COST:** ISSA members: \$10 & Non-Members: \$20
- **RSVP:** With Corey Perkins at: [cperkins@issa-centralva.org](mailto:cperkins@issa-centralva.org)



## FACTA Red Flag Requirements \*NEW DATE

Implementation Date: **August 1<sup>st</sup>, 2009**

Are you aware of the red flag requirements in the Fair and Accurate Credit Transactions Act (FACTA) of 2003?

Please read carefully as it is not only banks and financial institutions!

<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>



# UPCOMING EVENTS: MS-ISAC Webcast

## National Webcast!

**Wednesday, August 19, 2009, 2:00 to 3:00 p.m.**

**Topic: Security of Social Networking Sites/Web 2.0**

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/>



Any Other Business ???????





**ADJOURN**

**THANK YOU FOR ATTENDING!!**

