Phishing – Tackling the Problem

Session# A2

Michael T. Raggo

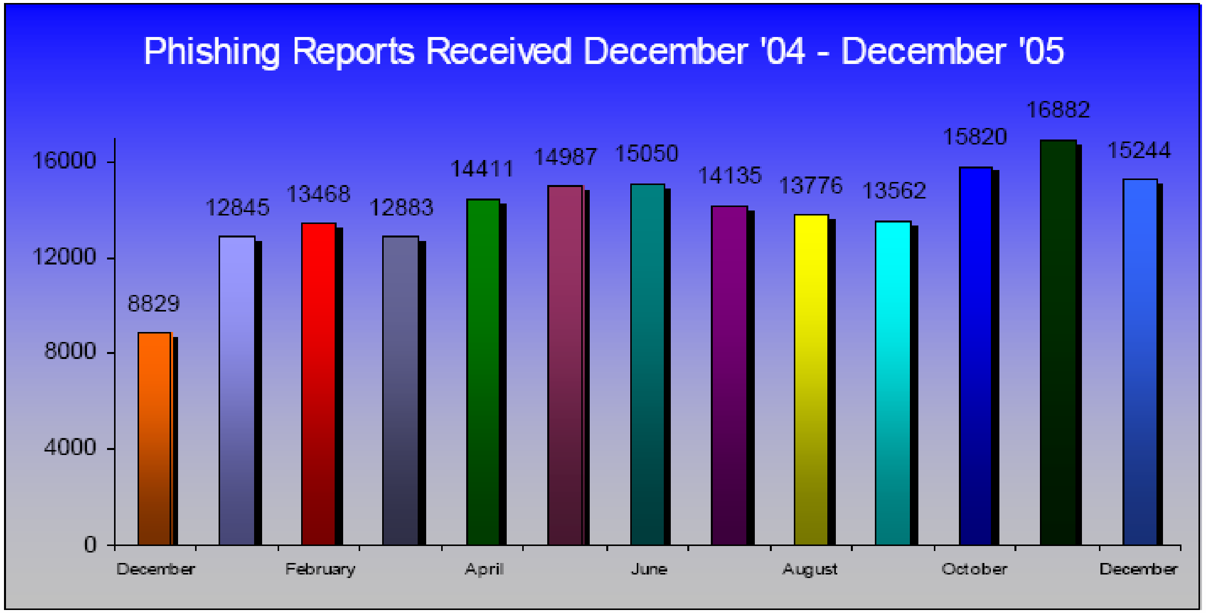
CISSP, IAM, CCSI, SCSA, CSI

VeriSign, Inc.

Monday, April 3 1:30-3PM

The Growing Phishing Problem

- **What is Phishing?**
  - Mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies.
  - Designed to fool recipients into divulging personal data such as account names, passwords, credit card numbers, social security numbers, etc.



Reference: Antiphishing.org

The Growing Phishing Problem (how did we get here?)

Cyber criminal can break their head against the steel walls of the bank's Internet security plan

Or

They can take the easy approach and just ask customers for their username and password for their account

- **Users are still not as protective of their online information as they should be.**
- **An informal survey found that 85% respondents compromised their passwords by providing their actual password, or hint about their password, for a $3 Starbucks gift card.**
- **Phishers are able to convince > 5% of recipients to respond.**

The Growing Phishing Problem (how did we get here?)

Phishing Harder to Detect

- **Phishers no longer send crude, misspelled emails in plain text.**
- **Traditionally, phishers have used social engineering to register "cousin" domains, which sound similar to the company they are trying to impersonate.**
- **Lately, phishers lure victims by forging an email' "from" address**
- **Phishers use browser camouflage techniques such as floating a JavaScript window over the Address Bar to fool people into thinking they are viewing a legitimate, branded site.**
- **The rogue JavaScript remains installed even after leaving the phisher's site.**
  - A phisher could easily write additional JavaScript routines to record everything sent or received through your Web browser until closing the application.

The Client Challenge

- Consumers and institutions suffer significant losses as a result of phishing attacks
  - **Credit card fraud**
  - **Identity theft**
  - **Financial loss**
- Adverse impact on brand image, loss of consumer confidence
- Demonstration of due care to stakeholders
- Resource constraints and the need to focus on high priority, high payoff activities for greatest business efficiency
- Responding requires paid highly skilled professionals on demand 24x7
- Phishing exploits are getting more difficult to detect and shut down
- Complexity of addressing through current incident response process

Phishers are abusing the trust relationship between the victim and the business.

The Client Challenge

- Number of unique phishing reports received in December: 15244
- Number of unique phishing sites received in December: 7197
- Number of brands hijacked by phishing campaigns in December: 121
- **Number of brands comprising the top 80% of phishing campaigns in December: 7**
- **Country hosting the most phishing websites in December: United States**
- **Contain some form of target name in URL: 51 %**
- No hostname just IP address: 32 %
- Percentage of sites not using port 80: 7 %
- **Average time online for site: 5.3 days**
- Longest time online for site: 31 days

Phishing Activity Report December 2005

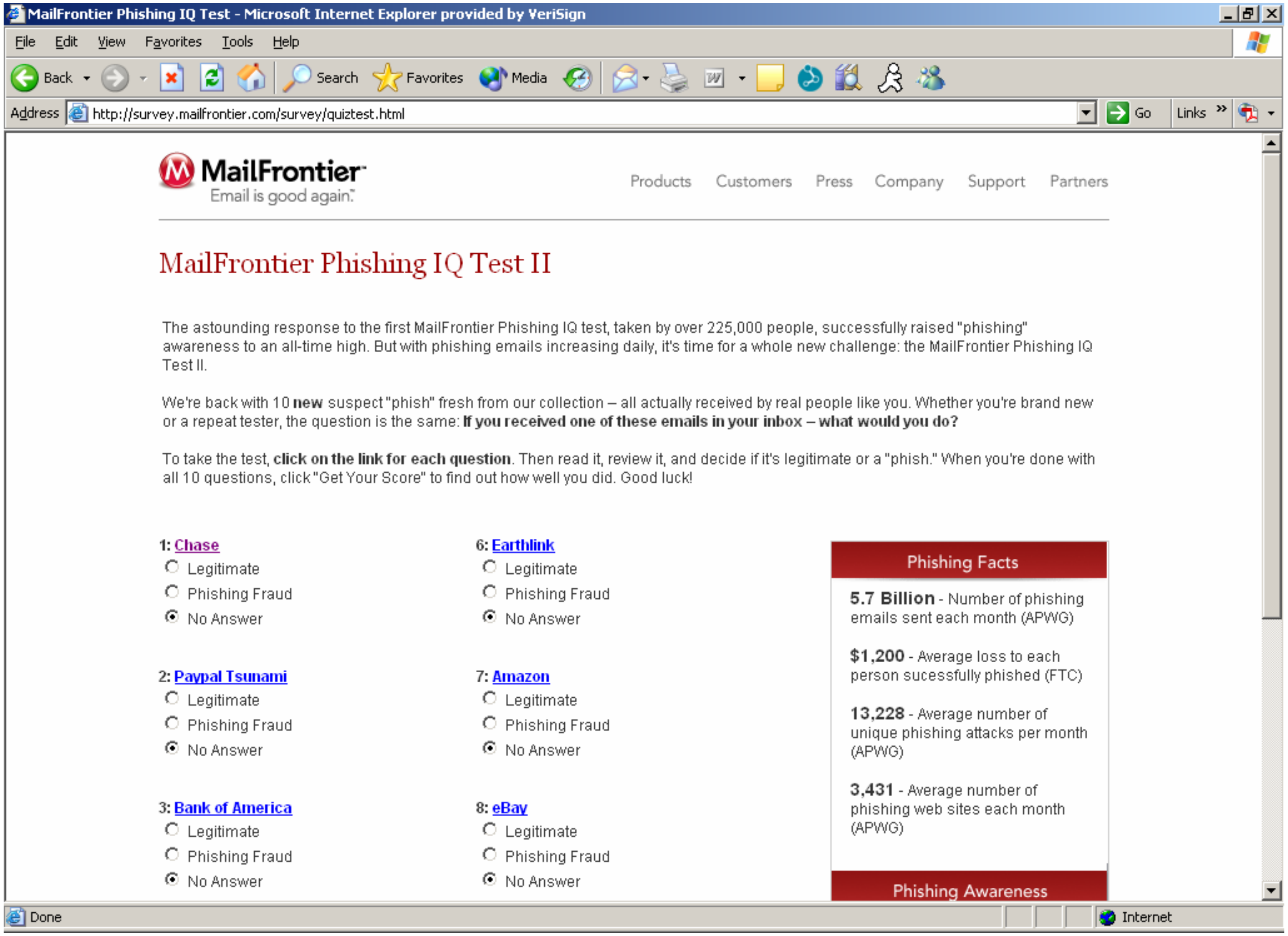
APWG – www.antiphishing.org

Recent targets...

