

ThinkSECURE  
Security Starts Here

1

Web Habits &  
Hacker-Defence

Christopher Low

OSSA, OSA, CISSP, GSEC, OPST,  
OPSA, CCSE, TCI


2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

ThinkSECURE  
Security Starts Here

2

About Me...

- Chief Technology Officer, ThinkSECURE Pte Ltd.
- More than 10 years of security experience
- Organised various hacking competitions
- Creator of various security tools ( Probemapper, MoocherHunter etc )
- Co-authored the wireless chapter in “Hacking Exposed: Linux 3<sup>rd</sup> Edition”



2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

ThinkSECURE  
Security Starts Here

## About Us...

ThinkSECURE ([www.securitystartshere.org](http://www.securitystartshere.org)) :

- Purely technical org doing practical technical IT-Security Certification & R&D
- Certifying body for accredited technical IT-Security Certifications
- Security services ( Penetration testing , incident response etc)

3

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

ThinkSECURE  
Security Starts Here

## Online Threats

```
graph TD;
    WH(Browser Hijacking) --> WA(Web Attack);
    BA(Browser Attack) --> WA;
    CBA(Cross browser attacks) --> WA;
    WB(Web Botnet) --> WA;
    PW(Phishing websites) --> WA;
    XSS(XSS/CSRF) --> WA;
```

4


2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

Think **SECURE**

## Online Threats

Web  
Attack

Phishing  
websites



Phishing websites

- Attempts to fool the end user
- Put up some fake web site
- Looks like the real thing
- Tricks end user to give away confidential data
- Banks & financial institutions are frequent targets


5
© 2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

Think **SECURE**

## Online Threats

Web  
Attack

XSS  
CSRF



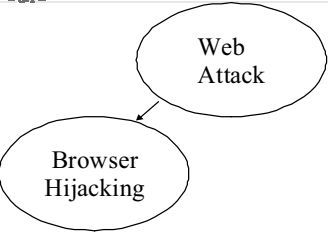
XSS / CSRF

- Attempts to attack the end user
- XSS - reflect scripts from vulnerable sites
- Scripts execute in user's browser
- Potentially steal user's credentials / snoop on user's activities

6
© 2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Online Threats



### Browser Hijacking

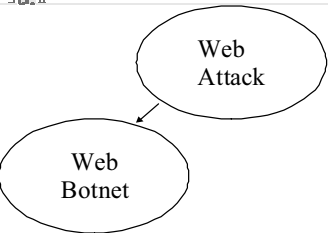
- Attempts to attack the end user
- Replace home page with its own
- In some cases, add bookmarks into browser
- Replace search engines with its own – thus could redirect you to other sites.
- String of popups appear – so fast that you don't have time to close them

7

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Online Threats



### Web Botnet

- Attempts to attack the end user
- “Recruit” vulnerable browsers into collecting information for attacker
- Uses vulnerable websites to spread its net

### Botnet gains, Web 2.0 pains

By Robert Slater  
 Staff Writer - CNN, News.com  
 Published: December 11, 2007, 4:00 AM PST  
[Link](#) [Share](#) [Print](#) [Email](#) [RSS](#) [Facebook](#) [Twitter](#)

While it started out in January 2007 as a traditional computer worm, Storm quickly emerged as a key element toward building one of the largest botnets active on the Internet today.

Subtlety, not violence, is the hallmark of computer worms. Or, at least it should be. Malicious software or attacking large corporations, easily became one of the biggest security stories of years by the time Storm was introduced.

Storm's attack on vulnerable browsers compromised 1.7 million computers. There are even rumors that state-sponsored malicious-software writers had targeted Storm with one of the first cyberwarfare attacks that included the use of botnets.

8

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

ThinkSecure

Security Starts Here

## Online Threats



**Web Attack**

**Cross Browser Attacks**

**Cross Browser Attacks**

- Attempts to attack the end user
- Makes use of vulnerabilities in one browser to attack another browser

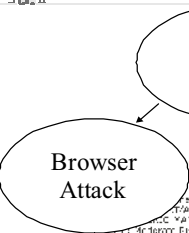


9
© 2008 Christopher Lee. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Lee.

