Bad Cocktail: Application Hacks + Spear Phishing

By Rohyt Belani

Who Am I?

- CEO of Intrepidus Group
- Adjunct Professor at Carnegie Mellon University
- Frequent Speaker at Black Hat, OWASP, MISTI, Hack In The Box, FSP

What Is Spear Phishing?

How Does It Work?

Killer Cocktail =

Phishing

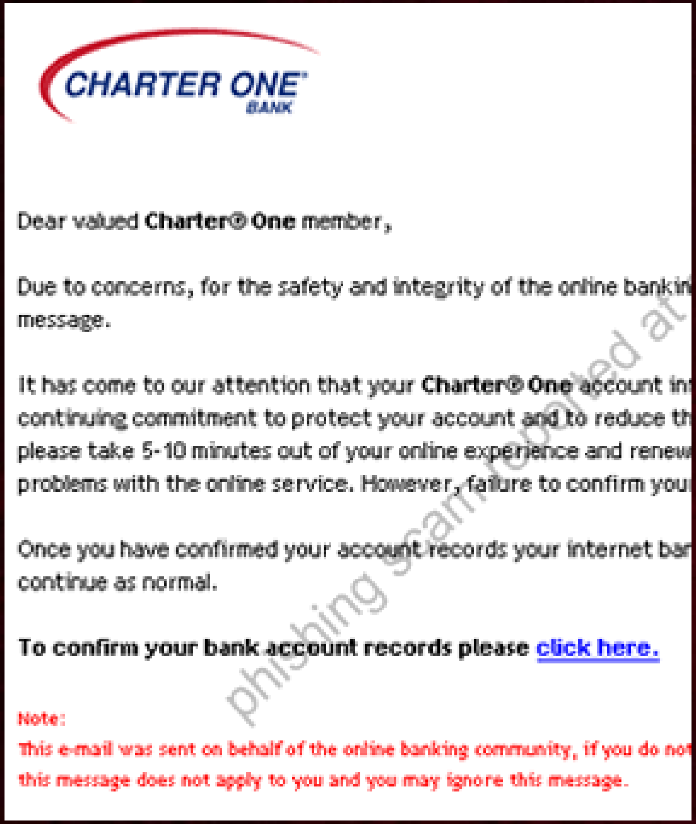
+

Application Hacks

Phish n' Scripts

- More realistic phishing attack because it uses the actual site (often even over HTTPS)
- XSS Tricks
  - Expect HEX encoding of attack parameters
    - "<script>" = "%3C%73%63%72%69%70%74%3E"
  - Short attack parameter that links to a remote ".js" file for more javascript or an "iframe" tag that loads remote HTML form

XSS Emails in the Real World



CHARTER ONE BANK

Dear valued Charter® One member,

Due to concerns, for the safety and integrity of the online bankin
message.

It has come to our attention that your Charter® One account in
continuing commitment to protect your account and to reduce th
please take 5-10 minutes out of your online experience and renew
problems with the online service. However, failure to confirm you

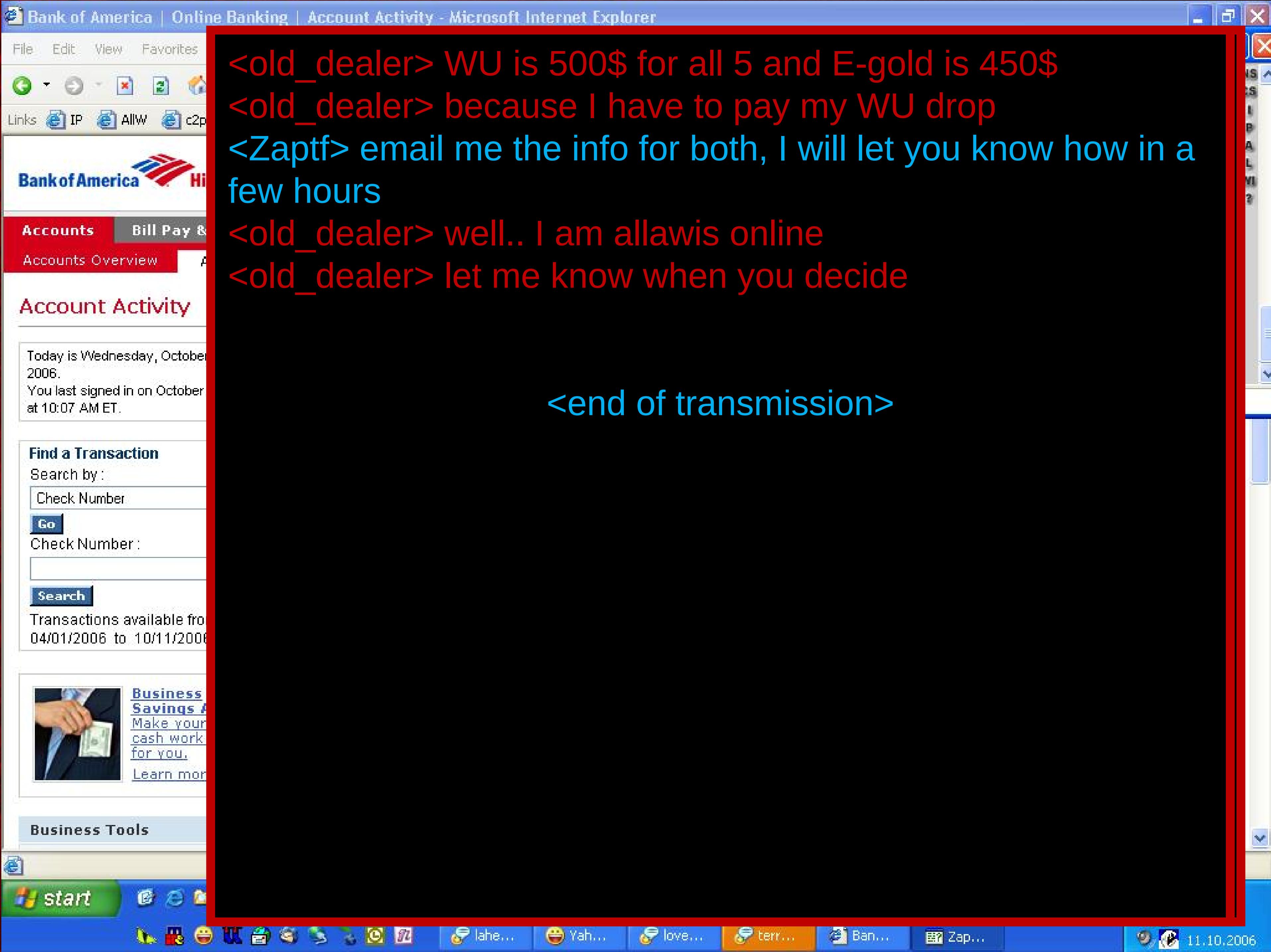
Once you have confirmed your account records your internet ba
continue as normal.