Recent targets other than banks

- **IRS**
  - A phishing attack is **exploiting an open redirect on a U.S. government web site** to gain credibility for bogus e-mails promising an IRS tax refund. The scam e-mail offers an IRS refund of $571 to recipients if they click on a link to govbenefits.gov, a legitimate federal web site that has recently been promoted by President Bush as a tool to streamline relief for victims of Hurricane Katrina. (Source: netcraft.com)
- **Credit Unions**
  - Targets people who are members of credit unions and it looks very official. Not only are the graphics very real looking, but the link in the e-mail looks real too. You never want to update your information or your accounts through an e-mail. Always go to the Web site itself or call the organization.
- **Non-profit organizations**
  - Donations for **Katrina victims**
  - The US Federal Bureau of Investigations (FBI) issued a warning on Jan. 11, 2006, alerting Internet users of a new phishing e-mail requesting financial aid for Randy McCloy Jr., the sole survivor of the **West Virginia mine explosion** that killed 12 men.
- **U.S. Navy and Airforce**
  - In addition, naval seamen who use the Navy Knowledge Online (NKO) Web portal and Air Force personnel with access to the Air Force Portal are also exposed to phishing emails leading them to fictitious Websites. Users are urged to double check the Website address and to change their portal password if they believe they have fallen victim to the scams.

Can you detect a phishing attempt? Take the test!



Address http://survey.mailfrontier.com/survey/quiztest.html

MailFrontier
Email is good again.

MailFrontier Phishing IQ Test II

The astounding response to the first MailFrontier Phishing IQ test, taken by over 225,000 people, successfully raised "phishing" awareness to an all-time high. But with phishing emails increasing daily, it's time for a whole new challenge: the MailFrontier Phishing IQ Test II.

We're back with 10 **new** suspect "phish" fresh from our collection – all actually received by real people like you. Whether you're brand new or a repeat tester, the question is the same: **If you received one of these emails in your inbox – what would you do?**

To take the test, **click on the link for each question**. Then read it, review it, and decide if it's legitimate or a "phish." When you're done with all 10 questions, click "Get Your Score" to find out how well you did. Good luck!

1: Chase
○ Legitimate
○ Phishing Fraud
● No Answer

2: Paypal Tsunami
○ Legitimate
○ Phishing Fraud
● No Answer

3: Bank of America
○ Legitimate
○ Phishing Fraud
● No Answer

6: Earthlink
○ Legitimate
○ Phishing Fraud
● No Answer

7: Amazon
○ Legitimate
○ Phishing Fraud
● No Answer

8: eBay
○ Legitimate
○ Phishing Fraud
● No Answer

Phishing Facts

5.7 Billion - Number of phishing emails sent each month (APWG)

$1,200 - Average loss to each person sucessfully phished (FTC)

13,228 - Average number of unique phishing attacks per month (APWG)

3,431 - Average number of phishing web sites each month (APWG)

Phishing Awareness

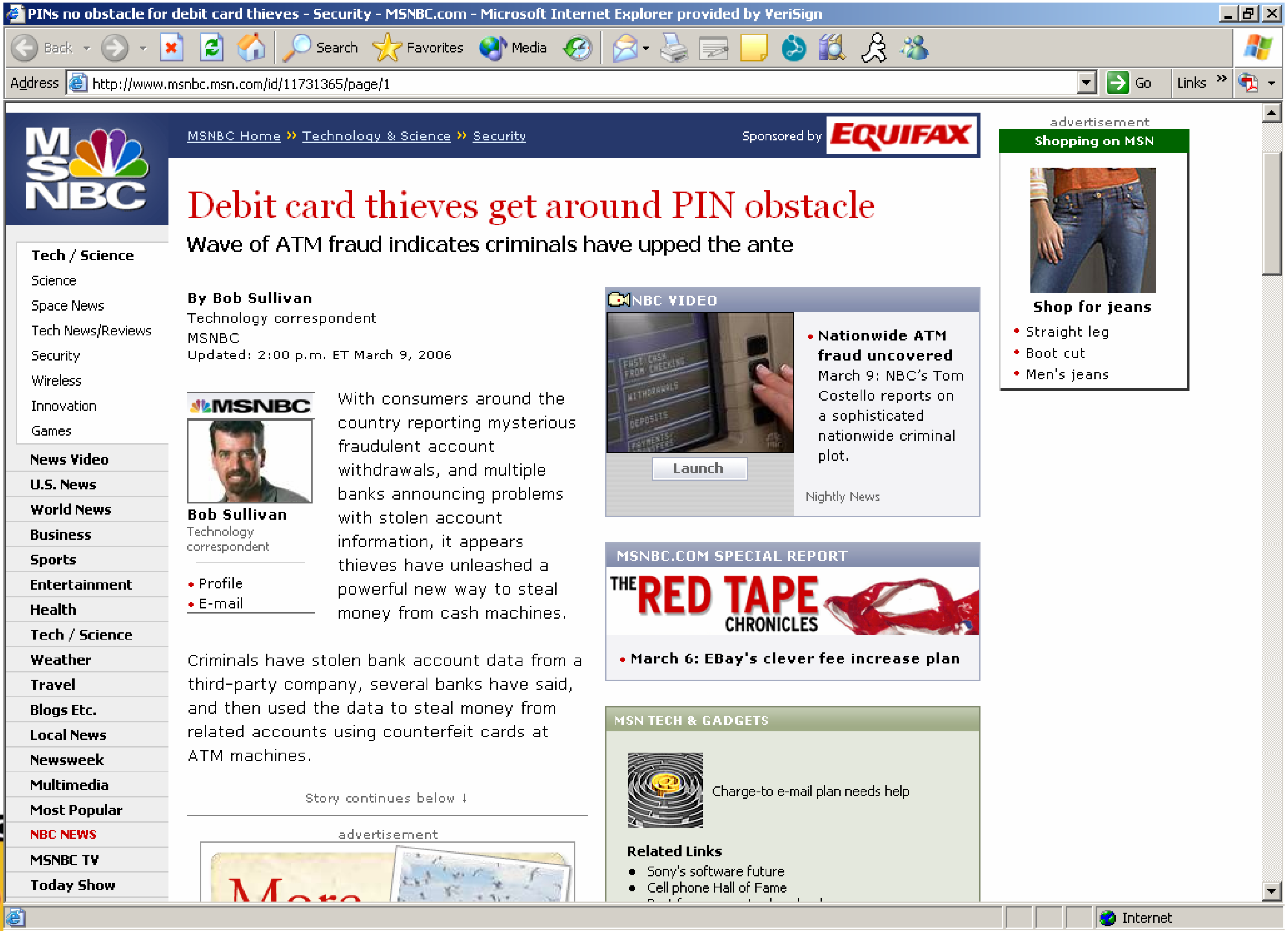
INFOSEC WORLD CONFERENCE & EXPO 2006

MIS TRAINING INSTITUTE

Real Cybercrime

- Stealing Credentials 'Phishing'
  - **Credit Card Numbers**
  - **Bank User Name, Password**
  - **Social Security Number, Address etc. to apply for credentials**
- Using Stolen Credentials 'Carding'
  - **Package Reshipping Schemes**
  - **Money Laundering Schemes**
  - **Identity Theft**
- Support Functions
  - **Compromise machines**
  - **Send Spam**

More Cybercrime


PINs no obstacle for debit card thieves - Security - MSNBC.com - Microsoft Internet Explorer provided by VeriSign
Back
Search
Favorites
Media
Address
Go
Links
Internet

http://www.msnbc.msn.com/id/11731365/page/1

MSNBC Home » Technology & Science » Security

Sponsored by EQUIFAX

Debit card thieves get around PIN obstacle

Wave of ATM fraud indicates criminals have upped the ante

By Bob Sullivan
Technology correspondent
MSNBC
Updated: 2:00 p.m. ET March 9, 2006

Bob Sullivan
Technology correspondent

- Profile
- E-mail

With consumers around the country reporting mysterious fraudulent account withdrawals, and multiple banks announcing problems with stolen account information, it appears thieves have unleashed a powerful new way to steal money from cash machines.

Criminals have stolen bank account data from a third-party company, several banks have said, and then used the data to steal money from related accounts using counterfeit cards at ATM machines.

Story continues below ↓

advertisement

NBC VIDEO

- **Nationwide ATM fraud uncovered**
March 9: NBC's Tom Costello reports on a sophisticated nationwide criminal plot.

