

# Security and The Independent Bank

**Ways to reduce your exposure and  
liability**

Presented by: Jim Stickley



# Topic of discussion

- Random concerns from Phishing solutions to bad physical security

# Phishing

- What not to do
- Does multifactor work?

## Phishing; what not to do

- Numerous financial institutions were compromised with a type phishing attack due to a third party vendor flaw
  - One financial institution decided the best course of action was to send an email to notify customers

## Bad choices with phishing response

- Letter number 1
  - The first one included a link that pointed its customers to a remedy Web page that wasn't within the financial institutions domain. (*i.e. a link that is not part of the bank's environment*).
  - Due to the confusion this letter caused, a second more detailed email was sent out.

## Bad choices with Phishing response

- Second follow up email
  - “On Thursday, May 25, 2006, XXXXXX Bank became aware of an apparent attempt by an unauthorized party to gain access to our third-party website host and thus to our Online Banking site.....Although there is no current evidence that customers information has been accessed, this incident may have increased the probability of your information being used for fraudulent purposes.....Your Online Banking password has been defaulted back to your original password; when you established your Online Banking service....you may not have access to your original login information, XXXXXX Bank has established a help center that you may contact at 1-800-527-6335 or by email at info@xxxxxxx.net.....A temporary Online Banking login website has been established at “XXXXXXXXXX”. This temporary site is safe.....”

# Phishing; what not to do

- Bad press
  - Ultimately the press picked up on it
  - Not the best public relations

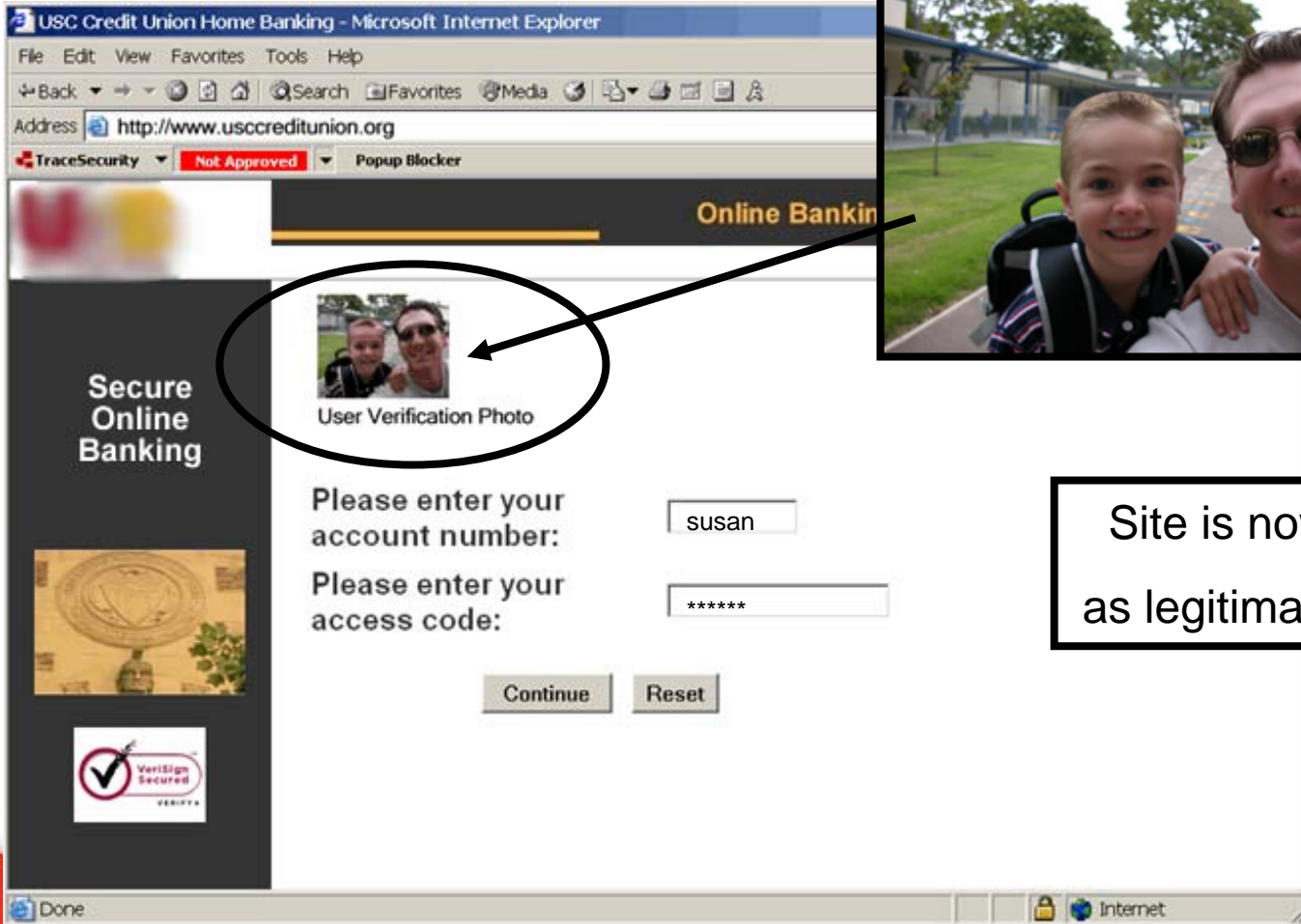
# What about Anti-Phishing?

- Many organizations are offering solutions to phishing schemes.
  - Site recognition
  - Personal questions
  - Two factor authentication
  - Third party products

# Site Recognition

- The user chooses a picture, most often from a limited list on the web site that they want to see when they connect to the site.
- The idea is that a malicious site wont know what image to display and therefore the user will know they are at a malicious site.
- For this to work, a cookie is placed on the users computer.

# Site Recognition



USC Credit Union Home Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail

Address <http://www.usccreditunion.org>

TraceSecurity Not Approved Popup Blocker

Online Banking

Secure Online Banking

User Verification Photo

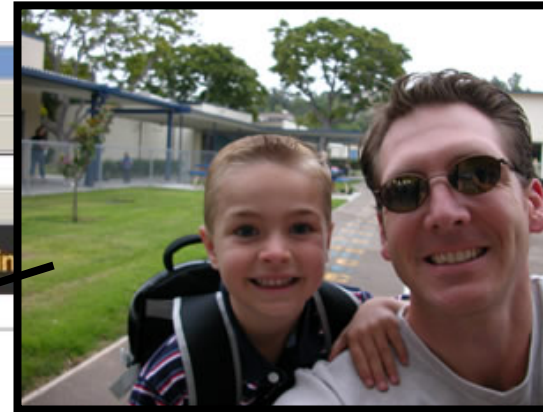
Please enter your account number:

Please enter your access code:

Continue Reset

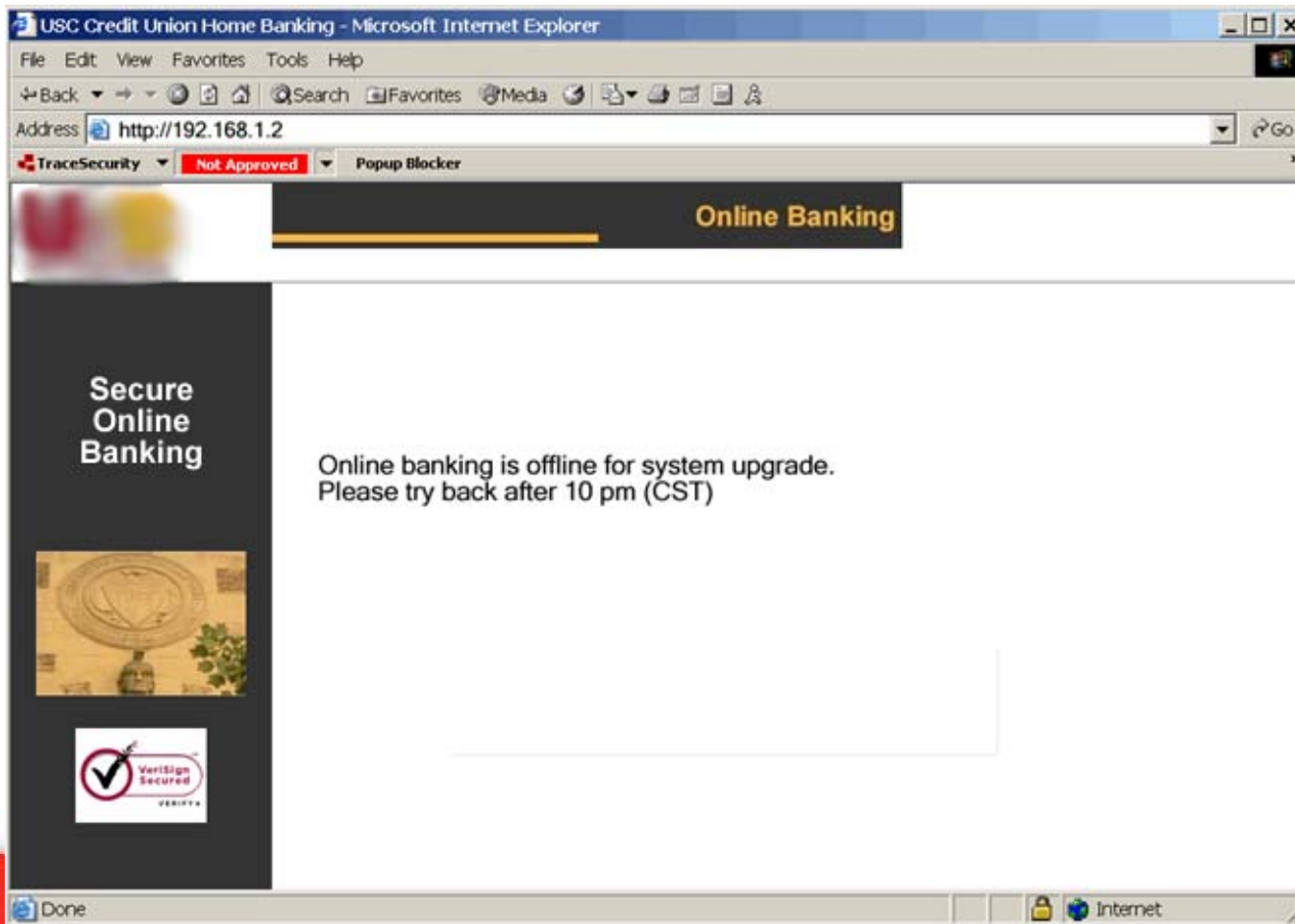
VeriSign Secured

Done Internet

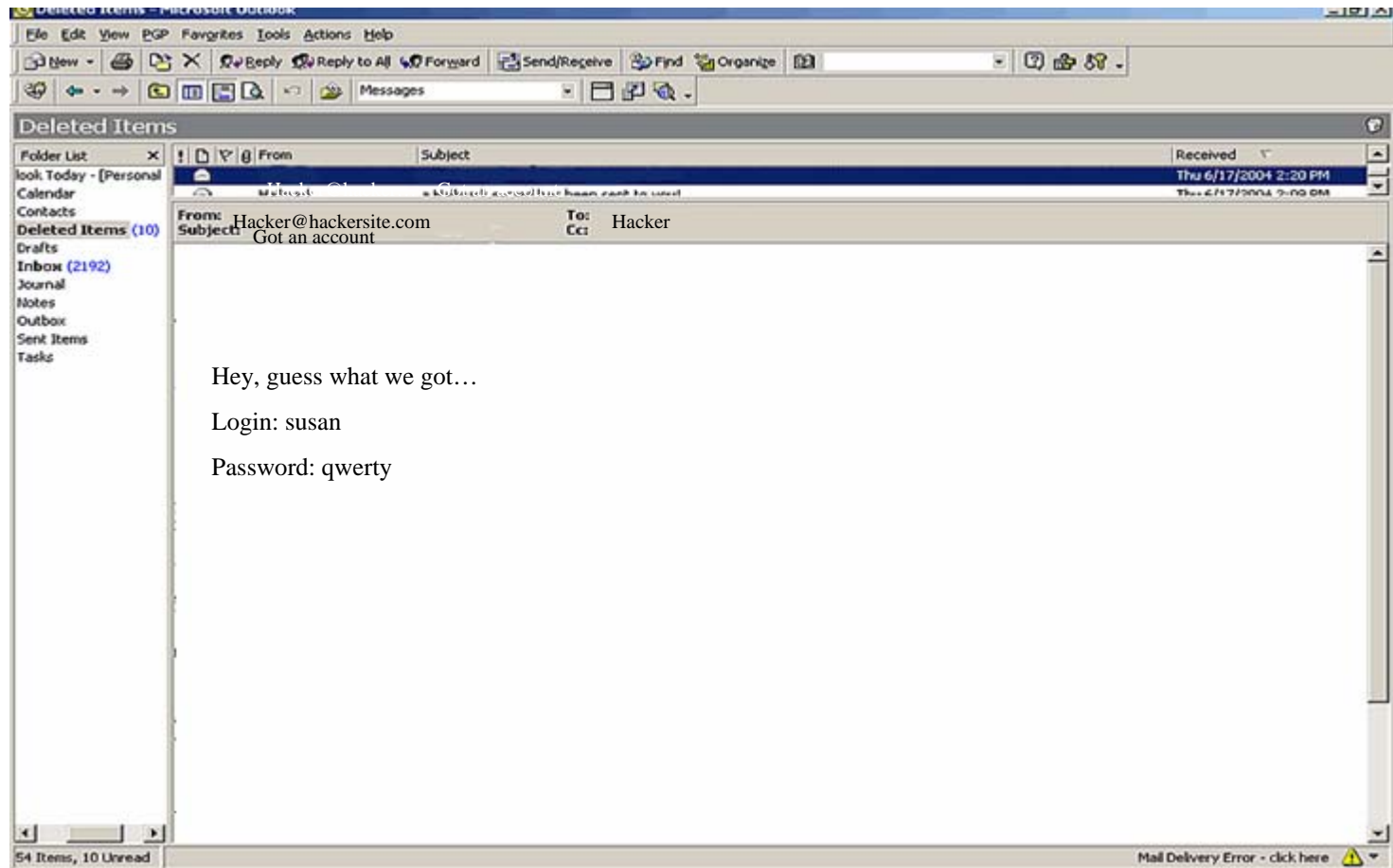


Site is now verified  
as legitimate by user

# Site Recognition



# Site Recognition



# Site Recognition

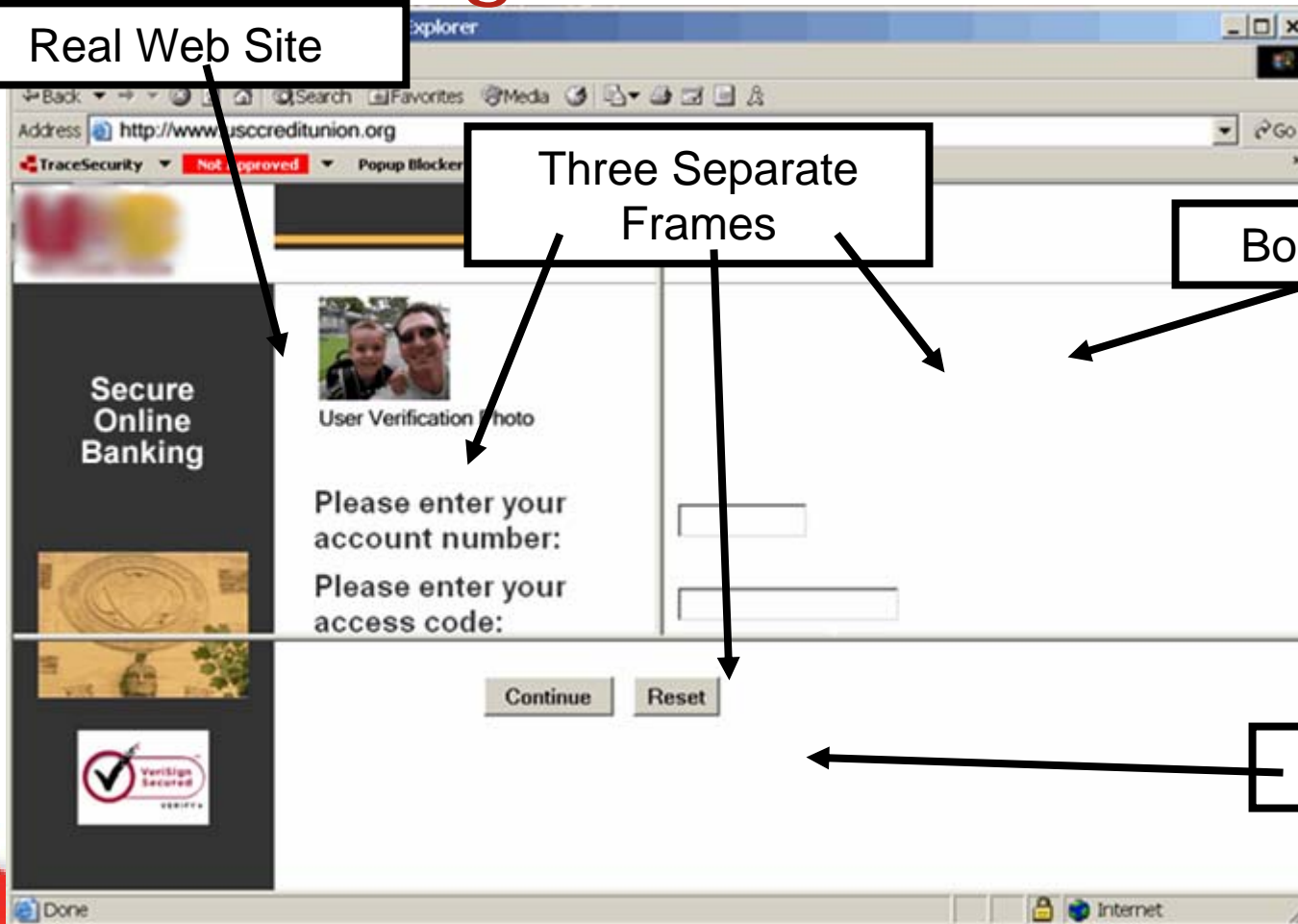
- How can that be?
  - The site had the proper URL.
  - The site showed the image that we expected.
  - The cookie on our computer was definitely used.
  - The site shown did not have any pop-ups.
- Obviously this must be the correct site..?

# Site Recognition Flaws

Real Web Site

Three Separate  
Frames

Bogus Web Site



Bogus Web Site

# What happened?

- Frames loaded the real web site
  - Tricked site into showing image via cookie
- Malicious web site used for input of data
- All pages go through SSL pages, less suspicious

## How do you catch it?

- Never allow your web page to be loaded in a frame.

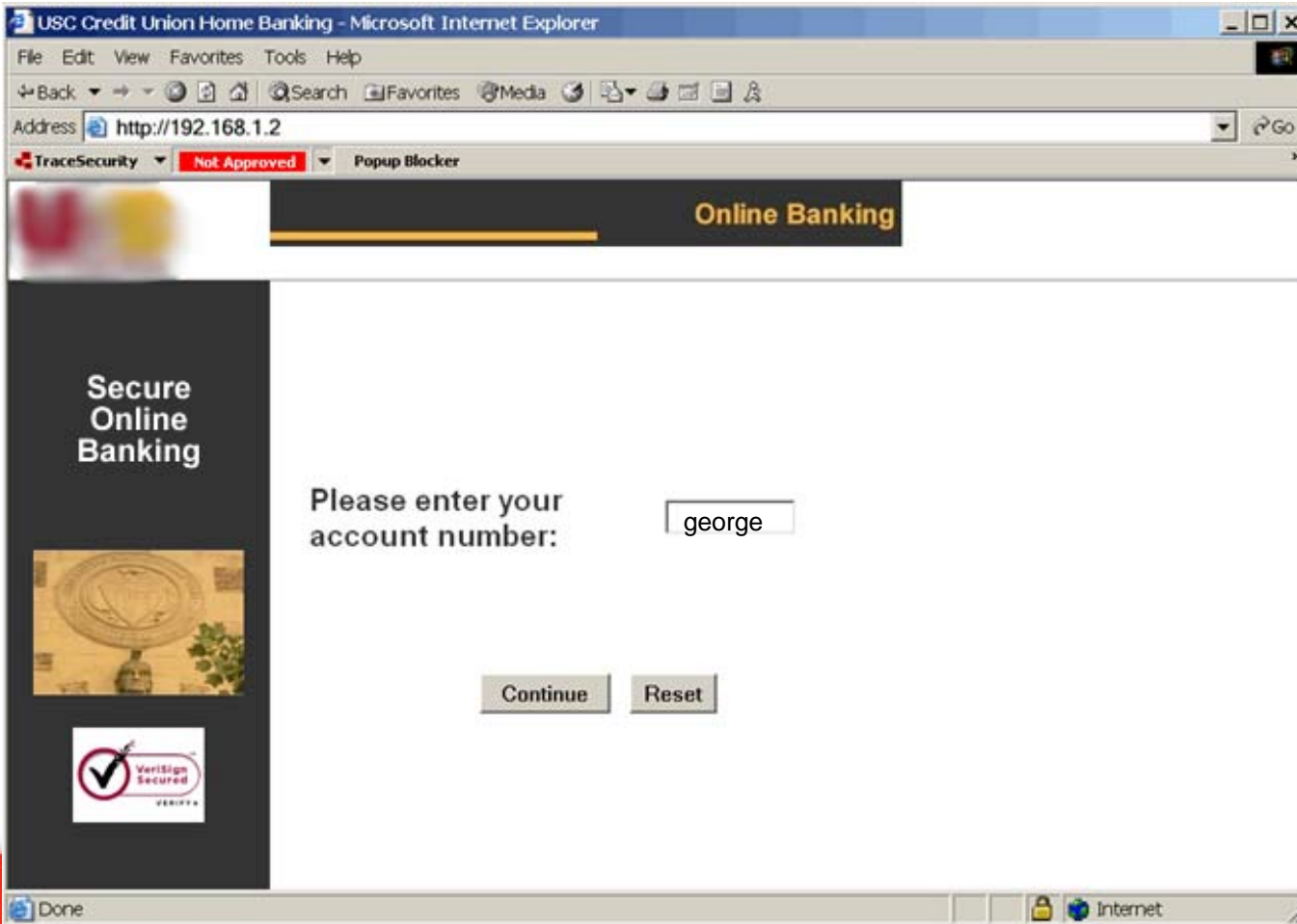
```
<script language=javascript type="text/javascript"> <!--  
  if (parent.frames.length) top.location.href=  
  document.location; // --> </script>
```

- Place image to right of input boxes.
  - More difficult to pull site into specific location

# Personal Question

- A user submits their user name.
- Instead of posting a password, the user is then prompted with a question they wrote themselves.
- After the user answers the question properly, the user is then prompted with a password.
- The idea is that only the legitimate web site would know the question and proper answer, all others would be malicious and user would stay away.

# Personal Question



USC Credit Union Home Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS

Address <http://192.168.1.2> Go

TraceSecurity Not Approved Popup Blocker

Online Banking

Secure Online Banking

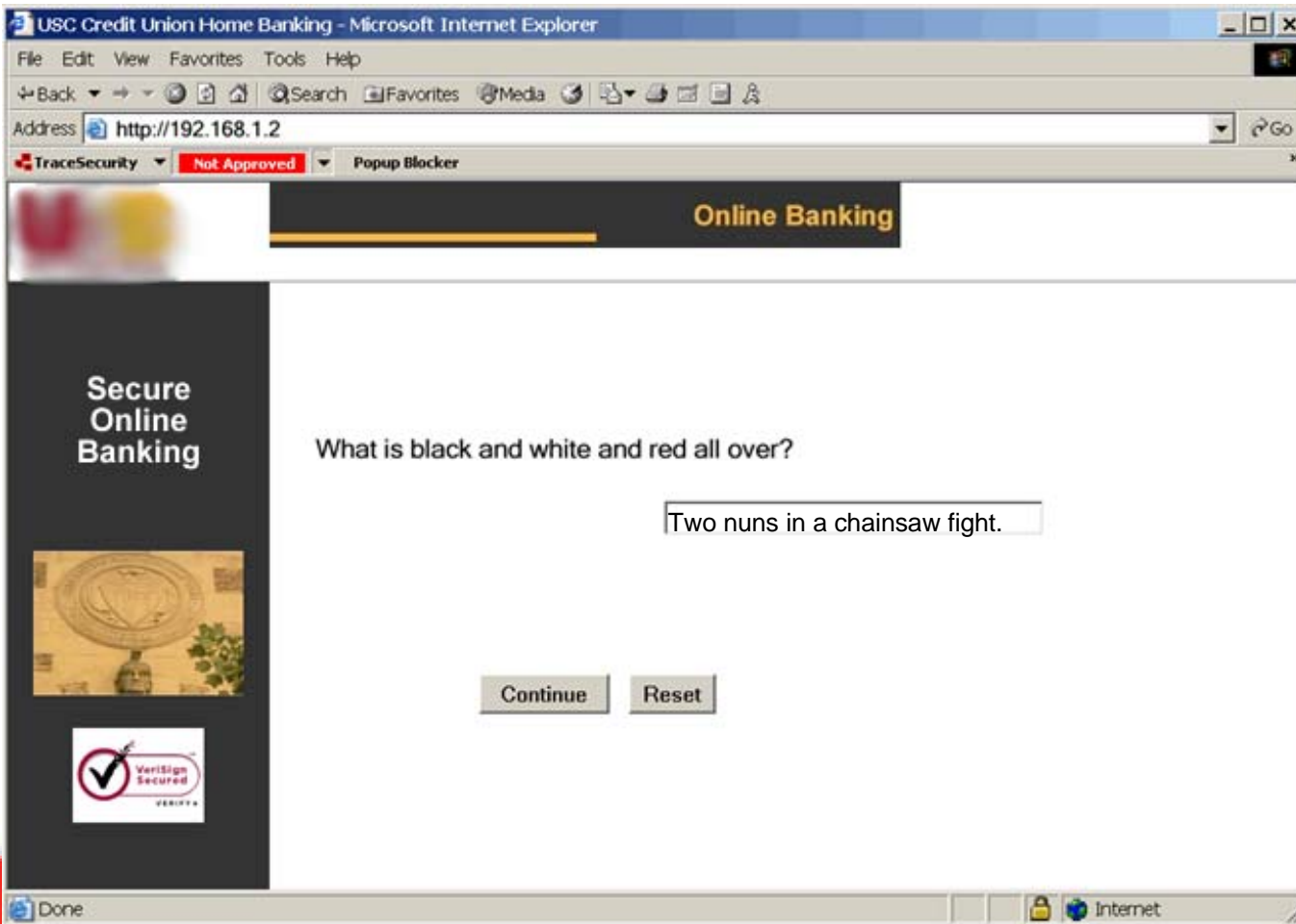
Please enter your account number:

Continue Reset

VeriSign Secured

Done Internet

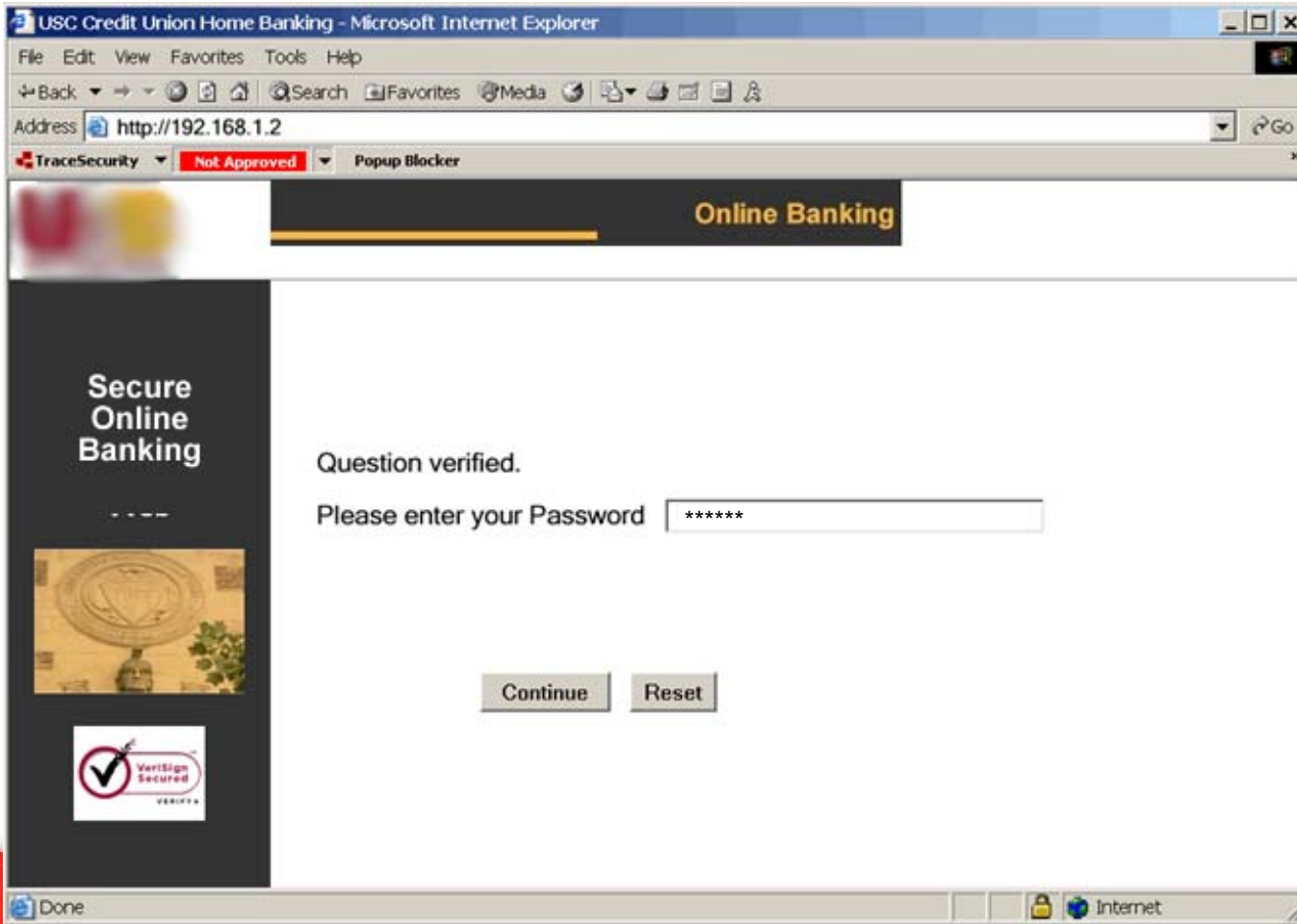
# Personal Question



The screenshot shows a Microsoft Internet Explorer browser window titled "USC Credit Union Home Banking - Microsoft Internet Explorer". The address bar displays "http://192.168.1.2". The browser's status bar at the bottom shows "Done" and "Internet".