To confirm your bank account records please click here.

Note:
This e-mail was sent on behalf of the online banking community, if you do not
this message does not apply to you and you may ignore this message.

- Charter One Bank (Citizens Financial Group)
  - March 2005

  https://www.charterone.com/pf/?ygtkt=%61%53%33%87%64%38%80%87%76%23%66%59%44%95%16%28%88%12%19%85%91%20...



Account Activity

Today is Wednesday, Octobe
2006.
You last signed in on October
at 10:07 AM ET.

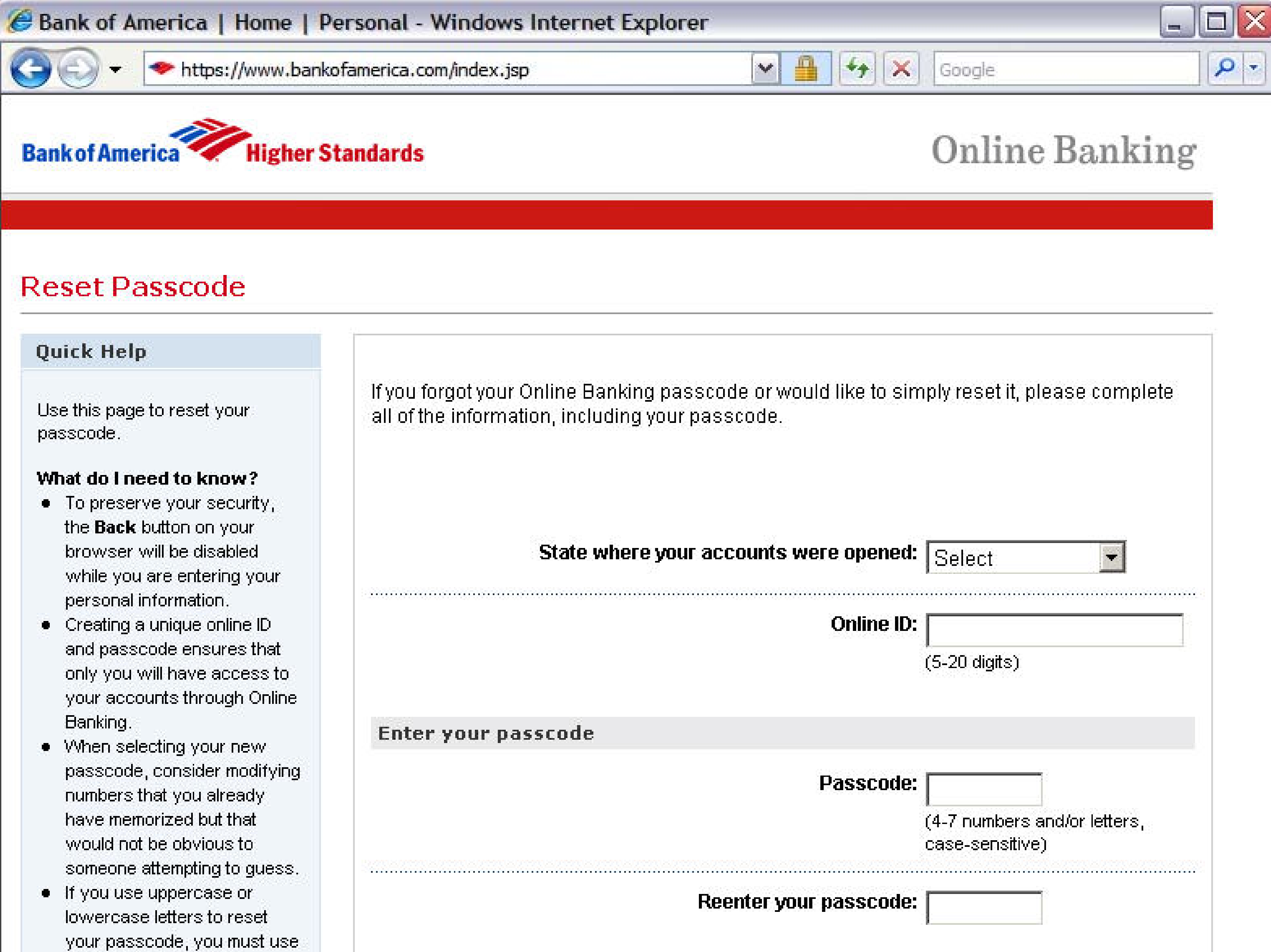
Find a Transaction
Search by :
Check Number
Go
Check Number :
Search
Transactions available fro
04/01/2006 to 10/11/200

Business
Savings A
Make your
cash work
for you.
Learn mor

Business Tools

<old_dealer> WU is 500$ for all 5 and E-gold is 450$
<old_dealer> because I have to pay my WU drop
<Zaptf> email me the info for both, I will let you know how in a few hours
<old_dealer> well.. I am allawis online
<old_dealer> let me know when you decide

<end of transmission>


Bank of America | Home | Personal - Windows Internet Explorer
https://www.bankofamerica.com/index.jsp
Google
Bank of America Higher Standards
Online Banking

Reset Passcode

Quick Help

Use this page to reset your passcode.