Launch

Nightly News

MSNBC.COM SPECIAL REPORT

THE RED TAPE CHRONICLES

- **March 6: EBay's clever fee increase plan**

MSN TECH & GADGETS

Charge-to e-mail plan needs help

Related Links

- Sony's software future
- Cell phone Hall of Fame

advertisement
Shopping on MSN

Shop for jeans

- Straight leg
- Boot cut
- Men's jeans

INFOSEC WORLD CONFERENCE & EXPO 2006

MIS TRAINING INSTITUTE

More Cybercrime

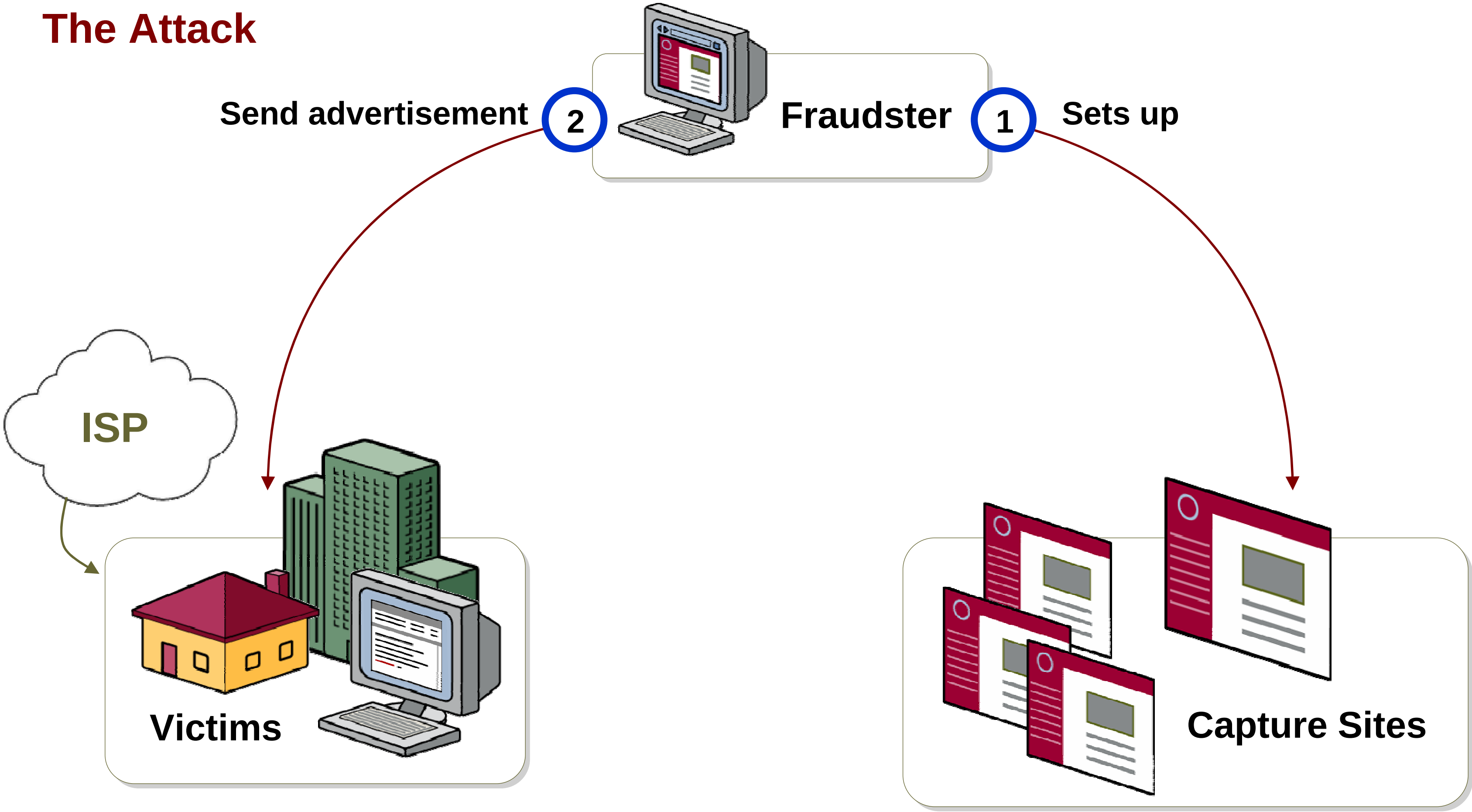
- Advance Fee Frauds (419)
  - **Gangs mostly operate from Nigeria**
  - **Internet application of 'Spanish prisoner' fraud dating to the crusades**
  - **New variant involves fake cashiers checks**
- Extortion / Protection
  - **Attacker compromises web site, offers consulting to solve security issue**

Phishing Attack Components

- Capture Site
  - **Usually a Zombie host or ISP account bought with phished card#**
  - **Impersonates a merchant or trusted brand**
  - **Takes the username/password, card #s, SSN, etc.**
- Means of Advertising Capture Site
  - **Usually Spam sent out from Zombie hosts**
  - **Often uses misleading domain name [payments@*brand*-billing.com]**
- Means of Covering Tracks
  - **Recover data from the capture site**
    - Often use US hosted email provider
  - **Internet Cafes are popular**
- Its Easy to get Caught
  - **Several successful phishing prosecutions, many pending**

Anti-Phishing / Anti-Pharming

The Attack



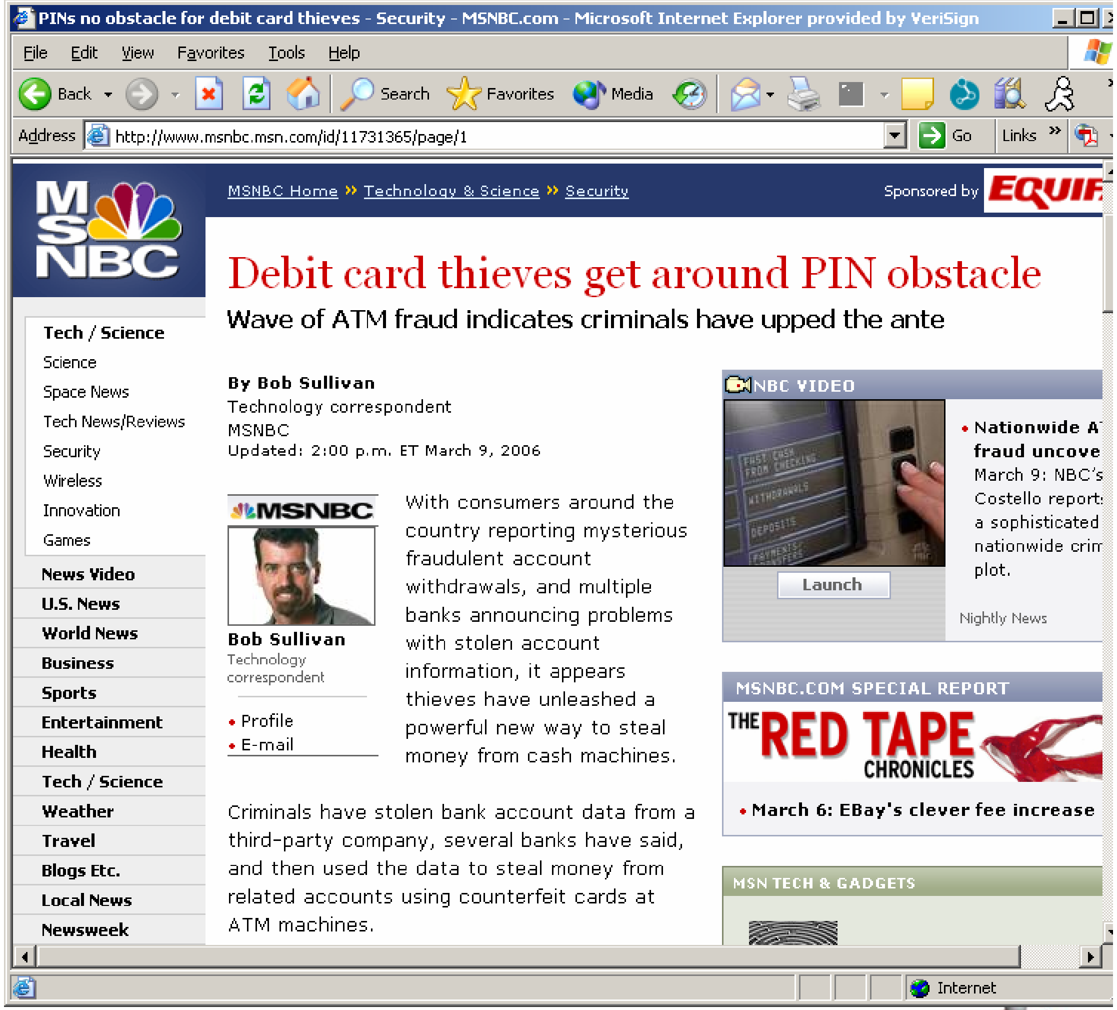
Phishing Tactics

- Hack a Merchant Site
  - **Hope the merchant is silly enough to leave database of plaintext card #s**
- Pretend to be a Merchant
  - **You give me your credit card number, I will give you hijacked software**
  - **Old tactic, spam filtering may have made it unprofitable**
- Pretend to be a Trusted Brand
  - **Or how to get the undivided attention of the brand owner**
  - **Risky, but can be profitable**
- Trojan a Machine
  - **Load spyware onto a consumer machine**
  - **Currently a boutique approach**

“Spear” Phishing

- Dangerous form of e-mail phishing, from a person you know (social engineering aspects)
- Many times the result of a hacked online company
- Information is used to target the individual’s who’s information was stolen

+ Already knows some information about you AND who you do business with



Debit card thieves get around PIN obstacle

Wave of ATM fraud indicates criminals have upped the ante

By Bob Sullivan
Technology correspondent
MSNBC
Updated: 2:00 p.m. ET March 9, 2006

MSNBC
Bob Sullivan
Technology correspondent
- Profile
- E-mail

With consumers around the country reporting mysterious fraudulent account withdrawals, and multiple banks announcing problems with stolen account information, it appears thieves have unleashed a powerful new way to steal money from cash machines.

Criminals have stolen bank account data from a third-party company, several banks have said, and then used the data to steal money from related accounts using counterfeit cards at ATM machines.

- Nationwide A fraud uncove
March 9: NBC’s Costello report a sophisticated nationwide crim plot.