ThinkSecure

Security Starts Here

## Online Threats

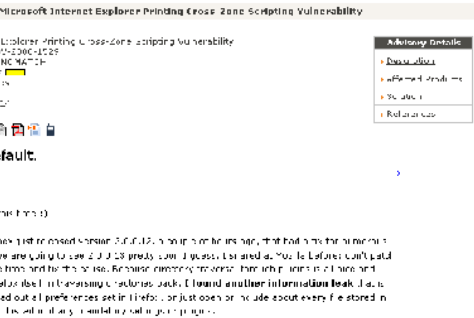


**Web Attack**

**Browser Attack**

**Browser Attack**

- Attempts to attack the end user
- Browser vulnerabilities are discovered on a more regular basis



10
© 2008 Christopher Lee. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Lee.

**ThinkSECURE**  
 Security Starts Here

## Online Threats

Web Attack

What is the common denominator in the above threats ?

The User and his Web Browser

11

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Browser Flavors

Does it really matter which browser you use to surf ?

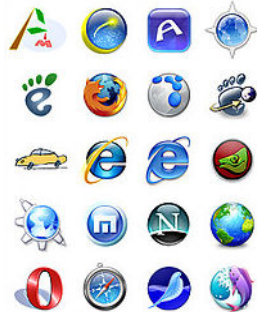
Month	Internet Explorer	Firefox	Safari	Opera	Other
June, 2007	79.12%	14.63%	4.51%	0.53%	0.36%
July, 2007	79.26%	14.45%	4.38%	0.59%	0.39%
August, 2007	79.00%	14.65%	4.71%	0.51%	0.28%
September, 2007	78.27%	14.99%	5.11%	0.51%	0.28%
October, 2007	78.26%	14.94%	5.09%	0.58%	0.25%
November, 2007	77.29%	16.01%	5.14%	0.69%	0.16%
December, 2007	76.04%	16.80%	5.59%	0.64%	0.19%
January, 2008	75.47%	16.98%	5.82%	0.62%	0.18%
February, 2008	74.88%	17.77%	5.70%	0.69%	0.19%
March, 2008	74.60%	17.87%	5.82%	0.69%	0.22%
April, 2008	74.63%	17.76%	5.81%	0.69%	0.19%

Here are more details about current browsers market share. Thanks to HitsLink.

12

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

## Browser Flavors

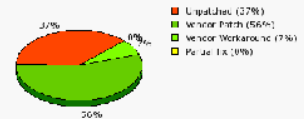


Apparently so ..

- Some applications are written and tested on some flavors of browser
- Some deploy technologies other browser do not natively support (e.g. ActiveX)
- Vulnerabilities are researched and published at different rates by different groups of people
- Some implement a more open architecture, thus encouraging a more vibrant development add-on platform

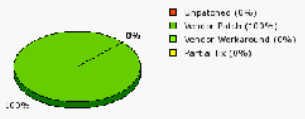
## Browser Flavors

Microsoft Internet Explorer 7.x  
Solution Status (Based on 27 advisories from 2003-2008)



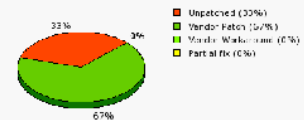
This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

Opera 9.x  
Solution Status (Based on 13 advisories from 2003-2008)



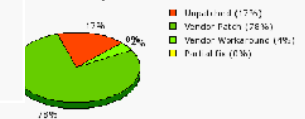
This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

Safari for Windows 3.x  
Solution Status (Based on 3 advisories from 2003-2008)



This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

Firefox 2.0.x  
Solution Status (Based on 23 advisories from 2003-2008)



This graph was generated by Secunia.  
Based on vulnerability information available at <http://secunia.com/>

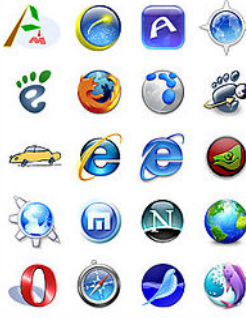
Are they equally vulnerable ?

**ThinkSECURE**  
 Security Starts Here

## Browser Flavors

Browsers each have their own strength ..