What do I need to know?

- To preserve your security, the **Back** button on your browser will be disabled while you are entering your personal information.
- Creating a unique online ID and passcode ensures that only you will have access to your accounts through Online Banking.
- When selecting your new passcode, consider modifying numbers that you already have memorized but that would not be obvious to someone attempting to guess.
- If you use uppercase or lowercase letters to reset your passcode, you must use

If you forgot your Online Banking passcode or would like to simply reset it, please complete all of the information, including your passcode.

State where your accounts were opened: Select

Online ID:

(5-20 digits)

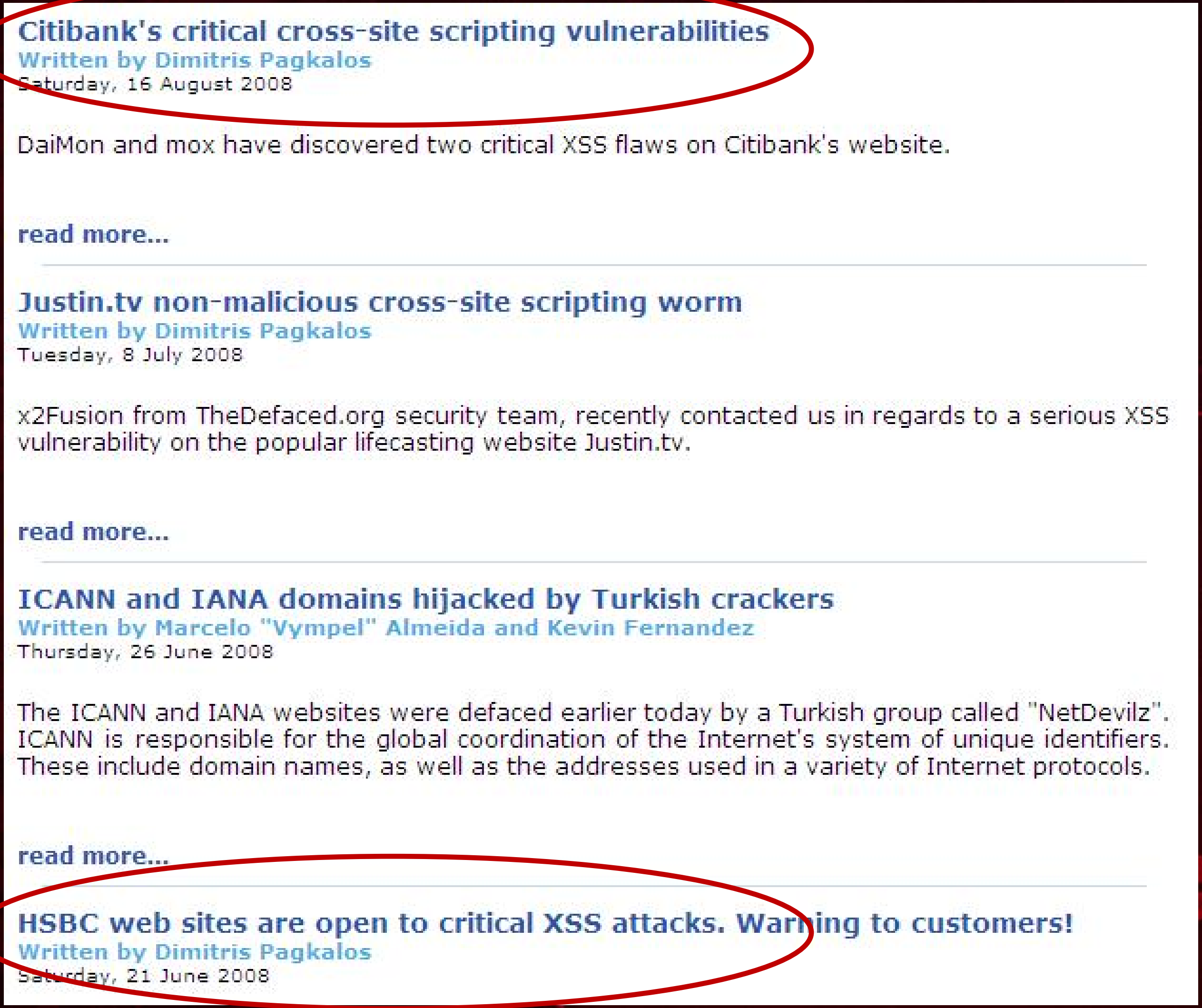
Enter your passcode

Passcode:

(4-7 numbers and/or letters, case-sensitive)

Reenter your passcode:

Cross Site Scripting Not Dead Yet



Citibank's critical cross-site scripting vulnerabilities
Written by Dimitris Pagkalos
Saturday, 16 August 2008

DaiMon and mox have discovered two critical XSS flaws on Citibank's website.

read more...

Justin.tv non-malicious cross-site scripting worm
Written by Dimitris Pagkalos
Tuesday, 8 July 2008

x2Fusion from TheDefaced.org security team, recently contacted us in regards to a serious XSS vulnerability on the popular lifecasting website Justin.tv.

read more...