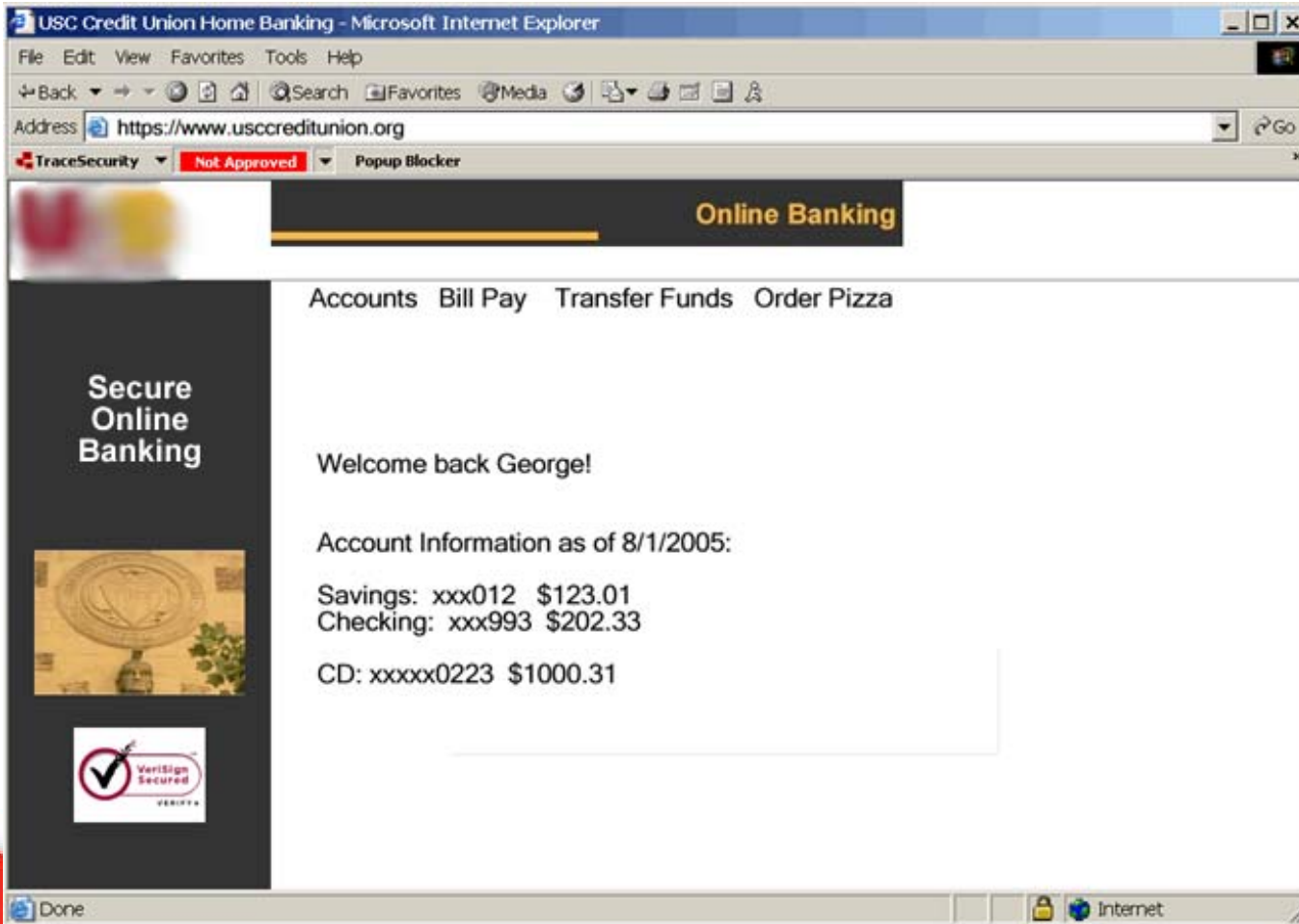
The webpage content includes a navigation bar with "Online Banking" and a sidebar with "Secure Online Banking" and a VeriSign Secured logo. The main content area features a security question: "What is black and white and red all over?". Below the question is a text input field containing the answer "Two nuns in a chainsaw fight.". At the bottom of the question area are "Continue" and "Reset" buttons.

# Personal Question



The screenshot shows a Microsoft Internet Explorer browser window titled "USC Credit Union Home Banking - Microsoft Internet Explorer". The address bar displays "http://192.168.1.2". The browser's status bar shows "TraceSecurity" with a "Not Approved" warning and a "Popup Blocker" icon. The webpage content includes a header with the "Online Banking" logo. A dark sidebar on the left contains the text "Secure Online Banking" and a VeriSign Secured logo. The main content area displays the message "Question verified." followed by a prompt "Please enter your Password" and a text input field containing six asterisks. Below the input field are "Continue" and "Reset" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

# Personal Question



USC Credit Union Home Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS

Address <https://www.usccreditunion.org> Go

TraceSecurity Not Approved Popup Blocker

**Online Banking**

Accounts Bill Pay Transfer Funds Order Pizza

**Secure Online Banking**

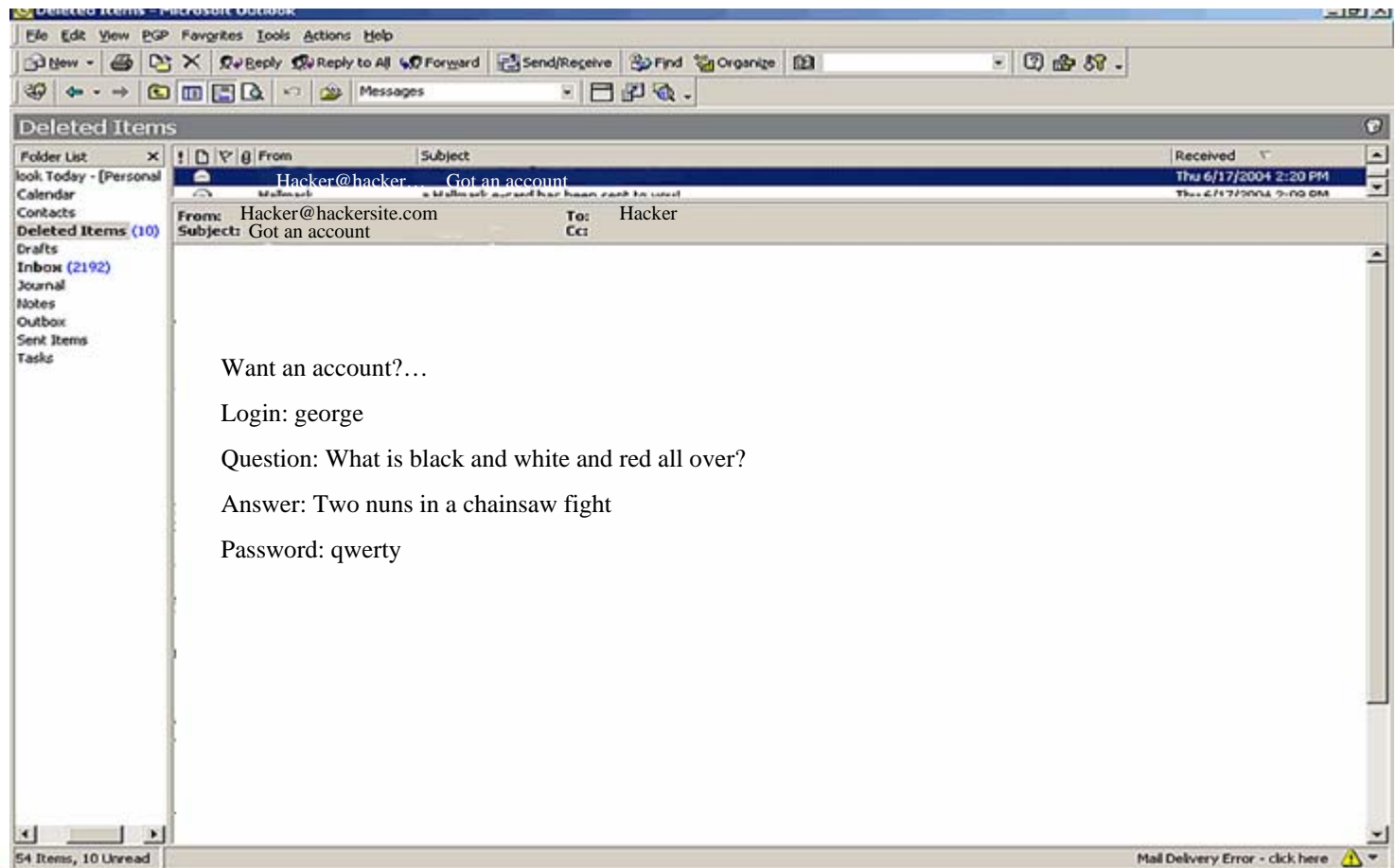
Welcome back George!

Account Information as of 8/1/2005:

Savings: xxx012 \$123.01  
Checking: xxx993 \$202.33  
CD: xxxxx0223 \$1000.31

Done Internet

# Personal Question



# Personal Question

- How can that be?
  - The site had the proper URL.
  - The site showed the question we expected.
  - The site knew we answered question correct.
  - The site showed did not have any pop-ups.
  - We were logged in!
- Obviously this must be the correct site..?

# How was it done?



User clicks link to connect  
to Banking web site



# How was it done?



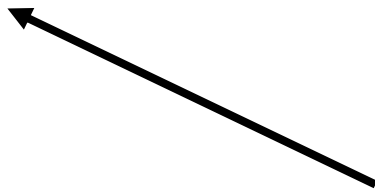
Click Link to connect to  
Banking web site



Malicious web site (Man in the  
middle) receives connection



# How was it done?



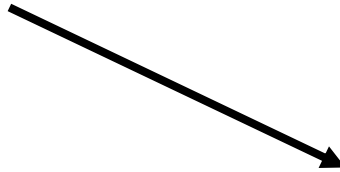
Malicious web site displays page as though it is Banking and prompts user to enter in user name.



# How was it done?



Enters in User Name



# How was it done?



Enters in User Name



Malicious Web site stores name and then passes User Name to Banking web site



# How was it done?



Enters in User Name



Banking web site verifies  
User Name and responds  
to malicious site with  
question



# How was it done?



Malicious Site Stores  
question and then posts it  
to the user

# How was it done?



User now answers  
question that he  
recognized as his own



# How was it done?



User now answers  
question that he  
recognized as his own



Malicious site stores the  
response and then passes the  
info to the Banking site



# How was it done?



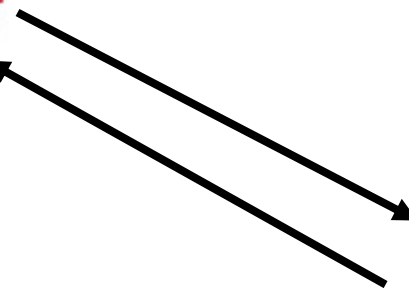
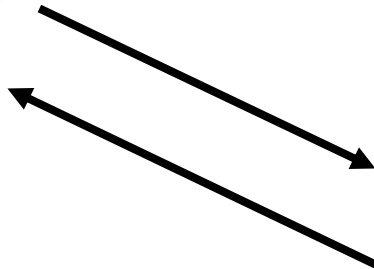
User now answers  
question that he  
recognized as his own



Banking site receives the  
response, verifies it is correct  
and then passes back a  
password request



# How was it done?

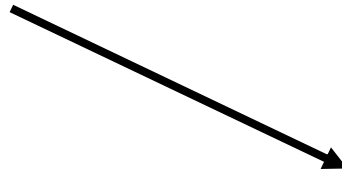


Malicious site logs that response was accepted and posts password request to user

# How was it done?



User responds to  
password request



# How was it done?



User responds to  
password request



Malicious site records  
submitted password and  
then passes it to Banking  
Site



# How was it done?



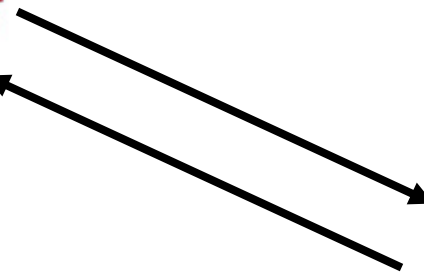
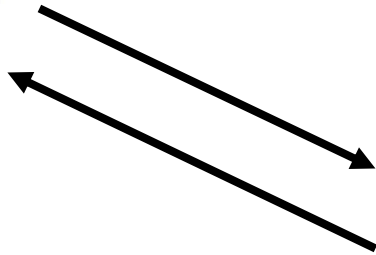
User responds to  
password request



Banking site verifies  
password and then logs  
user in by posting  
welcome page.