- March 6: EBay's clever fee increase

INFOSEC WORLD CONFERENCE & EXPO 2006

MIS TRAINING INSTITUTE

© If appropriate, Insert your organization’s copyright information

Pharming

Pharming

- **Virus' modifying host file (using malware)**
  - Does not rely on phony emails to lure the user
  - Pharming uses Trojan horse viruses that change the behavior of web browsers.
  - User attempts to access an online banking site or one of the other target sites actually trigger the browser
  - To redirect to a fraudulent site. Once a machine is infected, a user can type the correct URL and still end up at the fraudulent site.

Pharming

Pharming

- **Why use malware?**
  - More relevant data
  - Yields a far greater number of victims (500,000 vs 100 for standard phishing emails)
  - Generates a lot more data, most of it irrelevant
  - Good for about a week before A/V vendors release signatures

Pharming (Malware)

Pharming

- **New variant hides 'elaborate' eBay fraud**
    - Security experts have warned web users to guard against a newly intercepted Mutant of the Feebs trojan that attempts to dupe eBay users with an "elaborate" fraud (identified by Aladdin)
    - Disable the system's antivirus and other security-related products as well as executing other malicious code.
    - JS.Feebs usually arrives by email, but it could also exist in websites that would infect visitors upon access, Aladdin warned.
    - **The script modifies the HOSTS file found on the compromised target PC, thus overriding the default DNS servers**
    - Leads users to enter info at fraudulent site, and upon entering credentials takes the user to the legitimate EBay site.
    - Source: http://www.scmagazine.com/us/news/article/540214/?n=us

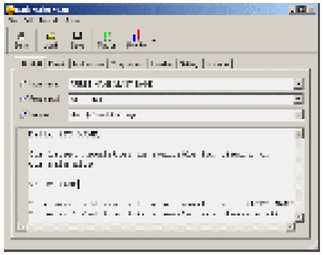
Pharming

Pharming

- **DNS Cache Poisoning**
  - Attacker exploits a flaw in the DNS server software that can make it accept incorrect information
  - Server does not correctly validate DNS responses to ensure that they have come from an authoritative source
  - The server will end up caching the incorrect entries locally and serve them to users that make the same request.
- **DNS Hijacking**
  - Hacking into DNS Servers and change IP addresses
  - Users automatically redirected to bogus site

Phishing Attack Components

- Distributing Mass Emails
  - **Mailer Tools**
    - Darkmailer
    - Sendsafe
    - mailerboy
  - **Means of Advertising Capture Site**
    - Built-in mail server
    - Email database
    - Personalization of macro tags
      - User can create more convincing phishing emails
    - Support for text and HTML emails



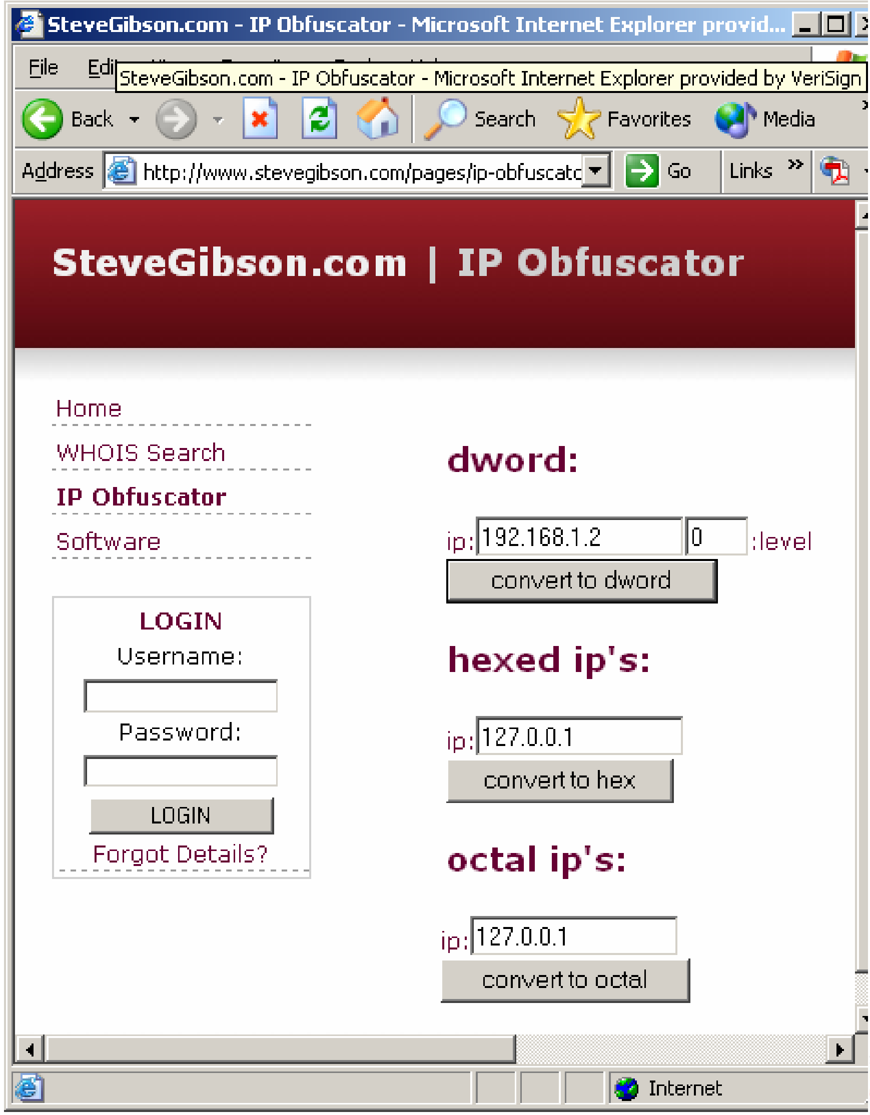
Attack Impersonation & URL Obfuscation

- Bogus Auth Info
  - http://www.cnn.com@www.PCGuide.com
- Deceptive Char Encoding
  - **http://%57%57%57.%50%43%47%55%49%44%45.%43%4F%4D**
- Dotted Octal IP address (leading “0” = octal)
  - http://0321.0104.016.0120
- Dotted Hexidecimal IP address (leading “0x” = hexidecimal)
  - http://0xD1.0x44.0x0E.0x50
- Single Number (Decimal)
  - http://3510898256/

Source: http://www.tcpipguide.com/free/t_URLObscurationObfuscationandGeneralTrickery-3.htm

IP Obfuscation

- IP Obfuscator
- stevegibson.com



Address: http://www.stevegibson.com/pages/ip-obfuscatc

SteveGibson.com | IP Obfuscator

LOGIN

dword:

ip: 192.168.1.2 0 :level

hexed ip's:

ip: 127.0.0.1

octal ip's:

ip: 127.0.0.1

INFOSEC WORLD CONFERENCE & EXPO 2006

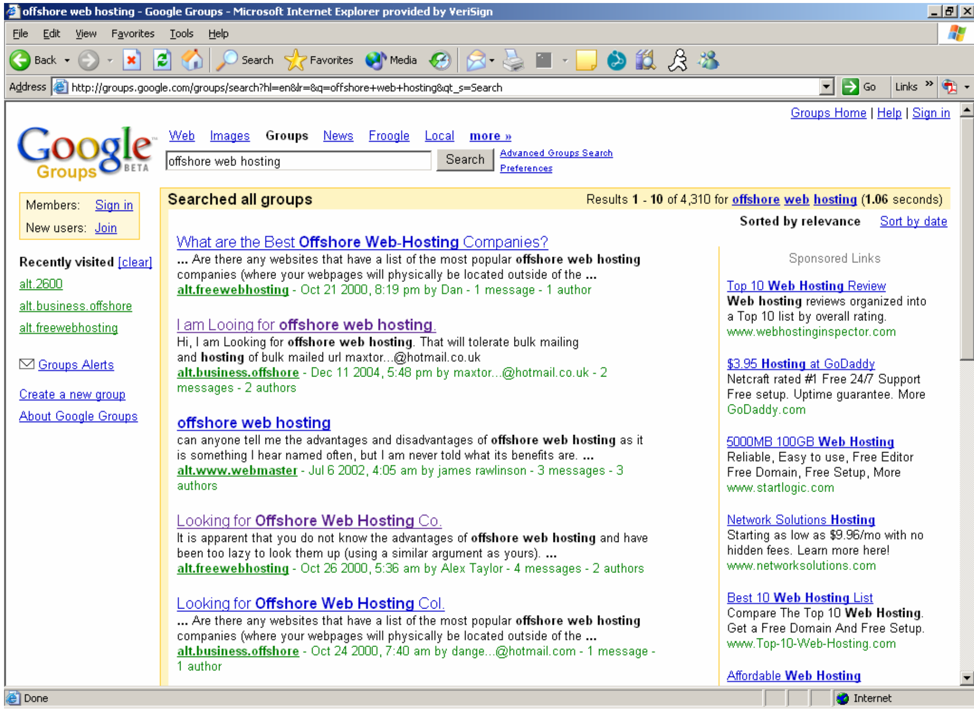
MIS TRAINING INSTITUTE

Mirroring

- What it does
  - A web crawler that crawls a particular site, recursively looks for hyperlinks, and makes an offline copy on the user's hard drive
  - Used for making a Mirror of the site, that looks very similar to the actual site
  - Download all or part of a website to your computer, enabling you to browse the site directly from your hard disk at much greater speeds than if you were to browse the site online
  - Create an exact duplicate, or mirror of a website, complete with subdirectory structure and all required files
  - Download a list of files at known addresses
  - Explore every website linked from a central website
  - Make a list of all pages and files on a website
- Tools
  - Wget
  - Teleport (http://www.tenmax.com)
  - Black Widow