Mozilla Firefox – Adopts an open architecture and allows addons / plugins to be written by anyone



Microsoft IE – Deployed with every copy of MS Windows, broad-based deployment and massive support for various web applications

Opera browser - One of the fastest performance browser, with some pretty interesting features in the latest version 9.5 release.

15

2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Browser Flavors

Mozilla Firefox Browser Addons

- Extensive library of addons to extend the various functionalities of the already rich-featured browser
- Addons.mozilla.org contains thousands of addons which one can easily find and install





16

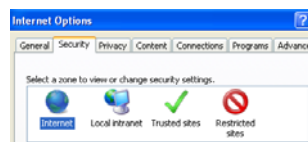
2008 Christopher Low; All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.



## Browser Flavors

### Microsoft's Internet Explorer Security Zoning

- With IE 7.0 today, one can set up security zoning via its interface
- Security zoning effectively segregates the sites you visit into different risk categories, so that IE could render them accordingly
- 4 zones exist : Internet, Local Intranet, Trusted Site, Restricted site



## Browser Flavors

### Microsoft's Internet Explorer Security Zoning


- Trusted Site : Sites where user trusts and would like IE to render with medium security setting
- Restricted Site : Sites where user does not trust and would like IE to render with High security setting
- Local Intranet : Sites determined by IE to be on intranet and would be rendered with medium-low security setting
- Internet : Any site not included in the above category and rendered with medium-high security setting



Think**SECURE**  
Security Starts Here

## Good Browsing Habits

- Different browser
- USB-based browser
- Different machine
- Clearing history
- Applying patches
- Different configuration
- Anti-Virus / Anti-Spyware / Child Protection



19

2008 Christopher Low; All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low

Think**SECURE**  
Security Starts Here

## Good Browsing Habits

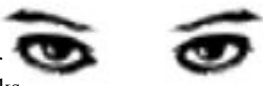
Different browser

- Use a different browser for a different set of tasks

E.g. Use IE for financial transaction, Firefox for casual surfing and Opera for “Social networking sites”

- Why ?

Prevents contamination from one source from compromising all data

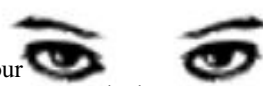


20

2008 Christopher Low; All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low

**ThinkSECURE**  
 Security Starts Here

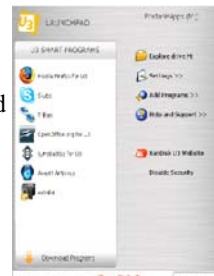
## Good Browsing Habits



USB-based browser

- When you are not at your workstation and needs to access the internet, a USB-based browser is a very good alternative
- E.g.  
 Use a U3 Firefox browser which you can carry with you on a usb-based thumb drive

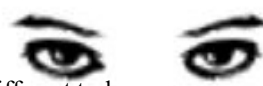
Portableapps.com has sometime equivalent, but does not need special hardware



21
2008 Christopher Low, All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low


**ThinkSECURE**  
 Security Starts Here

## Good Browsing Habits



Different Machine

- Can use physically different machine for different tasks
- Can alternatively install virtual machines e.g. Browsing appliance downloadable and usable with VMWare Server
- <http://www.mojopac.com>

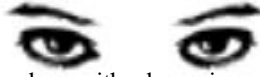


22
2008 Christopher Low, All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low

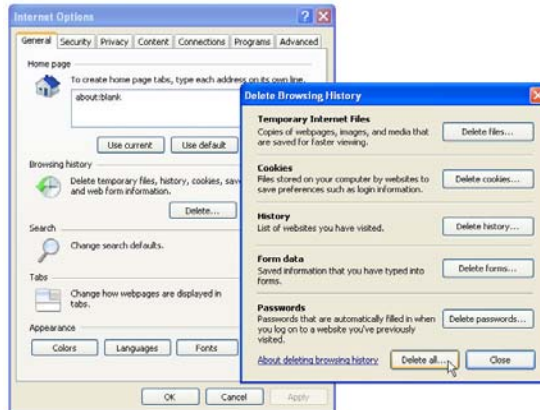
## Good Browsing Habits

### Clearing History

- Always clear your surfing traces after you're done with a browsing session
- Session information can contain important information about you
- In IE 7.0, you can clear it via “Delete Browsing History”