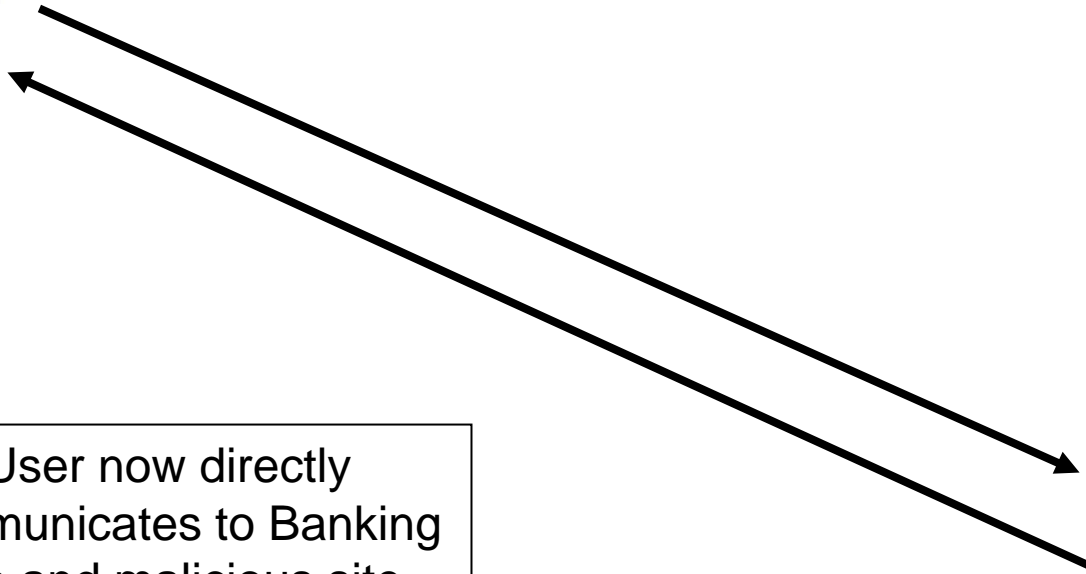


# How was it done?



Malicious site logs that password was accepted and then passes correct URL back to user

# How was it done?



User now directly  
communicates to Banking  
site and malicious site  
drops out of the loop



# How was it done?



Malicious site now has complete account information needed to login, bypassing anti-phishing technology

## How do you catch it?

- Must verify proper URL connection.
  - Domain name must match legit IP Address.
- Watch for other tricks learned earlier in this presentation.
- Don't assume because question is posted, site is real.

# Two Factor Authentication

- Instead of entering a password, the user is either prompted with a “challenge code” or is expected to enter in a time based password.
- Often times an additional password will also be required.
- The idea is that if entered into bogus site, real account will still be safe since password is valid one time only.

# Two Factor Authentication

USC Credit Union Home Banking - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Back Forward Stop Search Favorites Media Print Mail News RSS

Address <http://www.usccreditunion.org> Go

TraceSecurity Not Approved Popup Blocker


**Online Banking**

**Secure Online Banking**

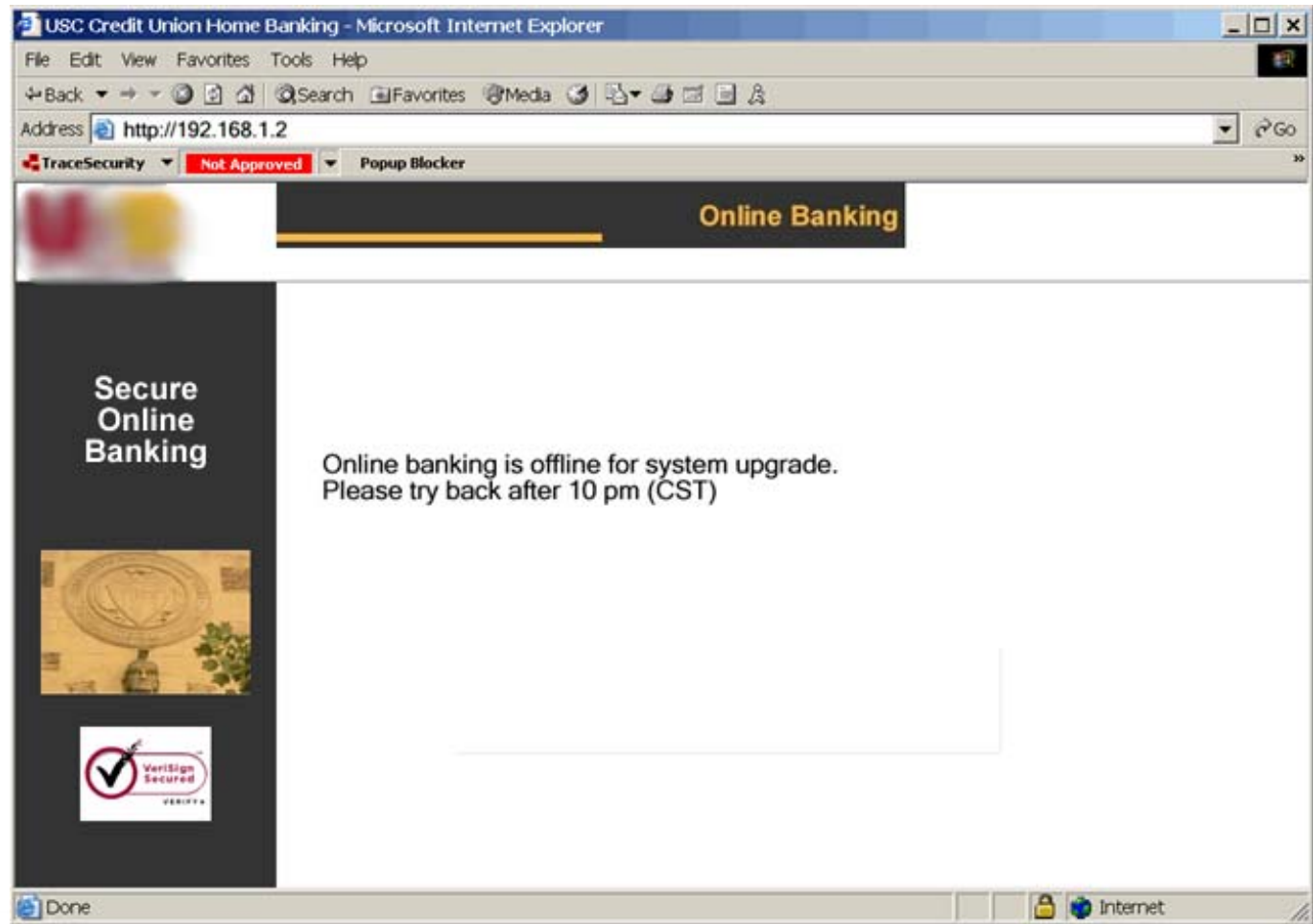
  
User Verification Photo

Please enter your account number:

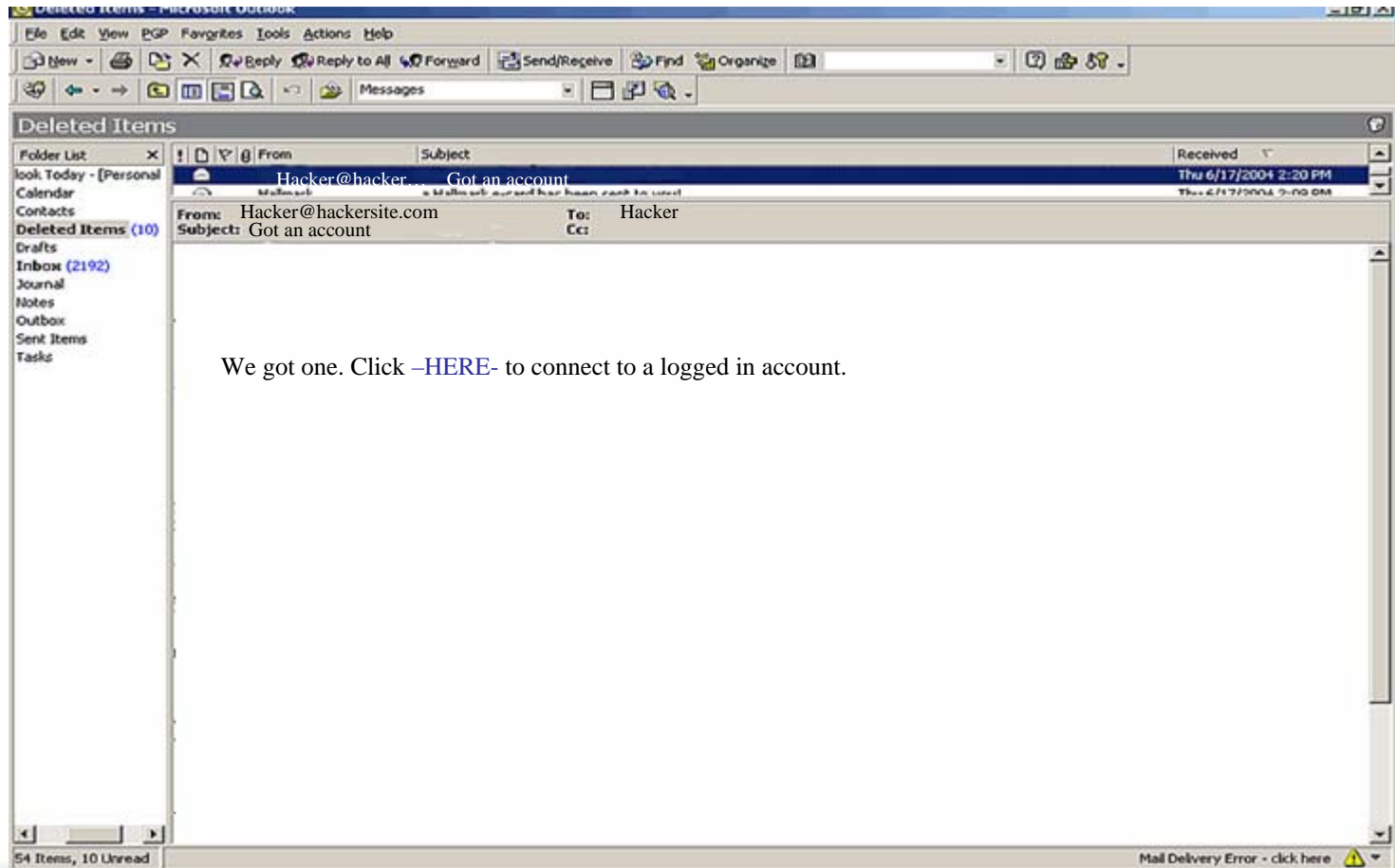
Authorization Challenge: 113776

Done  Internet

# Two Factor Authentication



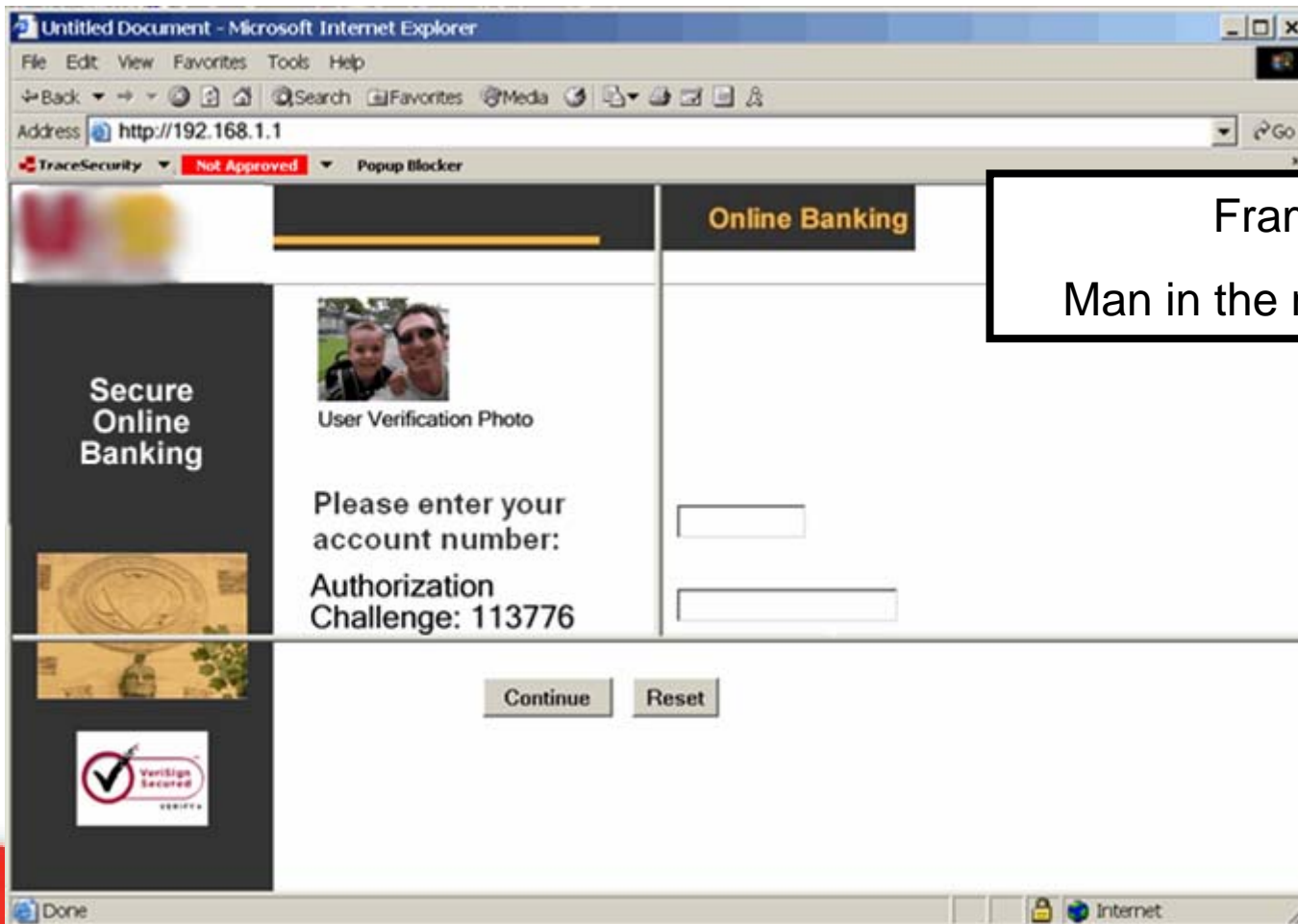
# Two Factor Authentication



# Two Factor Authentication

- How can that be?
  - The site had the proper URL.
  - The site showed the image that we expected.
  - The cookie on our computer was definitely used.
  - The site showed did not have any pop-ups.
  - Even if a user stored the data, the couldn't use it.
- Obviously this must be the correct site..?

# What happened?



Frames &  
Man in the middle attack

## What happened?

- Frames allows the image to properly respond.
- A man in the middle attack allows the malicious site to hijack a two factor authenticated session.
- User would assume all was ok and try back later.