Hosting the Phishing Site

- Legitimate Server with root access
  - **ISP**
  - **Vulnerable server hosted by someone else**
- Anonymous Hosting
  - **Offshore hosting**
    - Purchase with e-gold
    - Webmoney.ru
    - Western Union



http://groups.google.com/groups/search?hl=en&lr=&q=offshore+web+hosting&qt_s=Search

offshore web hosting

Members: Sign in
New users: Join

Recently visited [clear]

alt.2600
alt.business.offshore
alt.freewebhosting

Groups Alerts
Create a new group
About Google Groups

Searched all groups

Results **1** - **10** of 4,310 for **offshore web hosting** (**1.06** seconds)

Sorted by relevance Sort by date

What are the Best **Offshore Web-Hosting** Companies?
... Are there any websites that have a list of the most popular **offshore web hosting** companies (where your webpages will physically be located outside of the **...**
alt.freewebhosting - Oct 21 2000, 8:19 pm by Dan - 1 message - 1 author

I am Looing for **offshore web hosting**.
Hi, I am Looking for **offshore web hosting**. That will tolerate bulk mailing and **hosting** of bulk mailed url maxtor...@hotmail.co.uk
alt.business.offshore - Dec 11 2004, 5:48 pm by maxtor...@hotmail.co.uk - 2 messages - 2 authors

offshore web hosting
can anyone tell me the advantages and disadvantages of **offshore web hosting** as it is something I hear named often, but I am never told what its benefits are. **...**
alt.www.webmaster - Jul 6 2002, 4:05 am by james rawlinson - 3 messages - 3 authors

Looking for **Offshore Web Hosting** Co.
It is apparent that you do not know the advantages of **offshore web hosting** and have been too lazy to look them up (using a similar argument as yours). **...**
alt.freewebhosting - Oct 26 2000, 5:36 am by Alex Taylor - 4 messages - 2 authors

Looking for **Offshore Web Hosting** Col.
... Are there any websites that have a list of the most popular **offshore web hosting** companies (where your webpages will physically be located outside of the **...**
alt.business.offshore - Oct 24 2000, 7:40 am by dange...@hotmail.com - 1 message - 1 author

Sponsored Links

Top 10 **Web Hosting** Review
Web hosting reviews organized into a Top 10 list by overall rating.
www.webhostinginspector.com

$3.95 **Hosting** at GoDaddy
Netcraft rated #1 Free 24/7 Support Free setup. Uptime guarantee. More
GoDaddy.com

5000MB 100GB **Web Hosting**
Reliable, Easy to use, Free Editor Free Domain, Free Setup, More
www.startlogic.com

Network Solutions **Hosting**
Starting as low as $9.96/mo with no hidden fees. Learn more here!
www.networksolutions.com

Best 10 **Web Hosting** List
Compare The Top 10 **Web Hosting**. Get a Free Domain And Free Setup.
www.Top-10-Web-Hosting.com

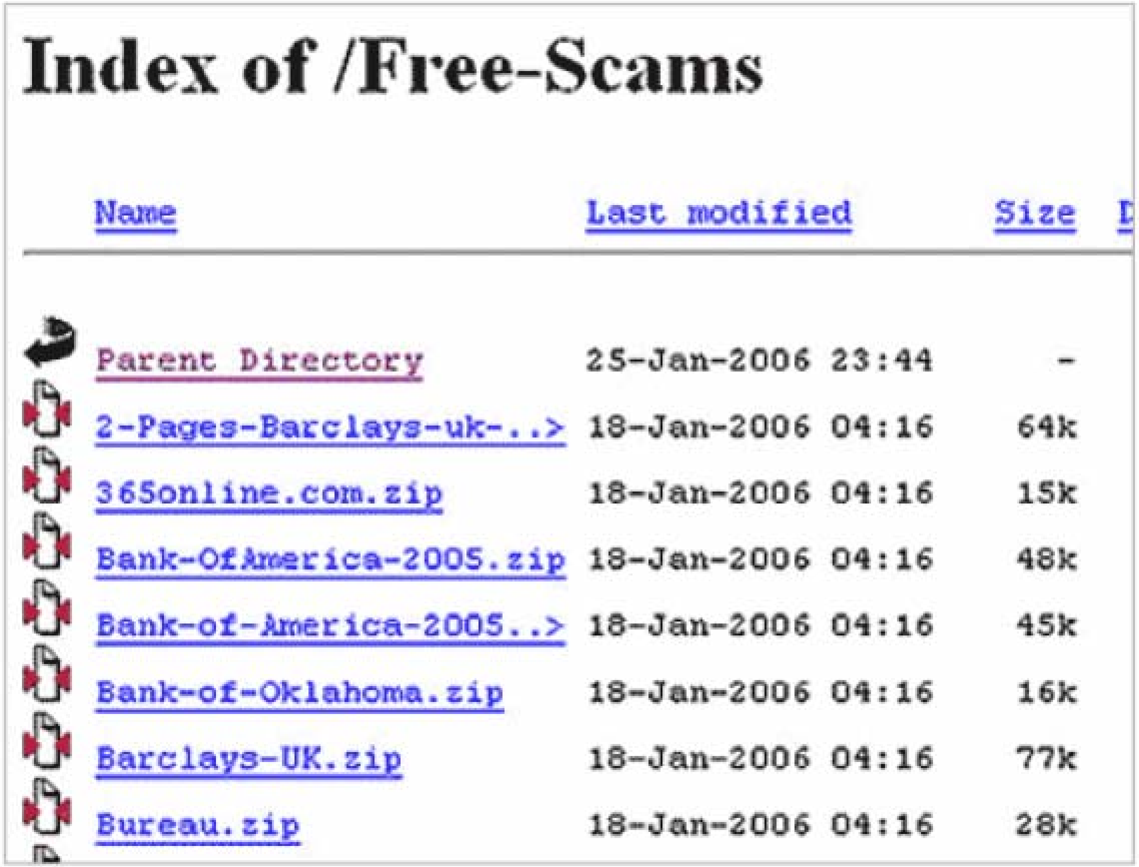
Affordable **Web Hosting**

DIY Phishing Kits

- A kit that includes files for impersonating a legitimate site
  - **Targeting major sites (PayPal, Citibank, Barclays, etc.)**
  - **Shadowcrew.com & carderplanet.com**
  - **Back-end (PHP code) for processing logons IDs and passwords**
  - **May include list of email addresses**

DIY Phishing Kits

- Downloads

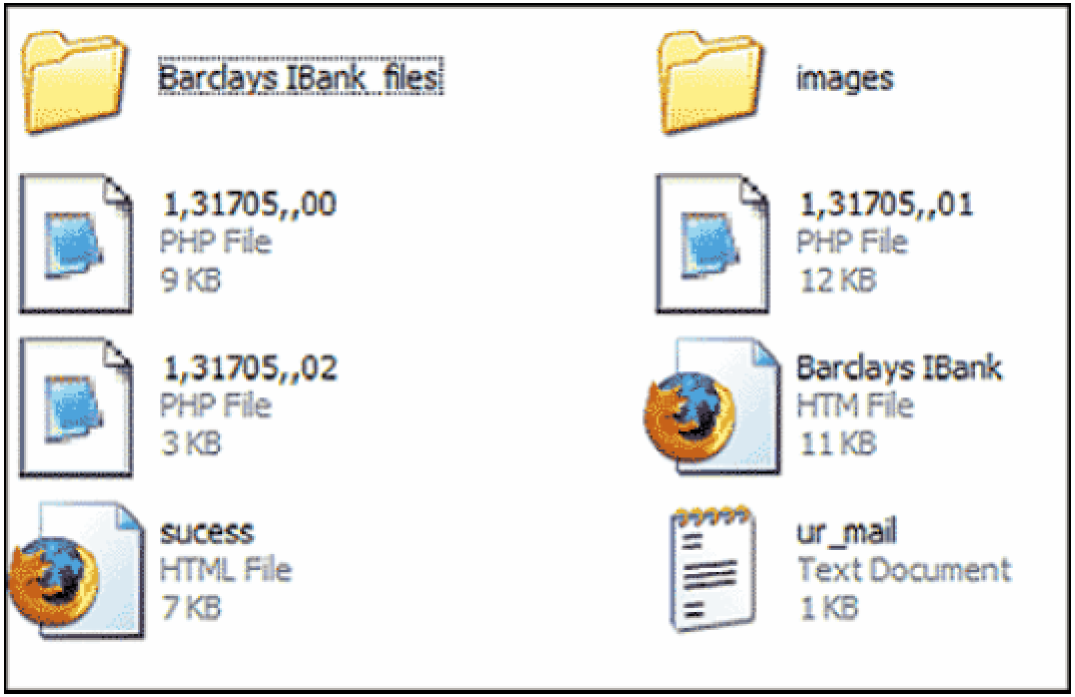


Index of /Free-Scams

Name	Last modified	Size	D
Parent Directory	25-Jan-2006 23:44	-	
2-Pages-Barclays-uk-..>	18-Jan-2006 04:16	64k	
365online.com.zip	18-Jan-2006 04:16	15k	
Bank-OfAmerica-2005.zip	18-Jan-2006 04:16	48k	
Bank-of-America-2005..>	18-Jan-2006 04:16	45k	
Bank-of-Oklahoma.zip	18-Jan-2006 04:16	16k	
Barclays-UK.zip	18-Jan-2006 04:16	77k	
Bureau.zip	18-Jan-2006 04:16	28k	