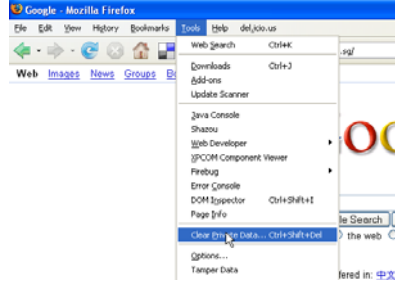
## Good Browsing Habits



## Good Browsing Habits

### Clearing History

- In Firefox, you can also clear your surfing traces via “Clear Private Data” menu item



## Good Browsing Habits

### Applying patches

- Need to constantly apply patches to your browser and every plugin / addon that you have added to your browser
- Applying patches to browser is usually automatically done
- Applying patches to addons / plugin might not  
E.g. Flash plugin



## Good Browsing Habits



Checking the version of flash in firefox

## Good Browsing Habits




Installing the most up to date flash plugin

Think **SECURE**

Security Starts Here

## Good Browsing Habits



Checking the version of flash in IE, they're not the same

29
© 2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.


Think **SECURE**

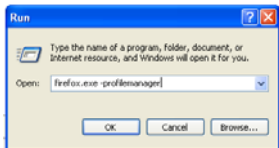
Security Starts Here

## Good Browsing Habits

Different Configuration

- You can setup different profiles for different users on the same system / for different tasks you do
- Firefox allows you to create profiles and you decide which profile you need when you start Firefox up everytime






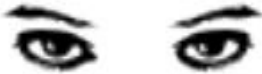
Activate the profile manager

30
© 2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

Think**SECURE**  
Security Starts Here

## Good Browsing Habits

### Different Configuration



Create individual profile



31

2008 Christopher Low: All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low

Think**SECURE**  
Security Starts Here

## Good Browsing Habits

### Different Configuration



Whenever you start Firefox, it will prompt you for the profile to use

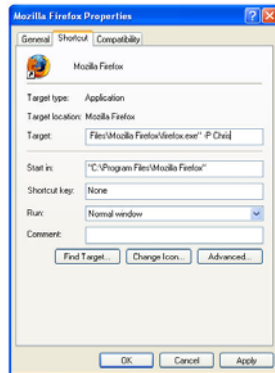
32

2008 Christopher Low: All Rights Reserved; No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low



## Good Browsing Habits

### Different Configuration



You can change the property of your firefox instance and have it start up different profiles for each icon.

## Good Browsing Habits

### Anti-Virus / Anti-Spyware / Child Protection

- Use common sense when deciding on what to download and install
- Tools could help – but no match for plain old common sense



## Browsing Locations

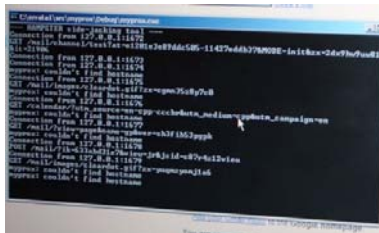
Where we browse from is also very important



Defcon Wall of sheep

## Browsing Locations

Wireless media – why is it dangerous ?



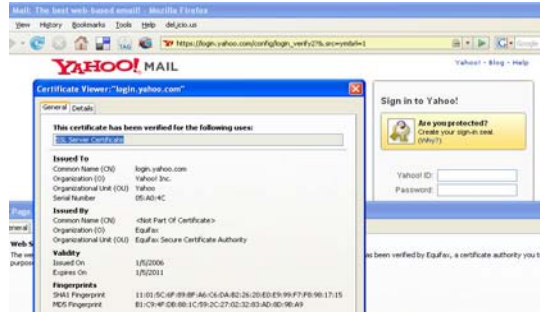
Hamster & Ferret stealing and replaying web session information

- Public hotspot w/o encryption
- Home wireless connection and have not setup encryption
- Data that you send / receive is as good as shouting over the air
- Emails could be read, web session hijacked passwords seen etc

## Browsing Locations

What precautionary measures to take ?