ICANN and IANA domains hijacked by Turkish crackers
Written by Marcelo "Vympel" Almeida and Kevin Fernandez
Thursday, 26 June 2008

The ICANN and IANA websites were defaced earlier today by a Turkish group called "NetDevilz". ICANN is responsible for the global coordination of the Internet's system of unique identifiers. These include domain names, as well as the addresses used in a variety of Internet protocols.

read more...

HSBC web sites are open to critical XSS attacks. Warning to customers!
Written by Dimitris Pagkalos
Saturday, 21 June 2008

Looking London Talking Tokyo

- Used to mask where the link is really taking you

- Often comes in one of two ways
  - – 3rd party trust (known vendor, popular search site)
  - – Or misconfiguration on your site

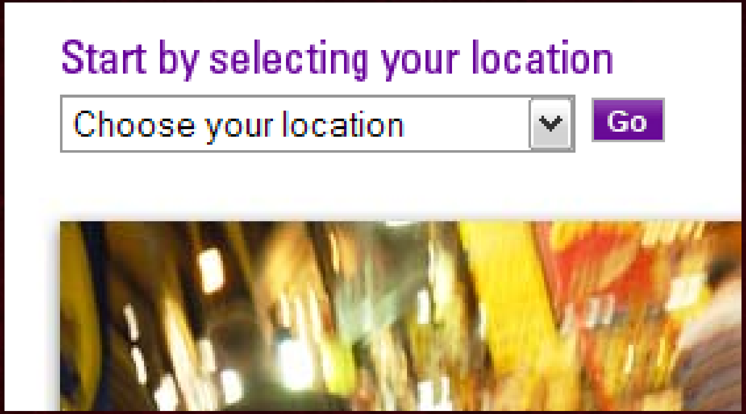
URL 3rd Party Redirection

- Because search engines never lie… right?
  - http://www.google.com/url?q=http://68.207.70.141/signin.ebay.com/Members_Log-in.htm
  - http://world.altavista.com/urltrurl?url=http%3A%2F%2Fworld2altavista.com%2FSearch

- Often used for tracking Ad clicks, many sites will have a way to redirect based off a URL sent in

Homegrown Redirection

- Be careful about how your own redirects are coded



Start by selecting your location

Choose your location

- http://site.com/?location=us may become http://site.com/?location=http://evil.com
- Again HEX encoding tricks can be used
  - “evil.com” = “%65%76%69%6C%2E%63%6F%6D”

Flashy Phish

- Flash Objects can perform their own redirects.
- “eBay Flash-redirect scam”
  - Reported in Aug 2007
  - Attacker creates legitimate auction page but places malicious flash “SWF” file in description
  - When another eBay user views their page, they are redirected to a cloned malicious site which ask them to login

Next Level: CSRF->DNS->Phish

- This attack as been described at “drive-by pharming” and seen in the wild in Jan 2008 targeting Mexican banking sites
- Complex Attack in 3 Steps
  - 1) Use a CSRF attack against home router to reconfigure DNS settings

```
https://192.168.1.1/apply.cgi?submit_button=Sub
mit&action=Apply&block_wan=1&block_loopbacks=0&
dns1=6.6.6.6
```

Next Level: CSRF->DNS->Phish

- Complex Attack in 3 Steps (continued
  - 2) Attacker hosts DNS server at “6.6.6.6” and returns malicious DNS responses for known banking sites.
  - 3) Malicious response point to fake cloned site. The URL matches the legitimate site, however DNS gave out the wrong IP address
- Attacker can just wait for victim to surf to their trusted site, or send an email with a real link

Oh..and BTW Don’t Rely On SSL For Comfort

- Not all Certificate Authorities are made equal
- http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202423911432

YOU CAN HAVE A CERTIFICATE FOR ANY DOMAIN!

A Report From The Trenches

Symptoms

- “I see a trade executed from my account …10000 shares of a company I haven’t even heard about, were purchased on January 17 (2006) @ 2 pm from my account!” – a client of a well-established brokerage firm in NYC.
- 7 other clients of the same brokerage firm report the same issue – in January 2006.

Investigation

- Was the brokerage firm hacked?
- Was it the end user who was hacked?
- We had dates and times of the trade executions as a clue.

Investigation

- Our team began reviewing the brokerage firm’s online trading application for clues
    - Network logs
    - Web server logs
    - Security mechanisms of the application
- We asked to duplicate the victim’s hard drive and review it for indicators of compromise.

Web Server Logs

- Requested IIS logs for January 17, 2006 from all the (load balanced) servers.
- Combined the log files into one common repository = 1 GB
- Microsoft's Log Parser to the rescue

Microsoft LogParser

Parsed out all requests to execute.asp using Microsoft Log Parser:

```
LogParser -o:csv "select * INTO
  execute.csv from *.log where
  cs-uri-stem like
  '/execute.asp%'"
```

Can You Find The Smoking Gun?

#Fields:time	c-ip	cs-method	cs-uri-stem	cs-uri-query	Status
1:03:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
1:04:35	172.16.54.33	POST	/execute.asp	sessionid=3840943093874b3484c3839de9340494	200
1:08:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
1:10:19	172.16.87.231	POST	/execute.asp	sessionid=298230e0393bc09849d839209883993	200
1:13:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
1:18:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
1:19:20	172.16.121.3	POST	/execute.asp	sessionid=676db87873ab0393898de0398348c89	200
1:21:43	172.16.41.53	POST	/execute.asp	sessionid=3840943093874b3484c3839de9340494	200
1:23:16	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
1:28:15	172.16.22.33	POST	/execute.asp	sessionid=90198e1525e4b03797f833ff4320af39	200
.	.	.	.	.	.
.	.	.	.	.	.