DIY Phishing Kits

- Inside the zip



Barclays IBank_files

images

1,31705,,00
PHP File
9 KB

1,31705,,01
PHP File
12 KB

1,31705,,02
PHP File
3 KB

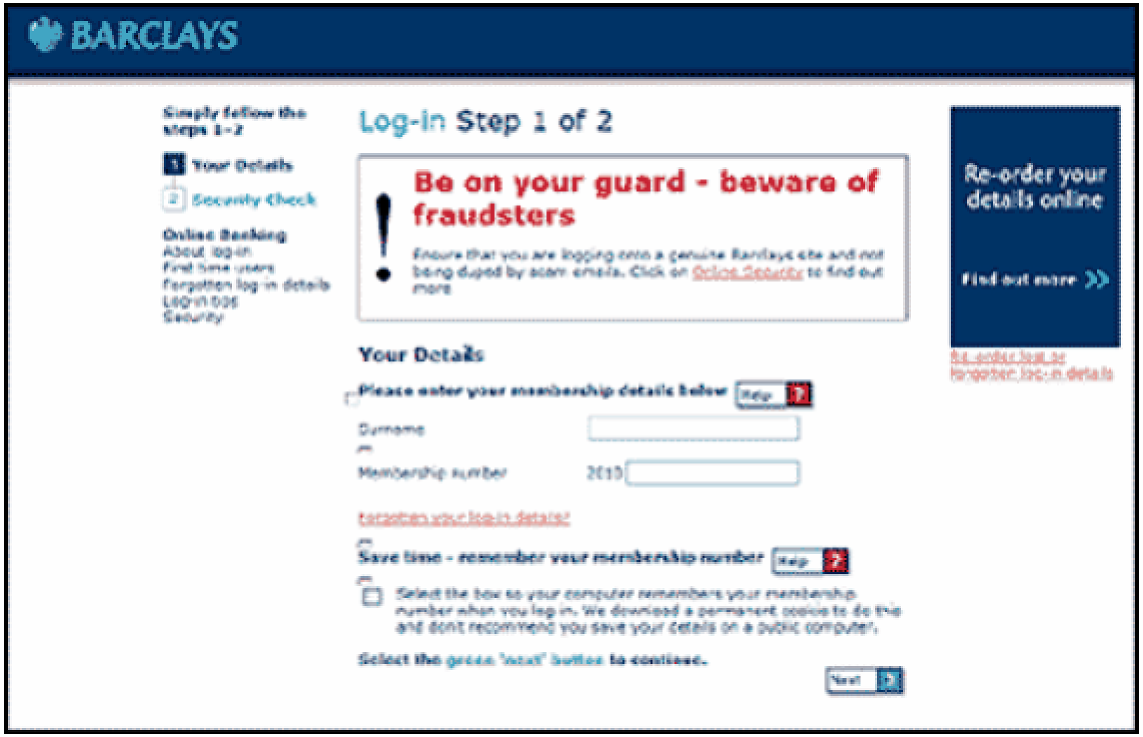
Barclays IBank
HTM File
11 KB

sucess
HTML File
7 KB

ur_mail
Text Document
1 KB

DIY Phishing Kits

- Setting up the site



BARCLAYS

Simply follow the steps 1-2

1 Your Details

2 Security Check

Online Banking
About log-in
First time users
Forgotten log-in details
Log-in box
Security

Log-in Step 1 of 2

Be on your guard - beware of fraudsters

Ensure that you are logging onto a genuine Barclays site and not being duped by scam emails. Click on Online Security to find out more

Your Details

Please enter your membership details below Help ?

Surname

Membership number 2010

forgotten your log-in details?

Save time - remember your membership number Help ?

□ Select the box so your computer remembers your membership number when you log in. We download a permanent cookie to do this and dont recommend you save your details on a public computer.

Select the green 'next' button to continue.

Next

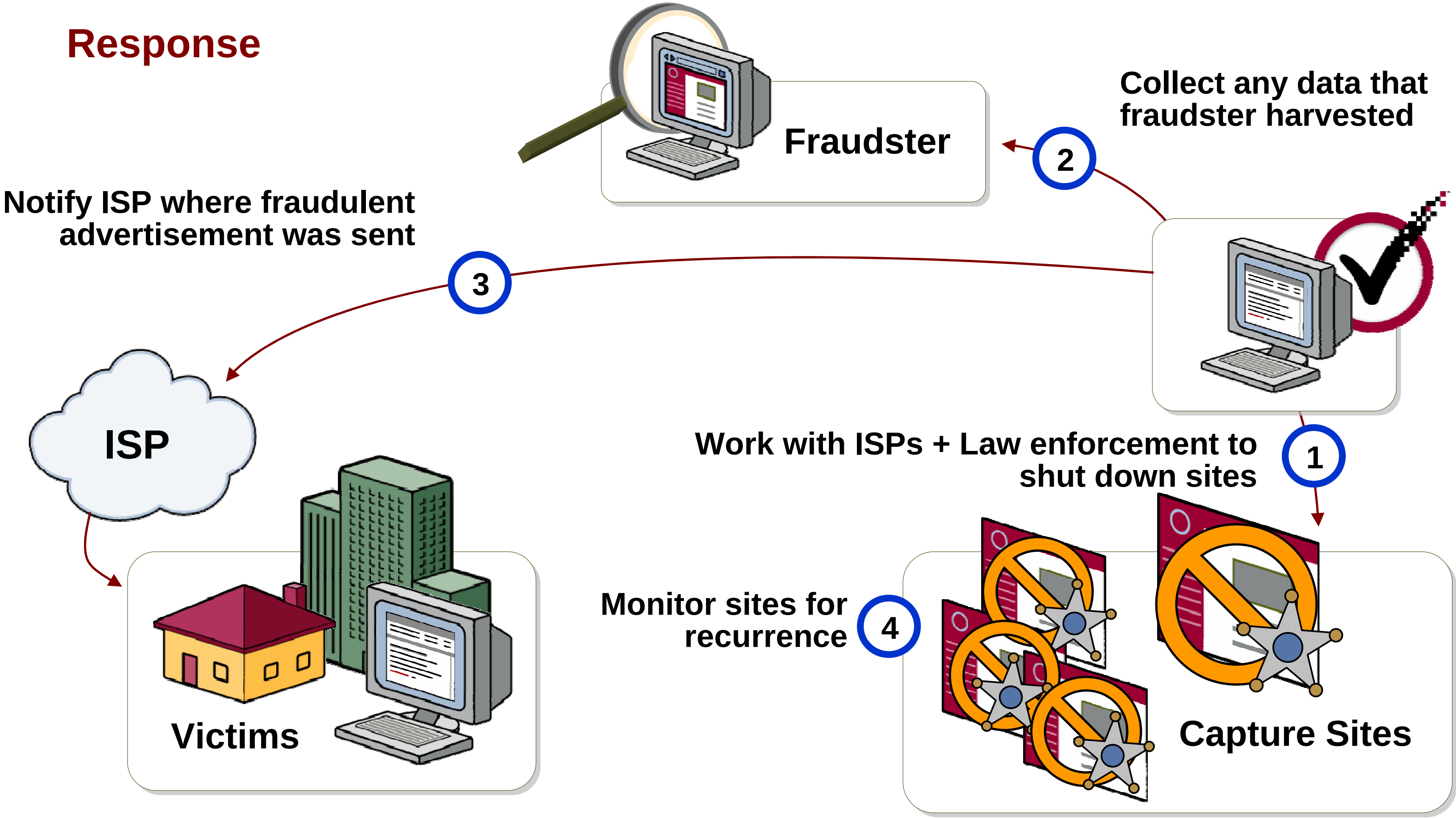
Re-order your details online

Find out more »