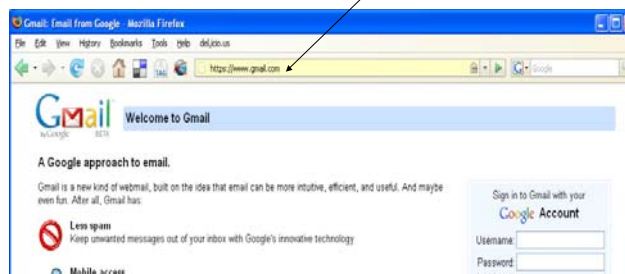
- Use some kind of application level encryption  
e.g SSL, Secure POP / SMTP



## Browsing Locations

What precautionary measures to take ?

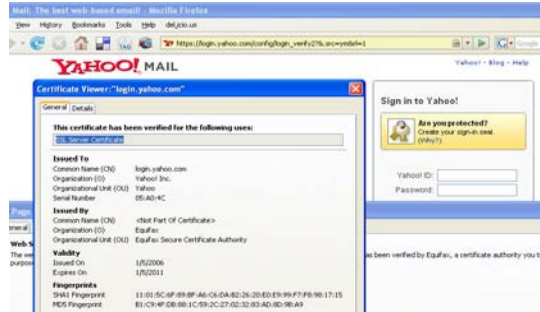
- Some web-based email provider provides for a SSL alternative



## Browsing Locations

What precautionary measures to take ?

- Use some kind of application level encryption  
e.g SSL, Secure POP / SMTP



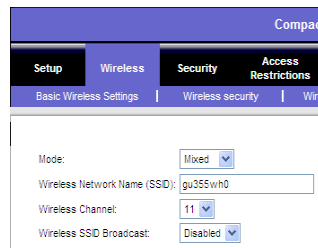
## Browsing Locations

What precautionary measures to take ?

- If you control the wireless AP, setup encryption on it

OPEN  
WEP  
WPA/PSK  
WPA Enterprise

- Change SSID to something unique
- Disable broadcast of SSID



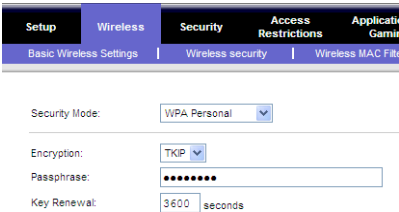
**Think SECURE**  
 Security Starts Here

## Browsing Locations

---

What precautionary measures to take ?

- How to setup WPA/PSK ?



- What passphrase to use ?

41
2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.


**Think SECURE**  
 Security Starts Here

## Browsing Locations

---

What precautionary measures to take ?

- What passphrase to use ?



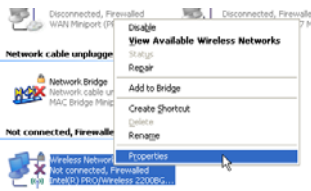
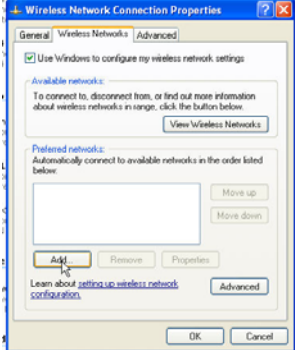
42
2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Browsing Locations

What precautionary measures to take ?

- How to configure your wireless client ?


43
2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

**ThinkSECURE**  
 Security Starts Here

## Browsing Locations

What precautionary measures to take ?

- How to configure your wireless client ?



44
2008 Christopher Low. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Low.

## Browsing Locations

Use someone else's computer  
(a.k.a Use a machine / browser that you do not have control over)

- Machine could be “bugged”  
(software or hardware based sniffing tool)
- Browser could be “bugged”  
(Demo)

Prevention

- Don't do it if you can help it
- Bring your own browser (USB-based)
- Use application level encryption (e.g. SSL)



## Demo

**Beware of Error Messages At Bank Sites - Security Fix - Mozilla Firefox**

File Edit View History Bookmarks Tools Help del.icio.us

http://blog.washingtonpost.com/securityfix/2008/06/beware\_of

**SECURITY FIX**  
Brian Krebs on Computer Security

About This Blog | Archives | RSS Feed | What's RSSD

**Beware of Error Messages At Bank Sites**

If you own or work at a small to mid-sized business, and are presented with an error message about data synchronization or site maintenance when trying to access your company's bank account online, you might want to give the bank a call. A criminal group that specializes in deploying malicious software to steal banking data is presenting victims with fake maintenance pages and error messages as a means of getting around anti-fraud safeguards erected by many banks.