## How do you catch it?

- Stop web page from showing up in frames.
- Must verify proper URL connection.
- Make sure users continue to be suspicious.
  - A major setback to stronger security is less paranoia.

# Other issues related to user verification

- Domains, Identifiers, and more...

## Similar domains a major risk

- Do you know who is close to your domain?
  - Example: First Community Bank of San Diego
  - Domain: [www.firstcommunitybanksd.com](http://www.firstcommunitybanksd.com)
  - Malicious: [www.firstcommunitybankofsd.com](http://www.firstcommunitybankofsd.com)

## User validation

- Mothers maiden name not that strong
  - Easy to get the mothers maiden name of just about anyone
  - Use more then one form of verification
    - Last 4 of social and their phone number
    - Phone number is often better then address since often address and social are stored together in database

# Phone number verification flawed

- Auto validate via phone system
  - When call center answers, user is verified automatically based on the phone number pulled over the line
  - Easy to spoof phone numbers using IP phones
  - Need to require additional information

# Physical security concerns

- Backup tapes
- camera systems
- Floor plans

# Backup tapes not properly secured

- Internal
  - Often tapes are left on open racks
  - Tapes are left on counters
  - Numerous versions of backup tapes
    - Easy to lose and not notice

# Backup tapes not properly secured

- External
  - Tapes are taken home for redundancy
    - Left in cars, brief cases, purses, etc.
    - Not secured at home
  - Shipped via commercial airlines
  - Information is transferred to remote location via FTP

## Video surveillance issues

- Many banks have gone to digital surveillance
  - Primary servers are improperly patched
  - Most are found to be left logged in as administrator
    - Easy to take offline
    - Easy to take over

# Physical security concerns

- Server Room Security Issues
  - Server room not locked
    - Keyboard loggers take less than 15 seconds
  - No secured rack for core servers
  - Poor / sloppy cabling
  - Remember that physical access to a server often means administrative access

# Physical security concerns

- Walk through your facility
  - Where are the printers?
  - Where is the restrooms?
  - Is there unobstructed access to employee desks?
  - Can you watch what is being typed on monitors?
  - How often is the file room door propped open?

# Physical security concerns

- Define the areas
  - Lobby: Public access
    - Printers should not sit in public access areas
  - Collections: Semi public access
  - HR: Employees only
  - Server Room: Limited employee access

# Physical security concerns

- Best practice
  - Awareness training at least once a month
  - Do not allow to take backup tapes home
  - If Confidential data must be transported it needs to be encrypted
  - Shred
  - Backup tapes must be secured even during shipping

# Network security concerns

- Wireless
- Patches
- Logs

## Wireless access in facilities

- Just because it's not on your internal network, doesn't mean it's not putting you at risk
  - Launch point for Internet attacks
  - Easy to monitor user traffic
  - Employees often bypass site security

# Watching your network

- Switches and hubs

- **Hubs**

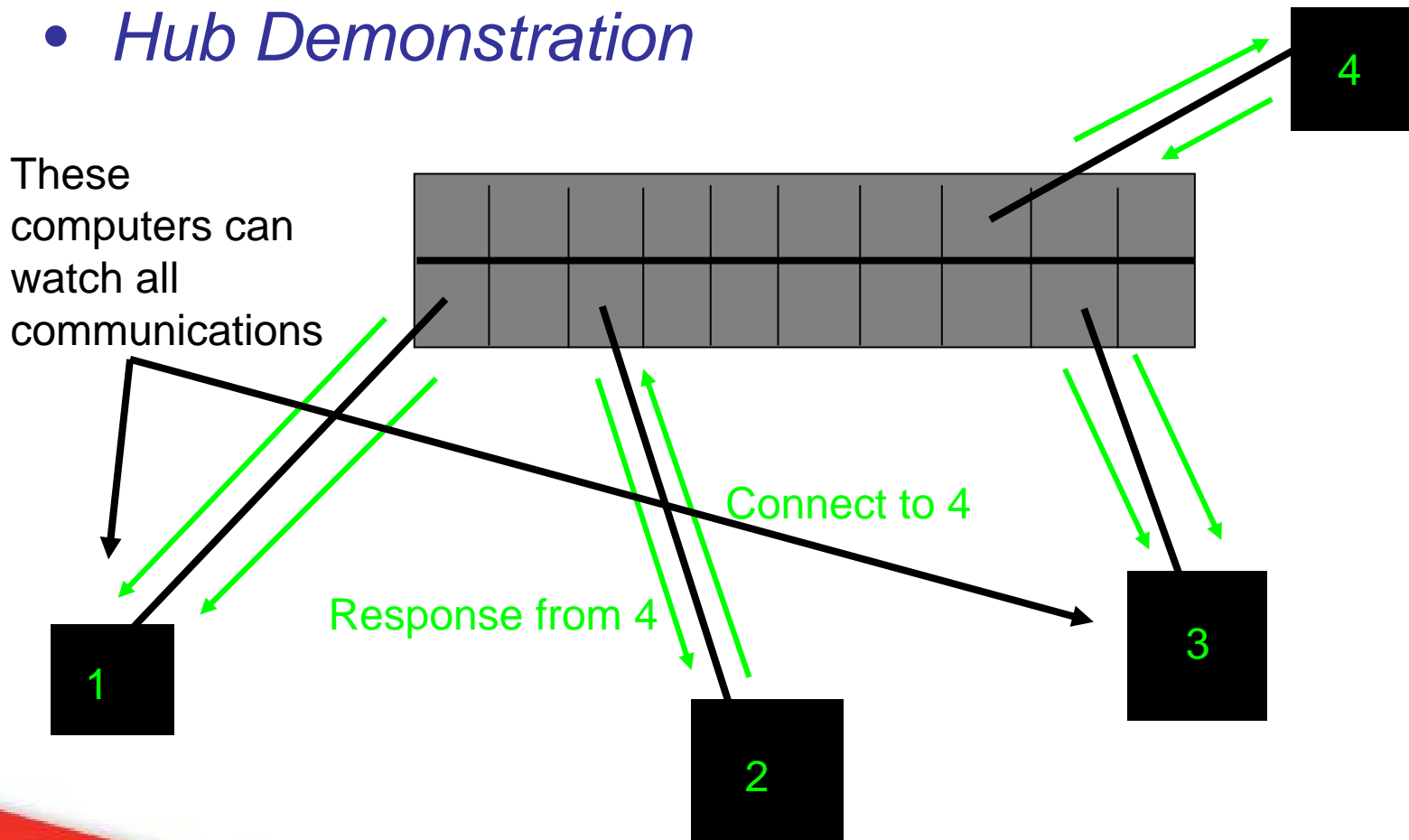
- Hubs are wide open to all traffic.
    - Packet collisions are common which reduces speed and efficiency.
    - Considered security risk to a network because of the easy of network sniffing.

- **Switch**

- Each connection assigned to a port.
    - Collisions are reduced since the switch knows where to pass data.
    - A port will only see traffic destined for that specific device.
    - Considered far more secure than a hub.