Re-order log-in
forgotten log-in details

Anti-Phishing / Anti-Pharming

Response



Fraudster

Collect any data that fraudster harvested

2

Notify ISP where fraudulent advertisement was sent

3

ISP

Work with ISPs + Law enforcement to shut down sites

1

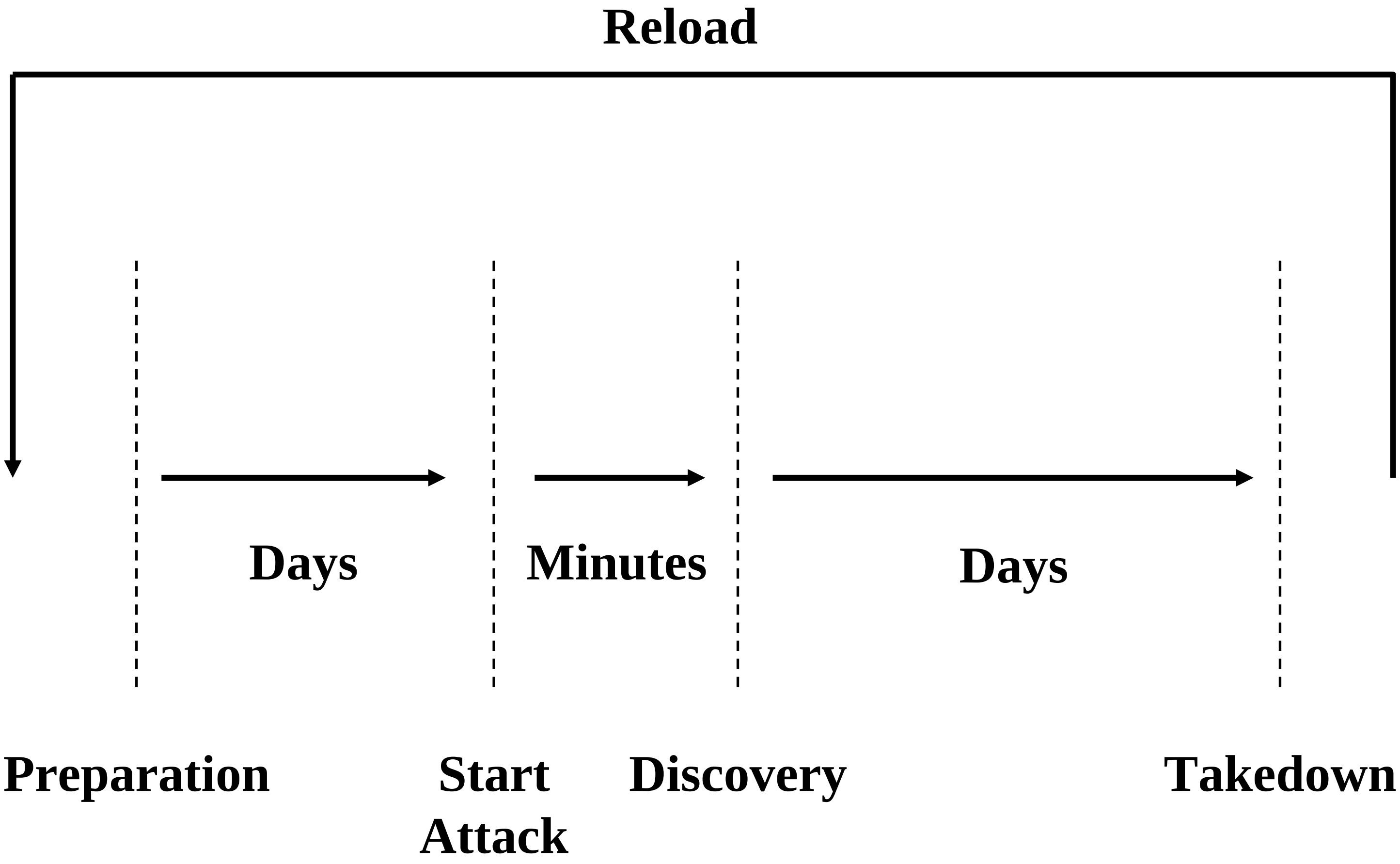
Victims

Monitor sites for recurrence

4

Capture Sites

Phishing Attack Timeline



Phishing Case Study

- **The Preparation – Approximately 4:00 am PST**
  - Anonymous host **server at an ISP in Tacoma, Washington on unprotected FTP share**
  - **Uploaded a rootkit onto the server**
  - **Created new logins into the terminal services for the server**
  - **The** capture site **was unlinked page off of an otherwise legitimate website**
  - **No** cousin domains
  - **Used a standard PERL mailer utility to send out the** fraudulent advertisements**.**

Phishing Case Study (Continued)

- **Attack Begins at 9:17 am PST**
- **Fraudulent Advertisement sent to customers**
- The time between when the phisher gained access to the anonymous host and uploaded the rootkit to mails sent is ***under 5 hours***
- The phisher covered his tracks by deleting the mail list once the emails went out

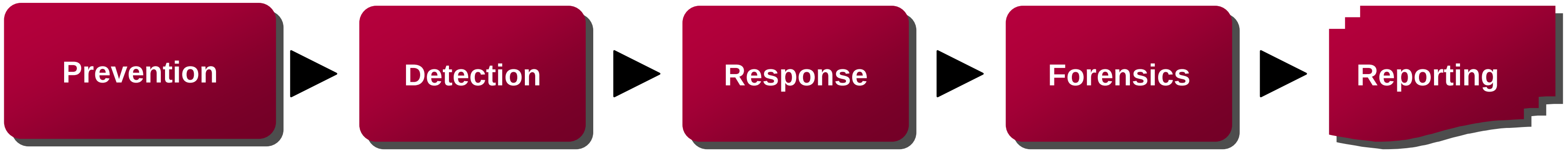
Phishing Case Study (Continued)

- Discovery – 9:42 am PST
  - VeriSign became aware of the scam email 25 minutes after attack launched
  - Link took the victim to a site that looked like the login page. No matter what data was entered for username and password, the phisher's site then took the victim to a page that collected further information.

Phishing Case Study (Continued)

- **The Take Down – 9:47 am PST**
  - **First try - ARIN “abuse@” contacts but only got voice mail**
  - **Leveraging our extensive database of contacts, our next attempt to contact them got us to a live person.**
  - **By 9:47 (5 minutes after VeriSign became aware of the attack) the scam page is taken down.**
  - **We were able to get the site down so quickly in part because the site was domestic and because of the quick response of our fraud team.**
- **Forensics Investigation**
  - **Copy of the scam site payload**
  - **We also had the FTP logs to give us details of where and when the phisher started this from.**
    - FTP logs show that he accessed the servers from 3 separate IP’s, two from Romania and one from Spain. Harvested data and sent it to a free web email account.

Anti-Phishing Solution



Prevention ▶ Detection ▶ Response ▶ Forensics ▶ Reporting

- ✓ Policy, Programs & Education
- ✓ Incident Response policy gap analysis
- ✓ Assessment services
- ✓ Strong Authentication

- ✓ Brand Management
- ✓ Domain Name Monitoring
- ✓ Web Crawlers
- ✓ Spam Filters
- ✓ Customer Notification

- ✓ 24x7 Support
- ✓ Integrated Processes
- ✓ Global Abuse Contact DB
- ✓ Shutdown Phishing Sites
- ✓ Damage Assessment

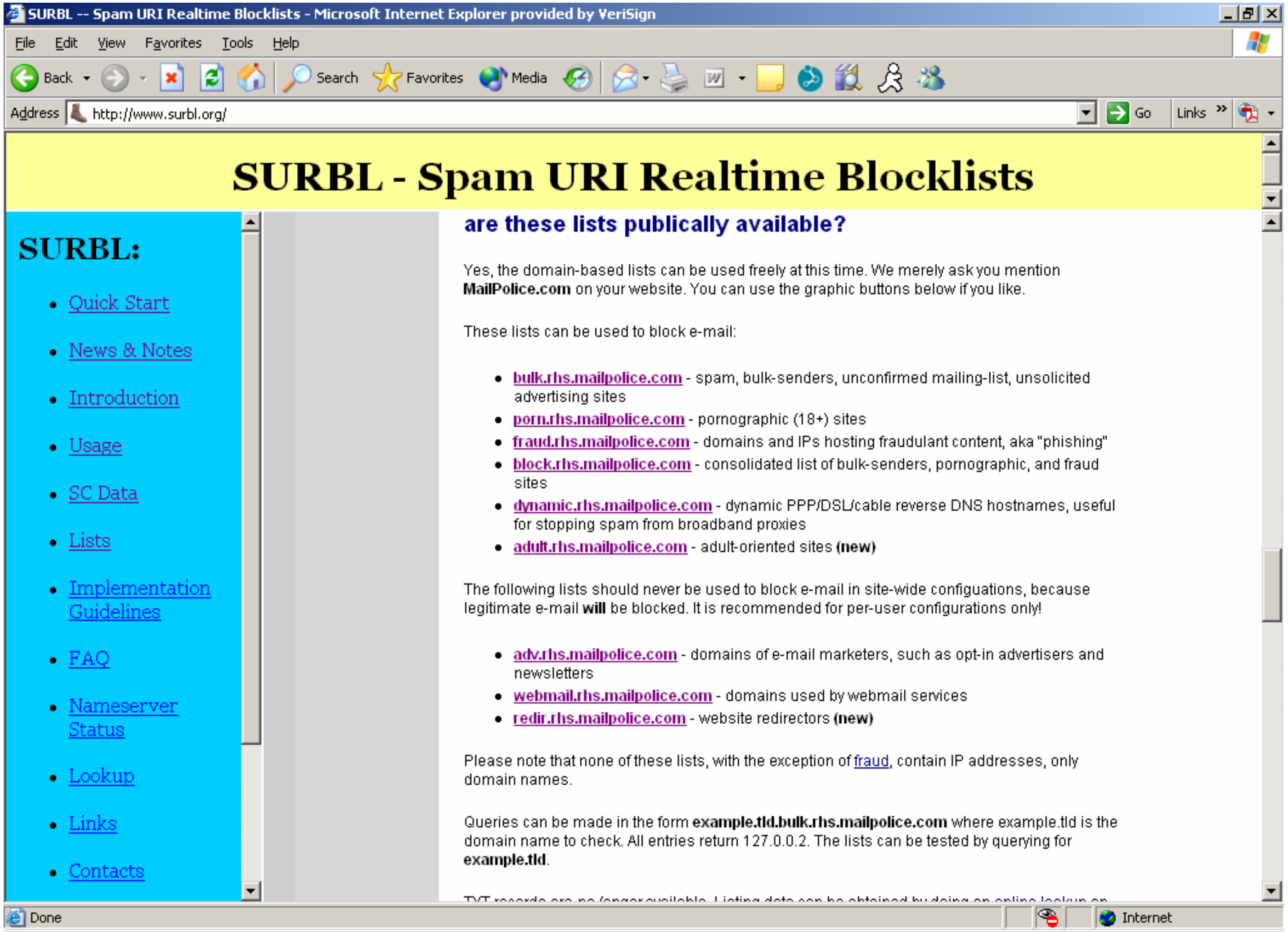
- ✓ Cyber Forensics
- ✓ Follow-up Investigation