Dozens of banks now require business customers to log in to their accounts online using so-called [two-factor authentication](#) methods, which generally require the customer to enter something in addition to a user name and password, such as a random, one-time-use numeric code generated by a key fob or a scratch-off pad.

But one of this past year's most prolific cyber gangs -- which targets virus-laden e-mail attacks against specific individuals at small to mid-sized businesses -- has devised a simple but ingenious method of circumventing these security measures. When a victim whose

**RELATED LINKS**

- The Archivers
- Security Fix Live! Web Chats
- About This Blog
- Password Primer

**RECENT POSTS**

- Anonymous Domains
- Calvin A. Spurgeon's Delight
- Data Loss: The Ultimate Checklist
- Opera 9.5 Offers Anti-Malware Protection
- Malware Silently Alters Wireless Router Settings
- Microsoft, Apple Issue Security Updates

**Stories by Category**

- Cyber Justice
- Fraud
- From the Banker
- Latest Warnings
- Blog
- News Patches
- Privacy
- Safety Tips
- U.S. Government

**Stories by Date**

- Full Story Archive

**Thank you for your submission.**

Please allow 15 to 30 minutes for your request to be synchronized with our server. You will be able to login after the request is synchronized.

Multifactor authentication will only be required for the pre-selected functions.

## Demo

According to researchers at iDefense, this tactic was most recently used in an attack nearly two weeks ago, in which the fraudsters sent thousands of targeted e-mails [spoofing the United States Tax Court](#). The messages included each recipient's name and employer, and were designed to look like a petition from the Tax Court in a case that lists the recipient's name as the respondent in a case versus the Commission of Internal Revenue.



The message prompts the recipient to click on a link to view the complaint. Those who do so are greeted with a prompt to install an Adobe Acrobat viewer. Of course, the program isn't a viewer at all, but a "browser helper object" (BHO) that allows the attacker to steal passwords and data when victims log on to encrypted ([https://](#)) Web sites.

More importantly, the BHO lets the attackers modify Web pages that the victim sees in real time. As a result, when victims are presented with one of these error pages, the message is inserted into the body of the bank's actual Web page. In such an attack, even an alert victim is unlikely to notice anything amiss: The URL in the address field of the victim's browser will still show the bank's real Web site address, the rest of the content on the page will look the same, and the little lock icon will remain visible in the browser.

## Demo

Matt Richard, director of rapid response at iDefense, said the criminal group responsible for this and a string of other such targeted attacks use the fake scam message for customers of roughly 50 different financial institutions that deploy two-factor authentication for business customers.

"I have this conversation a lot with security people, and banks in particular," Richard said. [If a bad guy has malicious code on a customer's machine, no matter what you do, he's going to have some way to get in to the customer's account.](#) The best you'll be able to do is try to stop the money transfers."

The slick aspect of this attack is that if the victim tries to log in to his or her account immediately after receiving the bogus message, the attackers go ahead and permit the login. "They've already got the victim's credentials at that point, and they don't want to do anything that's going to prompt the victim to pick up the phone and call their bank," Richard said.

iDefense estimates this latest scam was sent to around 6,000 to 8,000 targets, and the company has evidence that at least 690 people fell victim to the scam. A 10 percent success rate is about average for these types of targeted attacks. Security Fix has written about the take from these attacks before, including one that spoofed the Better Business Bureau and netted the fraudsters more than \$188,000 from a single victim.



Think**SECURE**  
Security Starts Here

## Demo

---

Demo

Using a browser you don't have control over

49

2008 Christopher Love. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Love.

Think**SECURE**  
Security Starts Here

## Q&A

---

Any Questions ?

50

2008 Christopher Love. All Rights Reserved. No copying, storage, transmission or reproduction allowed without the express, written consent of Christopher Love.

Thank You !

Sign up for our free newsletter  
@ <http://doyouthinksecure.securitystartshere.org>