Next Step

Parsed out all requests with the suspicious sessionid

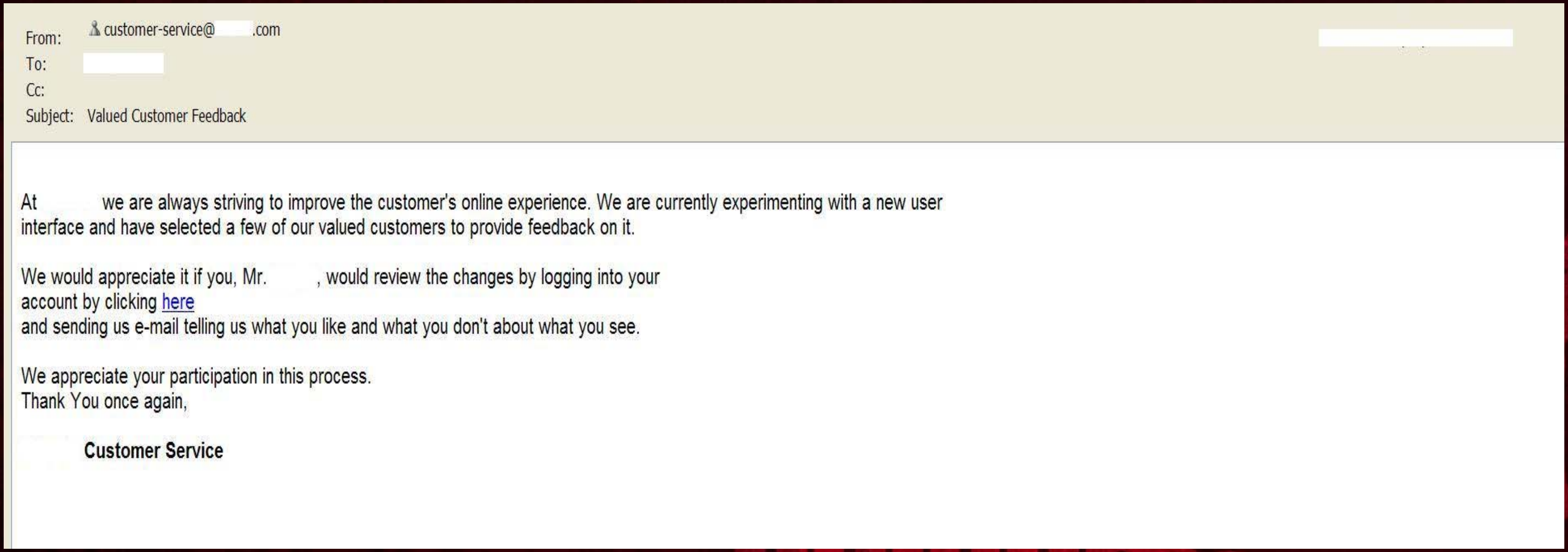
```
LogParser -o:csv "select * INTO
  sessionid.csv from *.log where
  cs-uri-query like
  '%90198e1525e4b03797f833ff4320af39'
  "
```

Can You Find The Smoking Gun?

```
                                cs-                                                                     Statu
#Fields:time    c-ip            method  cs-uri-stem     cs-uri-query                                        s
     1:18:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
     1:23:16    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
     1:28:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
           .          .            .          .                          .                                .
           .          .            .          .                          .                                .

    13:53:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
    13:58:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200

    14:03:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200

    14:07:23    172.16.14.166   POST    /login.asp      sessionid=90198e1525e4b03797f833ff4320af39       200

    14:07:54    172.16.14.166   POST    /account.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
    14:08:15    172.16.22.33    POST    /execute.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
    14:10:09    172.16.22.33    POST    /confirm.asp    sessionid=90198e1525e4b03797f833ff4320af39       200
```

Phishing?

- No indications of key logging trojans, malware, viruses, etc. were found on the victim's computer.
- Look what we found in the archived .pst file:



From: customer-service@[redacted].com [redacted]
To: [redacted]
Cc:
Subject: Valued Customer Feedback

At we are always striving to improve the customer's online experience. We are currently experimenting with a new user interface and have selected a few of our valued customers to provide feedback on it.