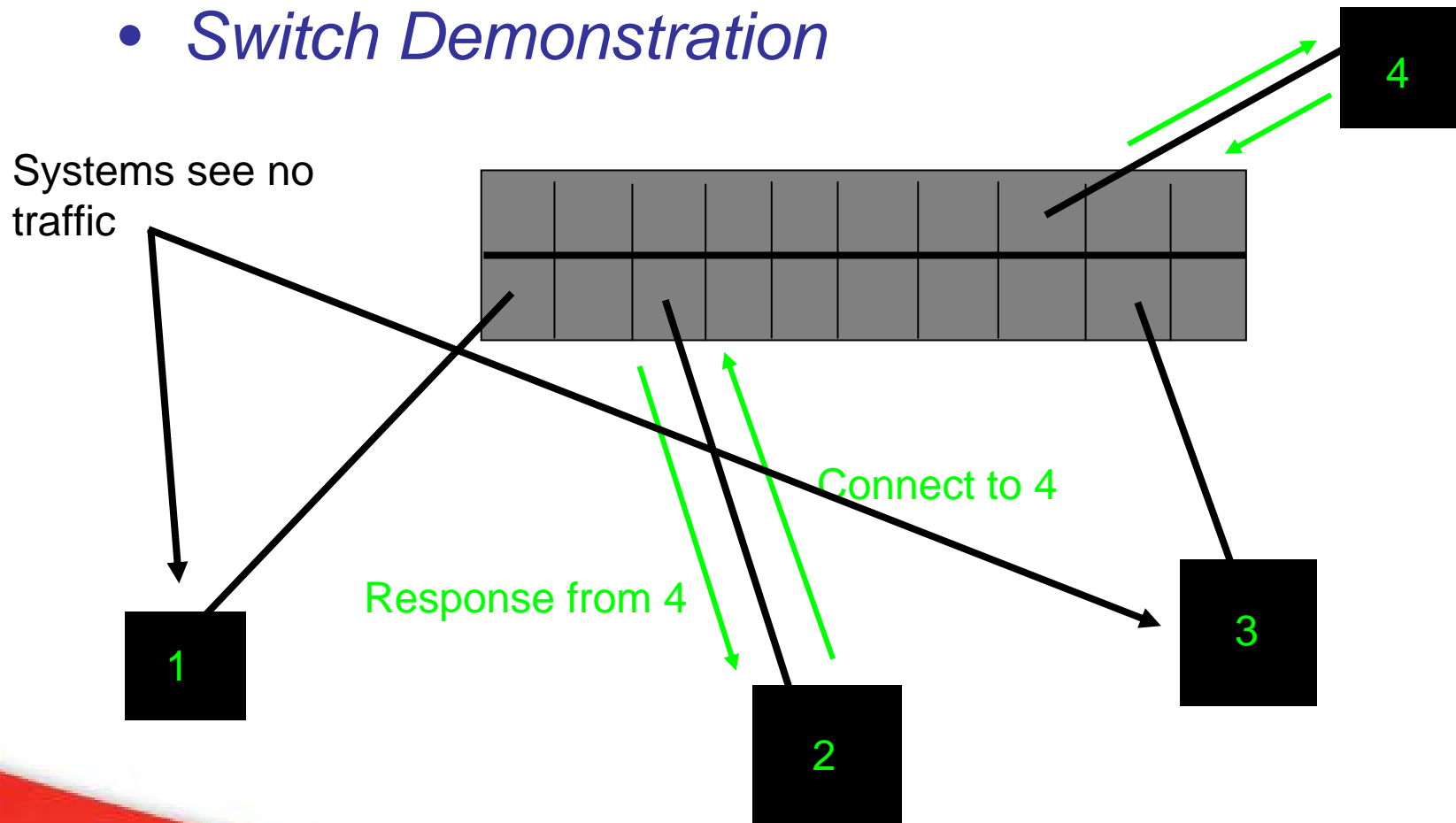
# Watching your network

- *Hub Demonstration*



# Watching your network

- *Switch Demonstration*

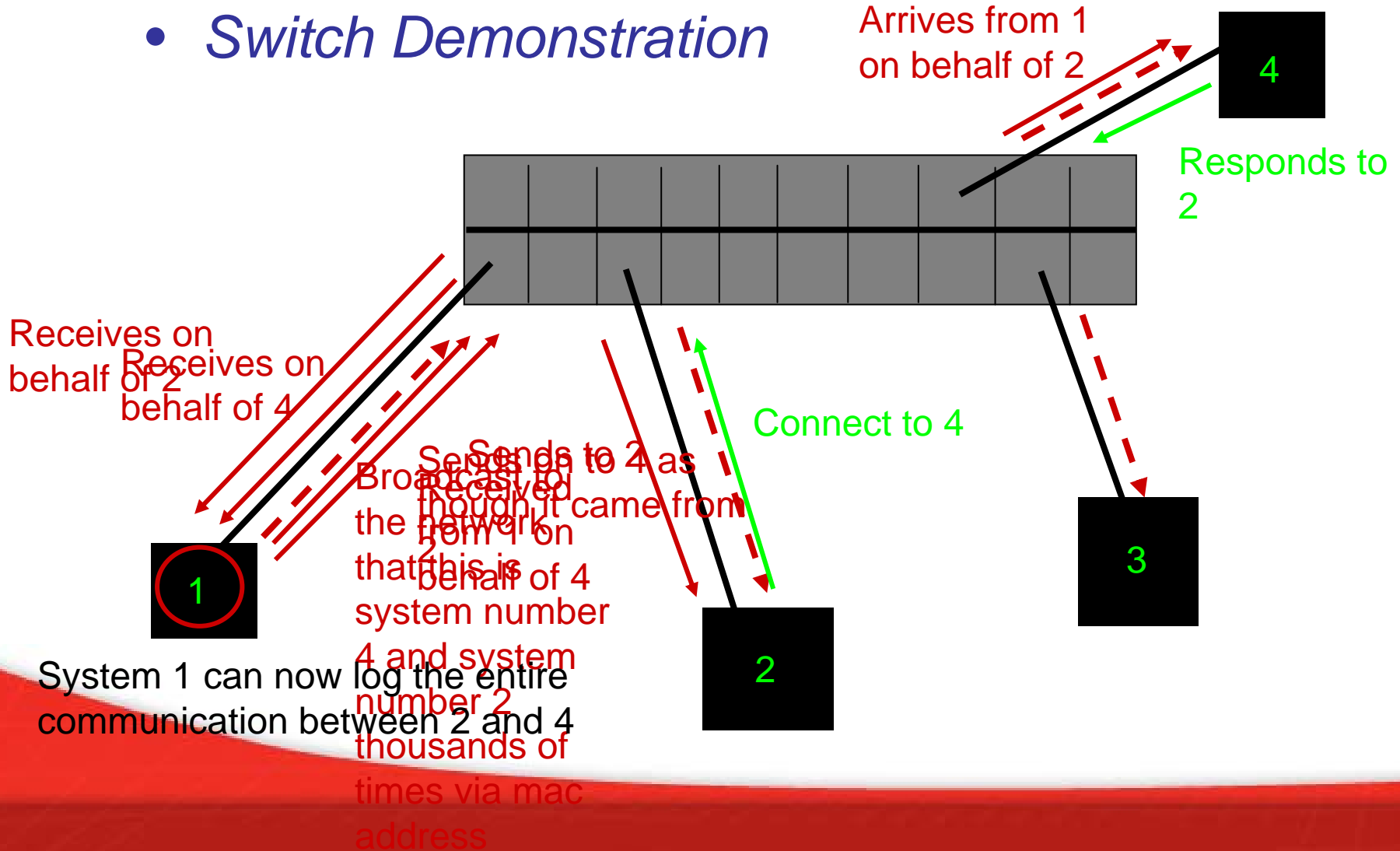


# Watching your network

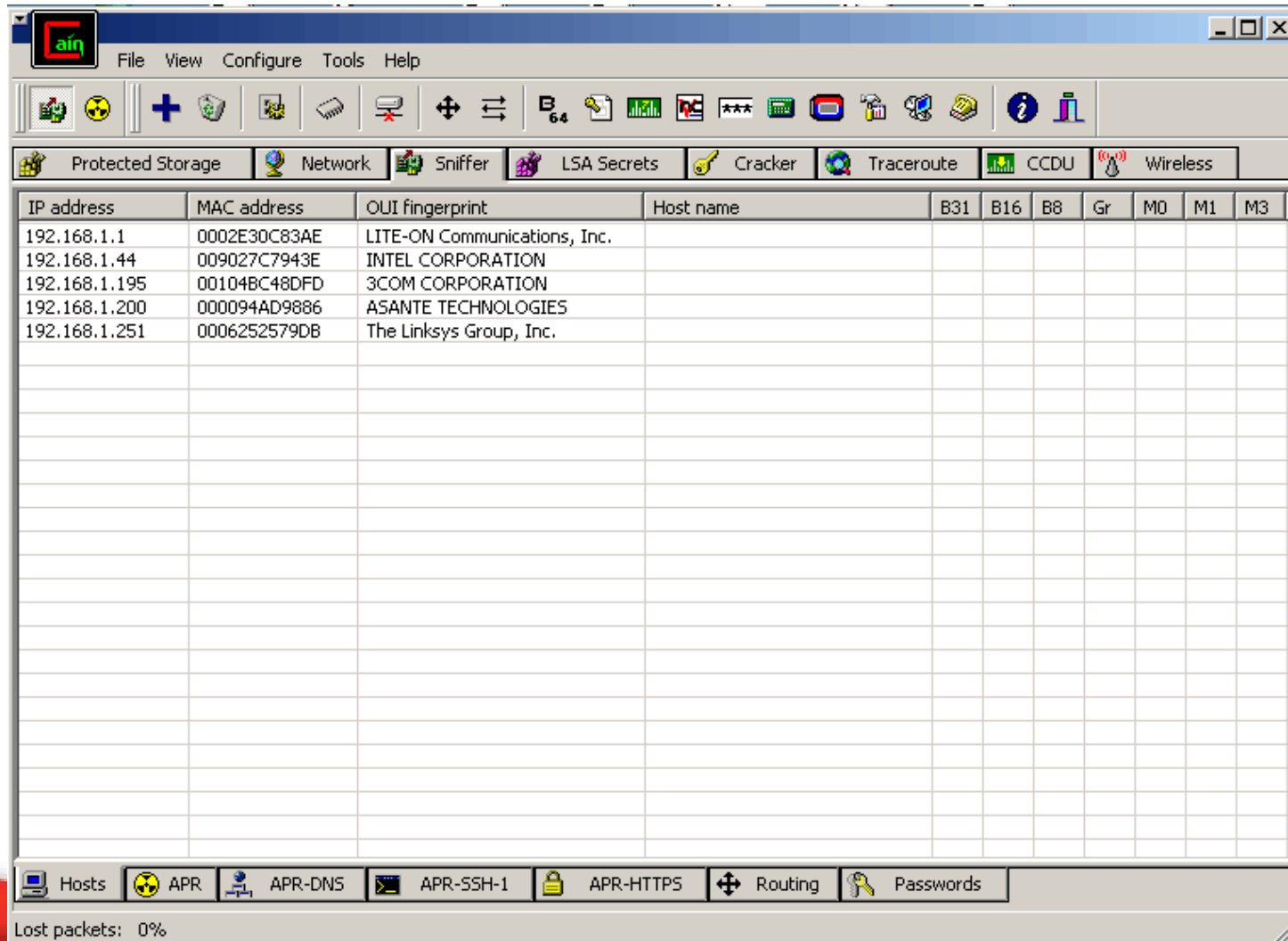
- *What if you could trick the switch*
  - **What if you told the switch that you were system 4 instead of the real system 4?**

# Watching your network

- Switch Demonstration



# Watching your network



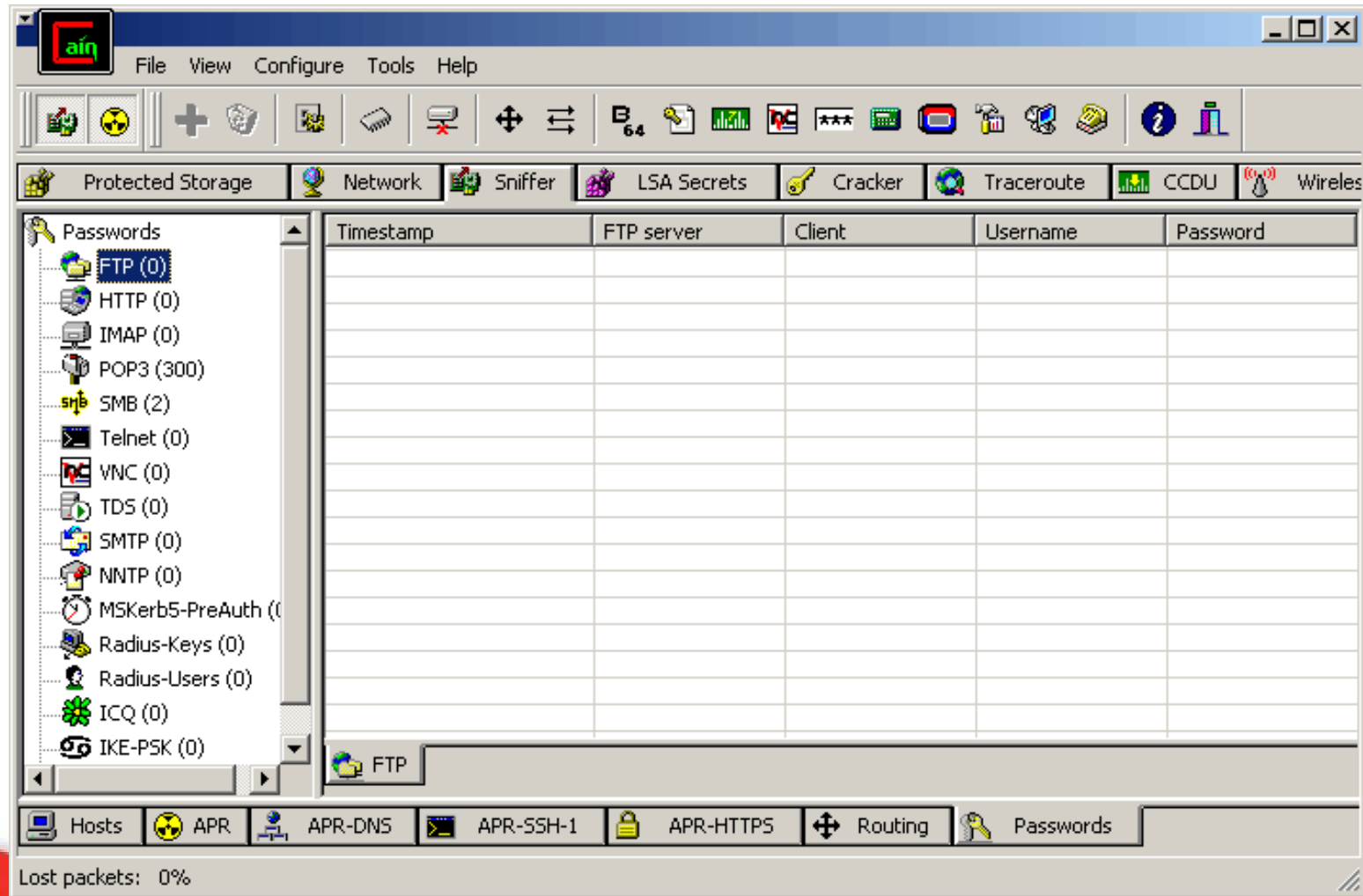
IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.1.1	0002E30C83AE	LITE-ON Communications, Inc.								
192.168.1.44	009027C7943E	INTEL CORPORATION								
192.168.1.195	00104BC48DFD	3COM CORPORATION								
192.168.1.200	000094AD9886	ASANTE TECHNOLOGIES								
192.168.1.251	0006252579DB	The Linksys Group, Inc.								

Hosts APR APR-DNS APR-SSH-1 APR-HTTPS Routing Passwords

Lost packets: 0%



# Watching your network



Protected Storage | Network | Sniffer | LSA Secrets | Cracker | Traceroute | CCDU | Wireless

File View Configure Tools Help

Timestamp FTP server Client Username Password

FTP (0)  
HTTP (0)  
IMAP (0)  
POP3 (300)  
SMB (2)  
Telnet (0)  
VNC (0)  
TDS (0)  
SMTP (0)  
NNTP (0)  
MSKerb5-PreAuth (0)  
Radius-Keys (0)  
Radius-Users (0)  
ICQ (0)  
IKE-PSK (0)

Hosts | APR | APR-DNS | APR-SSH-1 | APR-HTTPS | Routing | Passwords

Lost packets: 0%

# Watching your network

- Whats at risk?
  - Capture the password of all connections to the following services and more
    - FTP
    - Mail (Pop & SMTP)
    - Rlogin
    - Telnet

# Watching your network

- Whats at risk?
  - Read all mail sent inbound and outbound
  - Capture all transactions that take place over telnet
  - Access to all files transferred through FTP
  - Unlimited possibilities

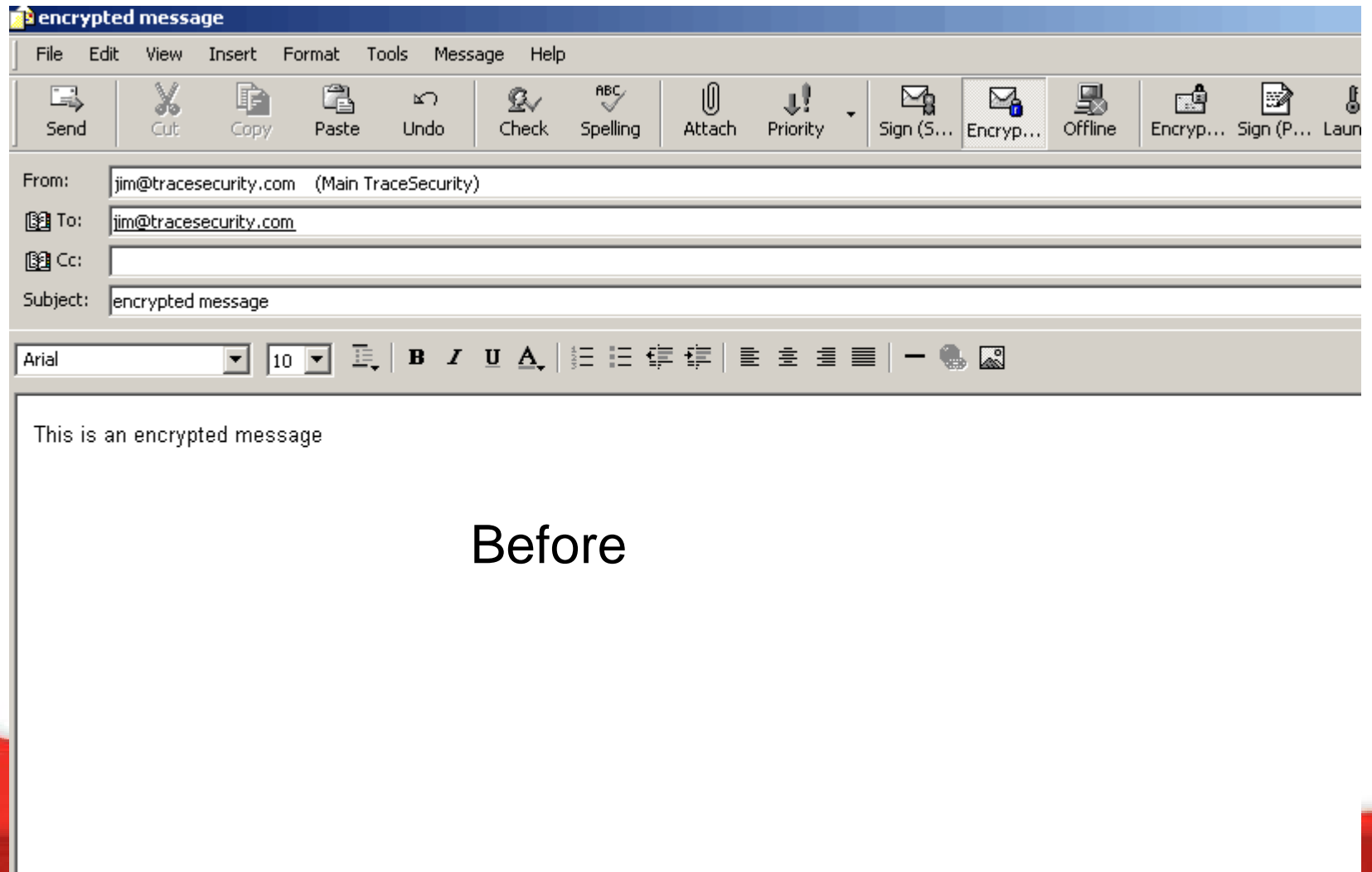
# Watching your network

- What can be done?