- ✓ Initial Incident Validations
- ✓ Progress Reports
- ✓ Investigative Report
- ✓ Trend Reporting

Prevention

- Security Consulting
  - **Vulnerability and application assessments – Penetration Test!**
  - **Assess current Incident Response processes, policies, and vulnerabilities**
  - **From gap analysis, recommend and create optimal Incident Response policies**
  - **Implement educational programs – send updates to customers/users**
- Authentication Services
  - **Prevent email spoofing**
    - Sender ID (Microsoft)
    - DomainKeys Identified Mail (Yahoo! & Cisco)
  - **Browser-based protection (prevention & detection)**
    - Netcraft Toolbar
    - WholeSecurity Web Caller-ID
    - TrustBar
  - **Digital signatures for outgoing emails, providing sender validation**
  - **Strong Authentication for bank site login**

Blocklists


SURBL -- Spam URI Realtime Blocklists - Microsoft Internet Explorer provided by VeriSign
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://www.surbl.org/
Go
Links
Done
Internet

SURBL - Spam URI Realtime Blocklists

SURBL:

- Quick Start
- News & Notes
- Introduction
- Usage
- SC Data
- Lists
- Implementation Guidelines
- FAQ
- Nameserver Status
- Lookup
- Links
- Contacts

are these lists publically available?

Yes, the domain-based lists can be used freely at this time. We merely ask you mention **MailPolice.com** on your website. You can use the graphic buttons below if you like.

These lists can be used to block e-mail:

- bulk.rhs.mailpolice.com - spam, bulk-senders, unconfirmed mailing-list, unsolicited advertising sites
- porn.rhs.mailpolice.com - pornographic (18+) sites
- fraud.rhs.mailpolice.com - domains and IPs hosting fraudulant content, aka "phishing"
- block.rhs.mailpolice.com - consolidated list of bulk-senders, pornographic, and fraud sites
- dynamic.rhs.mailpolice.com - dynamic PPP/DSL/cable reverse DNS hostnames, useful for stopping spam from broadband proxies
- adult.rhs.mailpolice.com - adult-oriented sites **(new)**

The following lists should never be used to block e-mail in site-wide configuations, because legitimate e-mail **will** be blocked. It is recommended for per-user configurations only!

- adv.rhs.mailpolice.com - domains of e-mail marketers, such as opt-in advertisers and newsletters
- webmail.rhs.mailpolice.com - domains used by webmail services
- redir.rhs.mailpolice.com - website redirectors **(new)**

Please note that none of these lists, with the exception of fraud, contain IP addresses, only domain names.

Queries can be made in the form **example.tld.bulk.rhs.mailpolice.com** where example.tld is the domain name to check. All entries return 127.0.0.2. The lists can be tested by querying for **example.tld**.

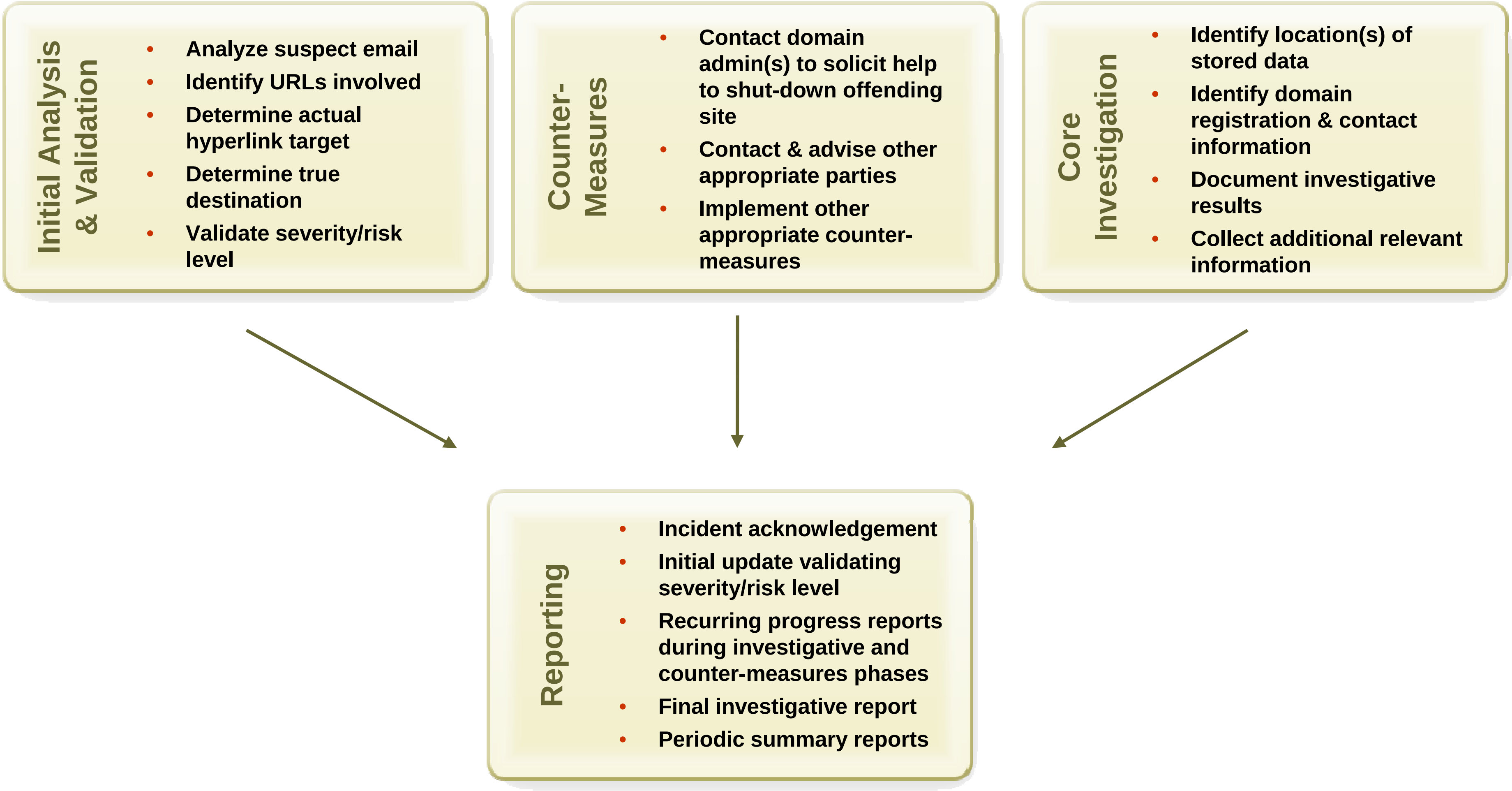
TXT records are no longer available. Listing data can be obtained by doing an online lookup on

Detection - Digital Brand Management

- Brand Equity
  - **Misuse of a company’s trademarks, logos, and intellectual property online**
    - Logo copied and stolen
    - Logo altered
    - Objectionable content
    - Unauthorized distributors of products or intellectual property
  - **Monitor and protect trademarks, logos, and intellectual property online**
    - Online global monitoring – brand audit of worldwide domain name registrations
    - Identify and shutdown unauthorized distributors of products or intellectual property – Renegade Sites
    - Identify and shutdown objectionable sites using company trademarks and logos

Are you in control of your brand in the digital world? Over 70% of the URLs associated with world’s top 25 brands are not owned by those brands!

Response: Phishing Response Methodology



Initial Analysis & Validation

- Analyze suspect email
- Identify URLs involved
- Determine actual hyperlink target
- Determine true destination
- Validate severity/risk level

Counter-Measures

- Contact domain admin(s) to solicit help to shut-down offending site
- Contact & advise other appropriate parties
- Implement other appropriate counter-measures

Core Investigation

- Identify location(s) of stored data
- Identify domain registration & contact information
- Document investigative results
- Collect additional relevant information

Reporting

- Incident acknowledgement
- Initial update validating severity/risk level
- Recurring progress reports during investigative and counter-measures phases
- Final investigative report
- Periodic summary reports

Resources & References

- Phishing Exposed by Lance James
- Anti-Phishing Workgroup
  - **http://www.antiphishing.org/**
- Tools and Resources
  - **http://www.scientis.com/Security/Phishing.html**
- Up to date scam listing
  - **http://www.millersmiles.co.uk/archives/17**

Q&A

INFOSEC WORLD™

CONFERENCE & EXPO 2006

Session
Title of Your Presentation

MIS® TRAINING INSTITUTE