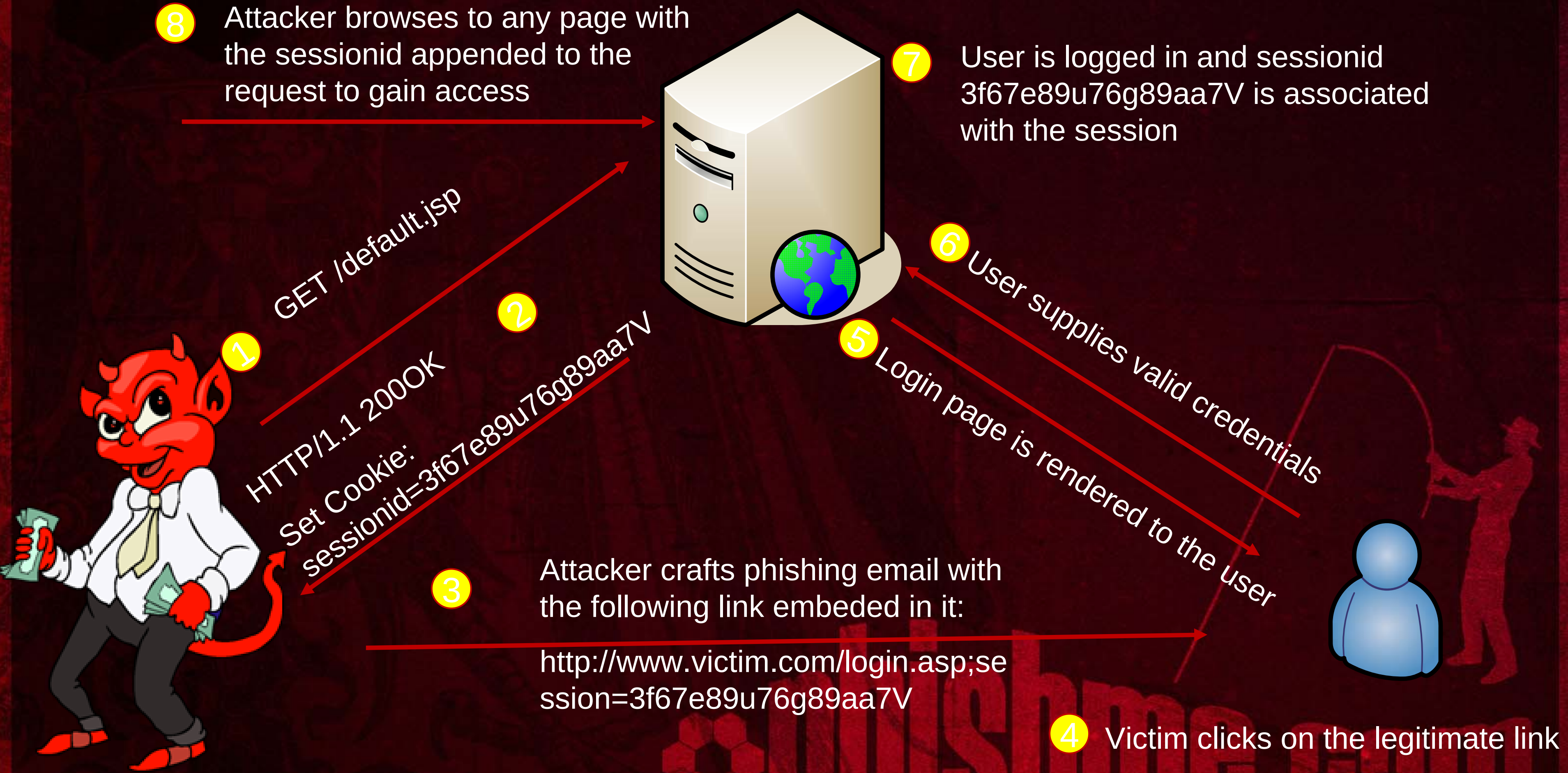
We would appreciate it if you, Mr. , would review the changes by logging into your account by clicking here
and sending us e-mail telling us what you like and what you don't about what you see.

We appreciate your participation in this process.
Thank You once again,

Customer Service

URL: https://www.xyzbrokerage.com/login.asp?sessionid=90198e1525e4b03797f833ff4320af39