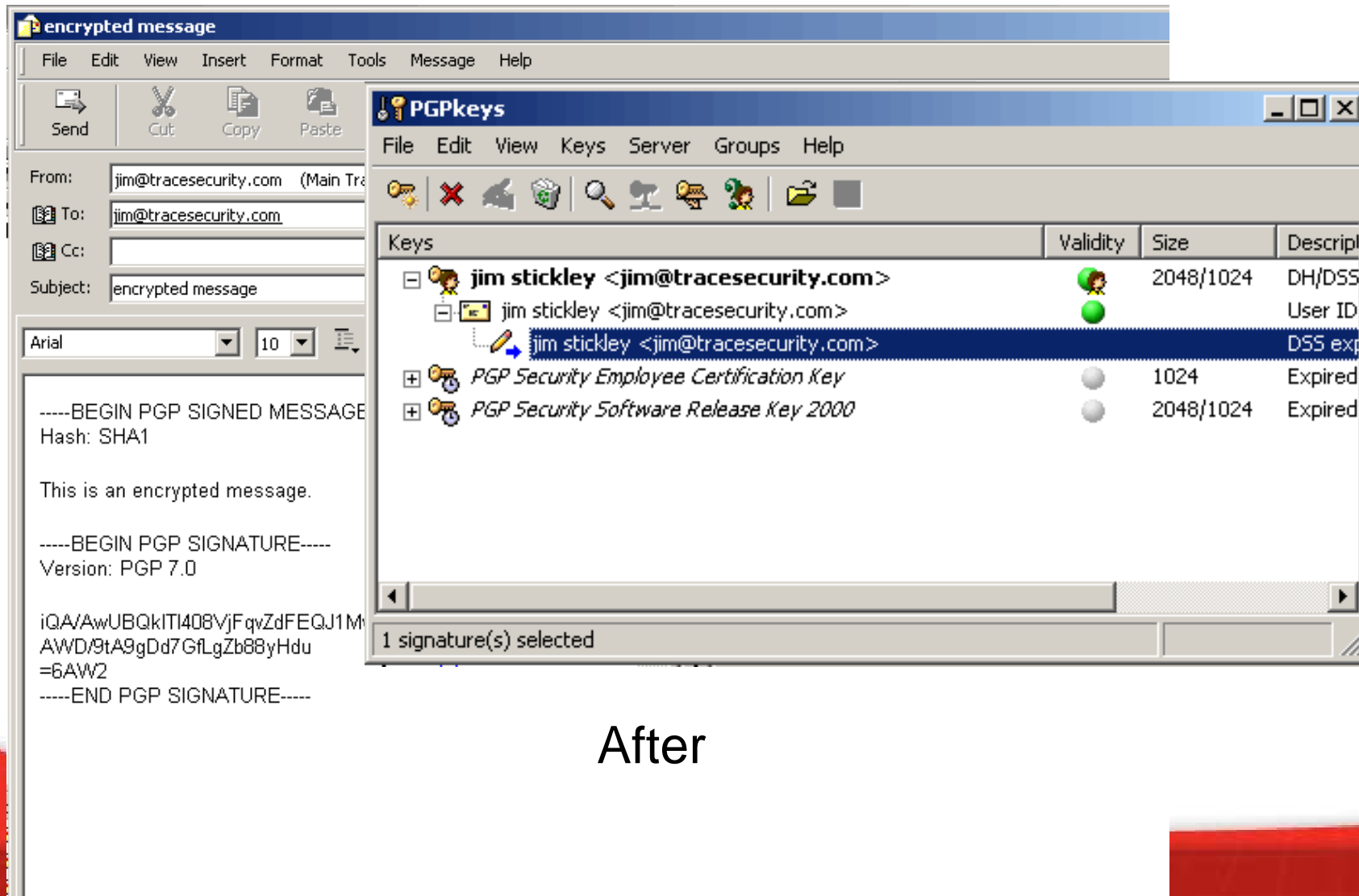
## – Outbound Email (SMTP)

- **Start with encryption on any confidential email**

# PGP



# PGP



The screenshot shows an email client window titled "encrypted message" and a "PGPkeys" window. The email content includes a PGP signature and a PGP message. The PGPkeys window displays a list of keys with columns for Validity, Size, and Description.

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1

This is an encrypted message.

-----BEGIN PGP SIGNATURE-----  
Version: PGP 7.0

iQA/AwUBQkITI408VjFqvZdFEQJ1M  
AWD/9tA9gDd7GfLgZb88yHdu  
=6AW2  
-----END PGP SIGNATURE-----

Keys	Validity	Size	Descript
<ul style="list-style-type: none"> <li>[-] jim stickley &lt;jim@tracesecurity.com&gt;</li> <li>[-] jim stickley &lt;jim@tracesecurity.com&gt;</li> <li>[-] jim stickley &lt;jim@tracesecurity.com&gt;</li> </ul>	<ul style="list-style-type: none"> <li>●</li> <li>●</li> <li>●</li> </ul>	<ul style="list-style-type: none"> <li>2048/1024</li> <li>2048/1024</li> <li>2048/1024</li> </ul>	<ul style="list-style-type: none"> <li>DH/DSS</li> <li>User ID</li> <li>DSS exp</li> </ul>
[+] PGP Security Employee Certification Key	●	1024	Expired
[+] PGP Security Software Release Key 2000	●	2048/1024	Expired

1 signature(s) selected

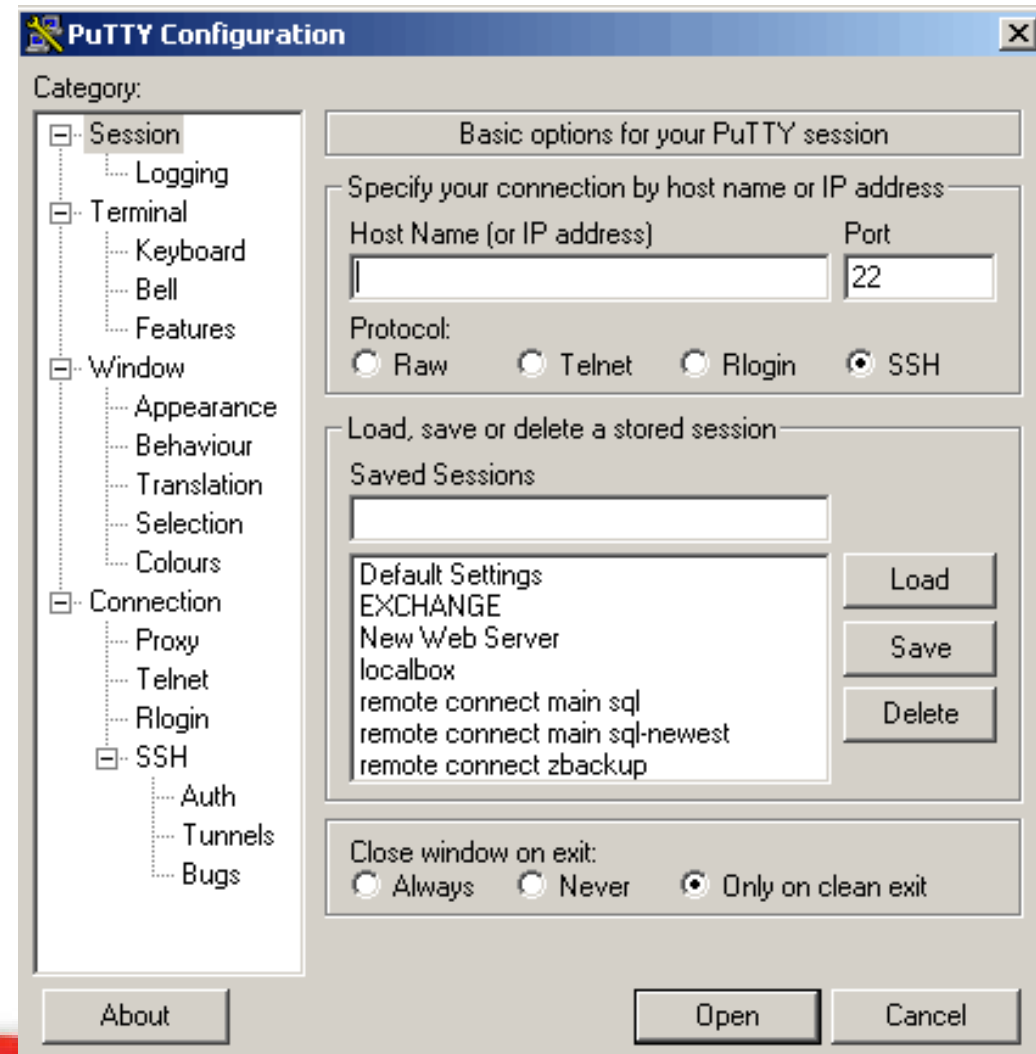
After

# SSH

- What can be done?

## – Encryption

- **FTP, telnet, rlogin can all be replaced with SSH**



# Managed Switches

- What can be done?
  - Managed switch
    - Assign mac address to port
      - This is more difficult but offers an enormous amount of security
      - Some IDS can detect anomaly's such as multiple mac addresses claiming same address

# Network topology best practice

- **Systems**
  - Encrypt data on your desktops
  - Access control for remote systems
  - Disable USB where possible
  - Disable Active-X in web browsers
  - Systems must be locked or logged out when users are away

# Unpatches systems on the rise

- Though easy to apply, often missing from critical servers
  - Third party vendors often overlooked
  - Third party software forgotten
    - Example: Veritas Backup Exec
  - Core processors avoided
  - Patch policy states there needs to be a delay before installation. Installation never happens

## Reviewing logs

- Logs are not being reviewed enough / at all
  - Critical servers should be reviewed daily
  - Use central logging to reduce time
  - High risk systems should store logs on separate server

# Other random threats

- Stuff you should be aware of...

## Music CD's overlooked risk

- Music cd's often stuck into computers without thinking
  - Any CD can be malicious

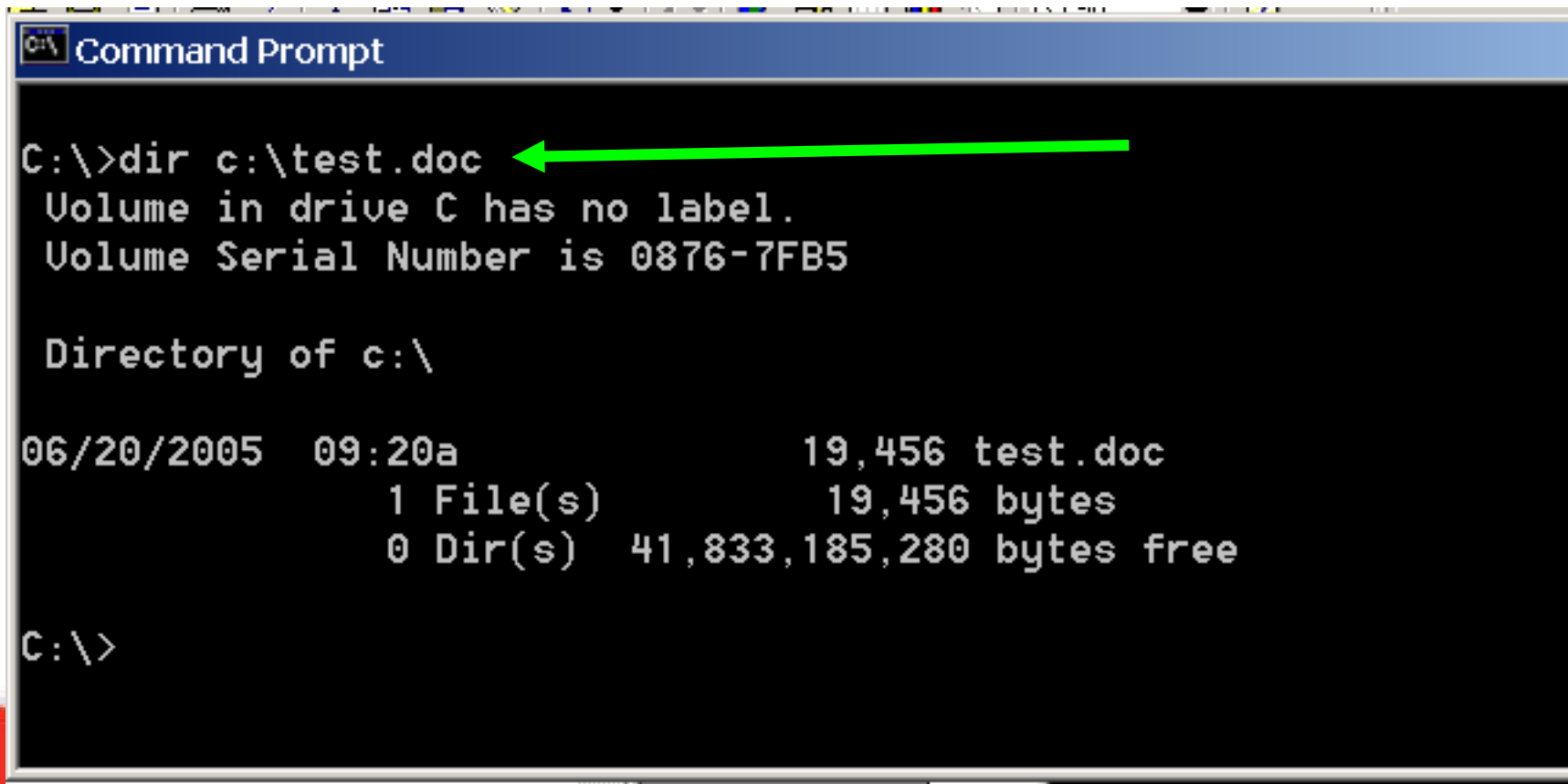
# Policies and Procedures

- Policy enforcement
  - Policies have become stronger but enforcement of those policies is missing
  - User awareness of the policies often missing
- Make sure procedures are documented

## Watching the Hosts

- Hidden Files with Alternate Data Streams (ADS)
  - NTFS file systems offer a unique way to hide files through the use of ADS

# Watching the Hosts



```
Command Prompt

C:\>dir c:\test.doc ←
Volume in drive C has no label.
Volume Serial Number is 0876-7FB5

Directory of c:\

06/20/2005  09:20a                19,456 test.doc
              1 File(s)                19,456 bytes
              0 Dir(s)  41,833,185,280 bytes free

C:\>
```

# Watching the Hosts

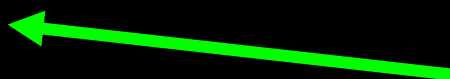
```
Command Prompt

C:\>dir c:\test.doc
Volume in drive C has no label.
Volume Serial Number is 0876-7FB5

Directory of c:\

06/20/2005  09:20a                19,456 test.doc
              1 File(s)                19,456 bytes
              0 Dir(s)  41,833,185,280 bytes free

C:\>type calc.exe > test.doc:calc.exe
C:\>
```



# Watching the Hosts

```
Command Prompt

C:\>type calc.exe > test.doc:calc.exe

C:\>dir c:\test.doc ←
Volume in drive C has no label.
Volume Serial Number is 0876-7FB5

Directory of c:\

06/20/2005  09:24a                19,456 test.doc
              1 File(s)                19,456 bytes
              0 Dir(s)  41,833,152,512 bytes free

C:\>
```