Session Fixation



1 GET /default.jsp

2 HTTP/1.1 200OK
Set Cookie:
sessionid=3f67e89u76g89aa7V

3 Attacker crafts phishing email with the following link embeded in it:

http://www.victim.com/login.asp;session=3f67e89u76g89aa7V

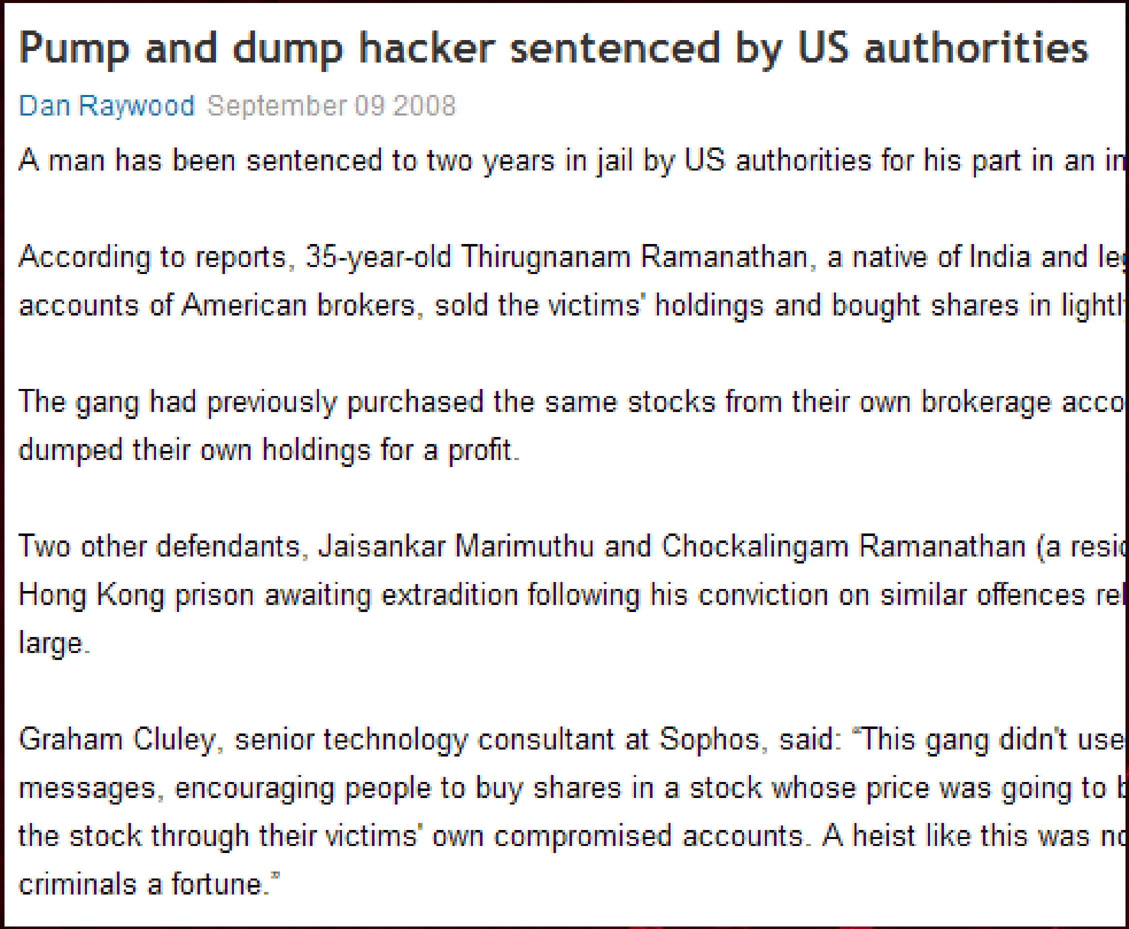
4 Victim clicks on the legitimate link

5 Login page is rendered to the user

6 User supplies valid credentials

7 User is logged in and sessionid 3f67e89u76g89aa7V is associated with the session

8 Attacker browses to any page with the sessionid appended to the request to gain access



Pump and dump hacker sentenced by US authorities

Dan Raywood September 09 2008

A man has been sentenced to two years in jail by US authorities for his part in an in

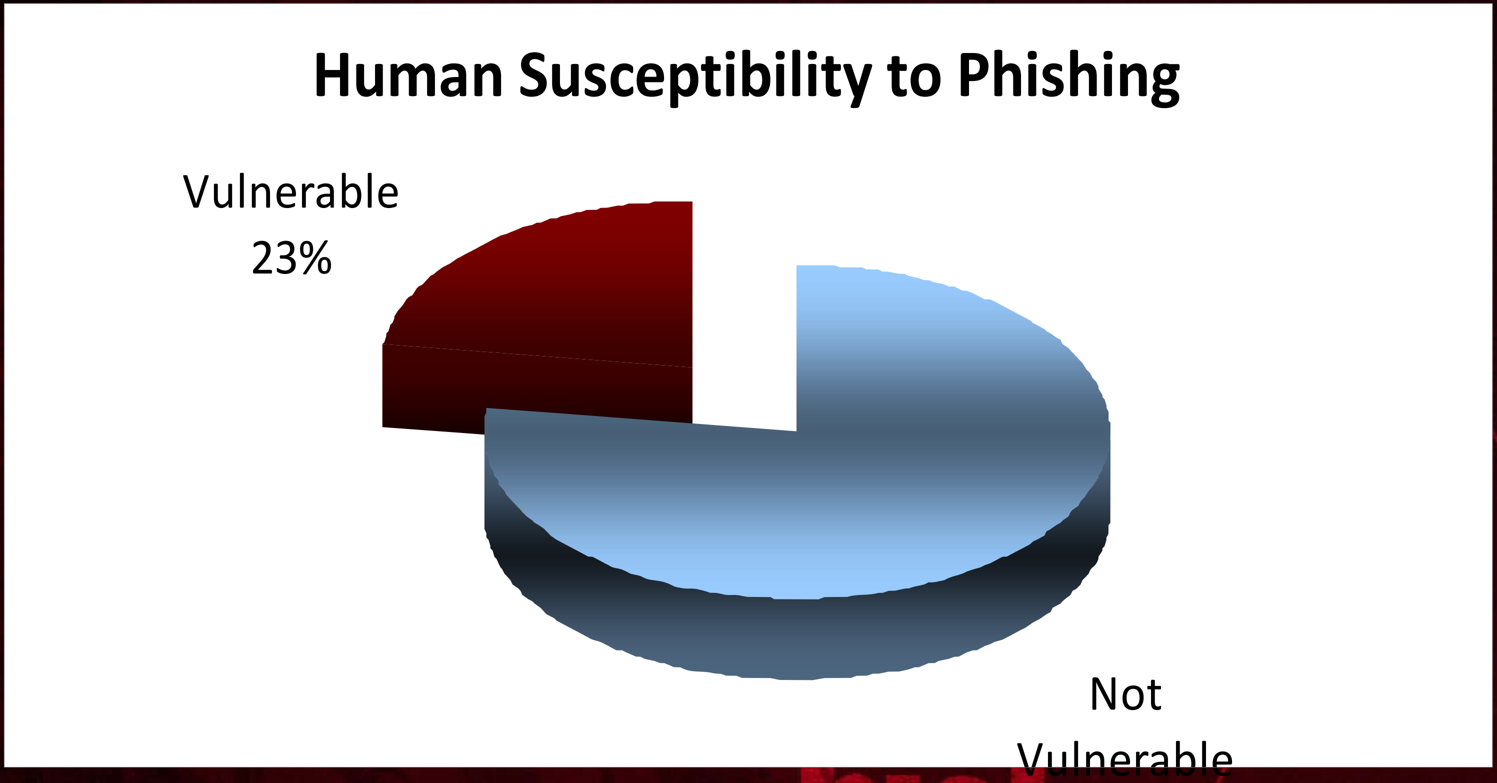
According to reports, 35-year-old Thirugnanam Ramanathan, a native of India and le accounts of American brokers, sold the victims' holdings and bought shares in light

The gang had previously purchased the same stocks from their own brokerage acco dumped their own holdings for a profit.

Two other defendants, Jaisankar Marimuthu and Chockalingam Ramanathan (a resi Hong Kong prison awaiting extradition following his conviction on similar offences rel large.