# Watching the Hosts

```
Command Prompt

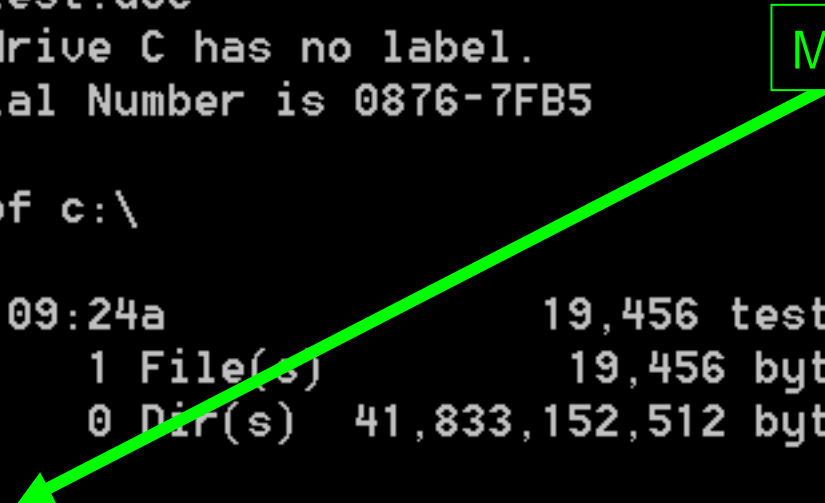
C:\>type calc.exe > test.doc:calc.exe

C:\>dir c:\test.doc
Volume in drive C has no label.
Volume Serial Number is 0876-7FB5

Directory of c:\

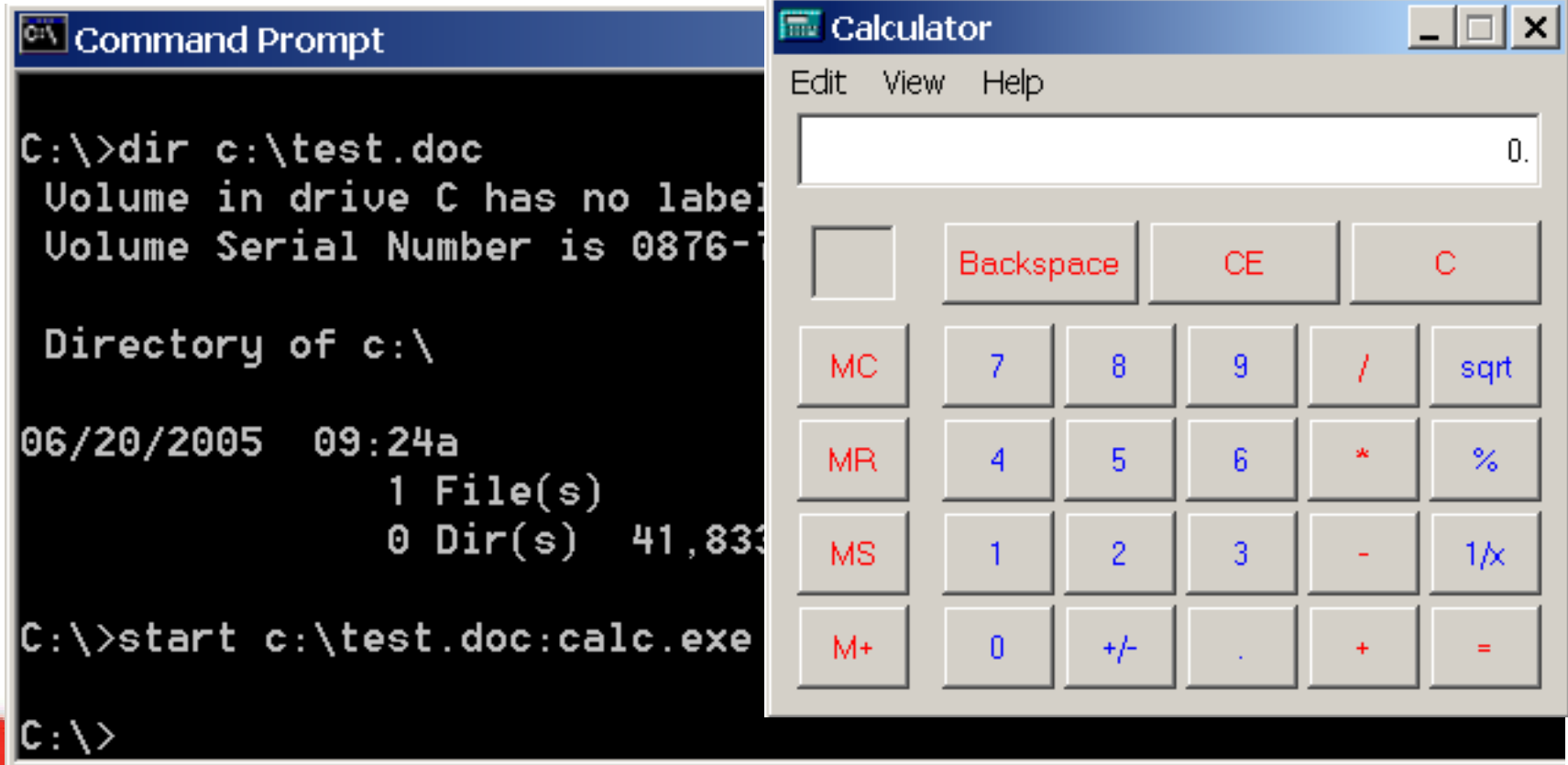
06/20/2005  09:24a                19,456 test.doc
              1 File(s)                19,456 bytes
              0 Dir(s)  41,833,152,512 bytes free

C:\>start c:\test.doc:calc.exe
```



Must include full path

# Watching the Hosts



The image shows two overlapping windows from a Windows operating system. The background window is the Command Prompt, and the foreground window is the Calculator.

**Command Prompt:**

```
C:\>dir c:\test.doc
Volume in drive C has no label
Volume Serial Number is 0876-7

Directory of c:\

06/20/2005  09:24a
             1 File(s)
             0 Dir(s)  41,833

C:\>start c:\test.doc:calc.exe

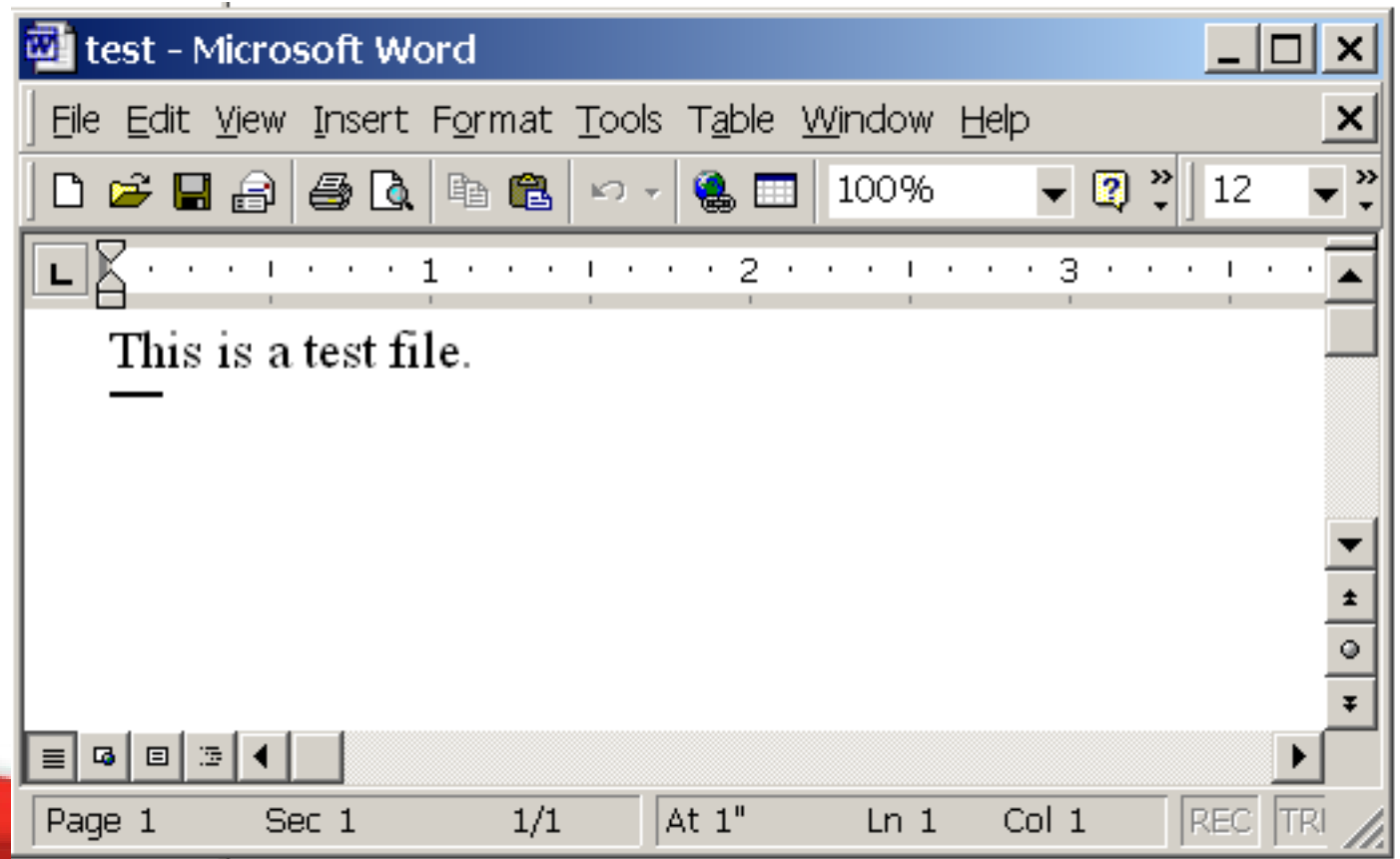
C:\>
```

**Calculator:**

The Calculator window is titled "Calculator" and has a menu bar with "Edit", "View", and "Help". The display shows "0.". The keypad includes buttons for "Backspace", "CE", "C", "MC", "MR", "MS", "M+", and numeric keys 0-9, along with mathematical operators: "/", "\*", "-", "+", and "=". The "sqrt" and "1/x" buttons are also present.

# Watching the Hosts

- Open file c:\test.doc with Microsoft Word



## Watching the Hosts

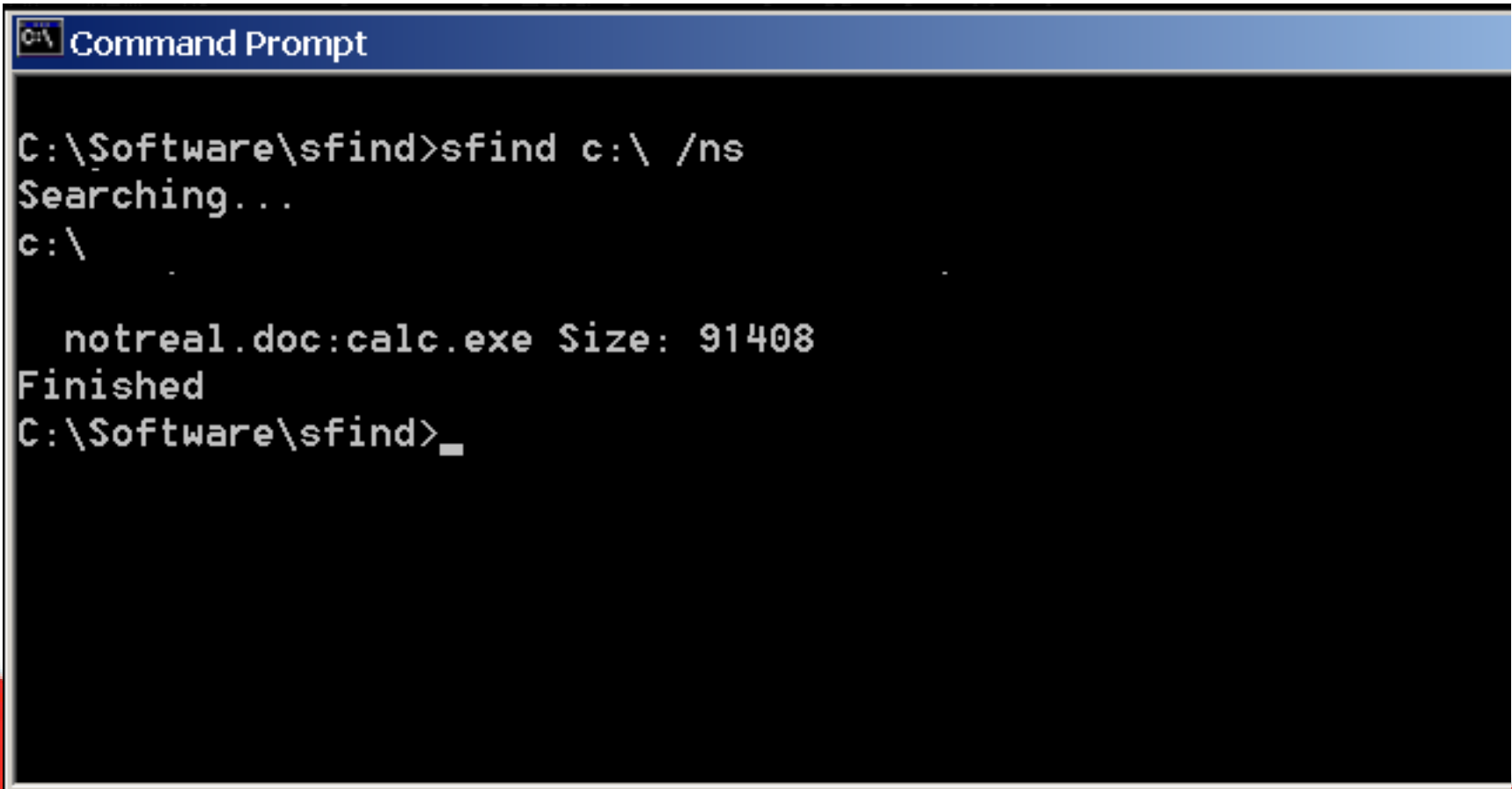
- What can be done about ADS?
  - Regular windows software will not detect these files
  - Third party products have been developed to help but are not perfect.

## Watching the Hosts

- Sfind
  - SFind scans the disk for hidden alternate data streams (ADS) and lists the last access times.
  - sfind [dir] /ns=no subs
  - **This tool must be run from cmd line.**

# Watching the Hosts

- Sfind



```
Command Prompt
C:\Software\sfind>sfind c:\ /ns
Searching...
c:\
    notreal.doc:calc.exe  Size: 91408
Finished
C:\Software\sfind>
```

## Watching the Hosts

- *Sfind & other third party limitations*

### **–IMPORTANT!**

- Sfind and Copy ADS will NOT locate files that have been created on top of existing word doc files. This means, if a word document was created first, then the command: `type filename > existing-document.doc:file.exe`, the file will not be traceable by these third party products

## In the end

- Security risk are everywhere
- Don't try to solve every risk in one week
- Don't assume because a protection has been put in place that there is no more risk
- Most risks can be greatly reduced with awareness training
- Security solutions today will be bypassed tomorrow

# TraceSecurity Inc.

**Comprehensive Security & Risk Assessments**

**IT Audits**

**Penetration Testing**

**Comprehensive Regulation Compliance Review**

**Online Banking Application Testing**

**Remote and Onsite Social Engineering**

**Policy Development and Review**

**Numerous Training Courses available (On site and remote)**

**Anti Phishing, Man in the Middle and Pharming solution**

**Multi Factor Authentication Solution**