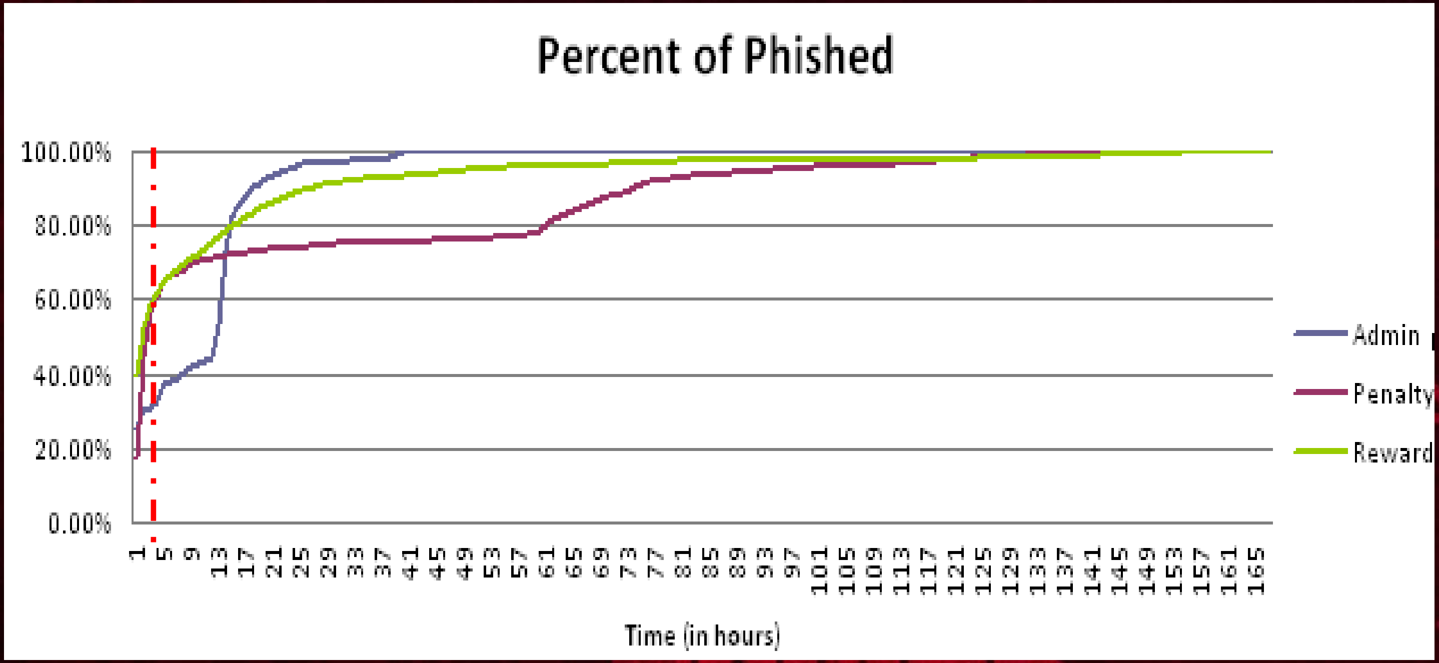
Graham Cluley, senior technology consultant at Sophos, said: "This gang didn't use messages, encouraging people to buy shares in a stock whose price was going to b the stock through their victims' own compromised accounts. A heist like this was no criminals a fortune."

Does It Really Work?



* ± 3% Margin of Error

Do We Have Time To React?

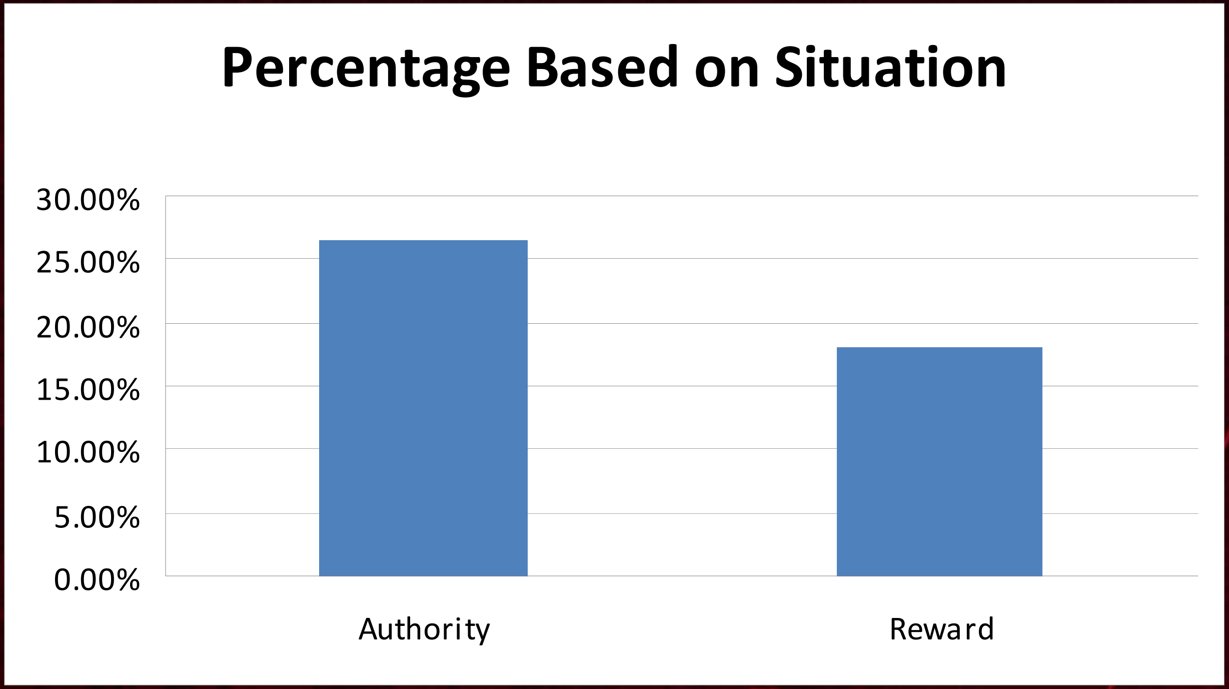


Why Does It Work?

Authority

Reward

Authority V/S Reward



Conclusion

Thank You

Rohyt Belani CISSP, CISM

rohyt.belani@intrepidusgroup.com