A Presentation on Computer Security

For the

Danbury Area Computer Society

By

Frank Kunst and Chris Milmerstadt

Survey

- PC Users
- MAC Users
- Business Owners
- Online Banking Users
- Social Networking Users

Topics

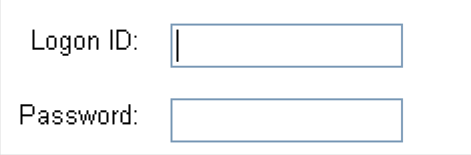
- Security Methods
- Web Activity/Email
- Social Networking Sites
- Wireless Networking
- Encryption

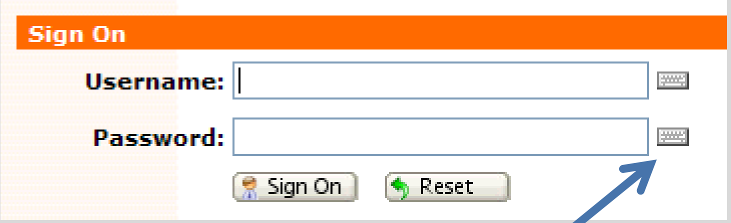
Topics (cont’d)

- Online Banking Account Hijacking
- Macs and Mobile
- Software Tools for Security
- Payments and Protections
- Questions

Evolution of Security Methods

- User Name and Passwords
  - Simplest of authentication methods
  - Susceptible to brute force attack and/or guessing
  - Strength limited by system configuration and ability to support complexity

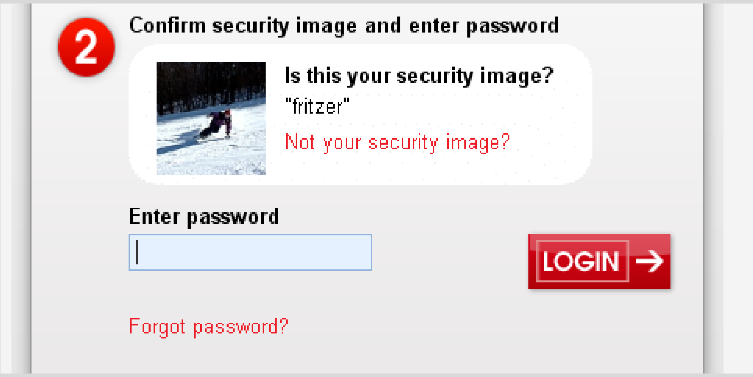




Virtual Keyboard

Evolution of Security Methods

- Site Authentication
  - User selected images and/or passphrase associated with credentials
- Multi-Factor Authentication
  - Adds “What you have” ie Tokens
  - Advanced malware can intercept and defeat

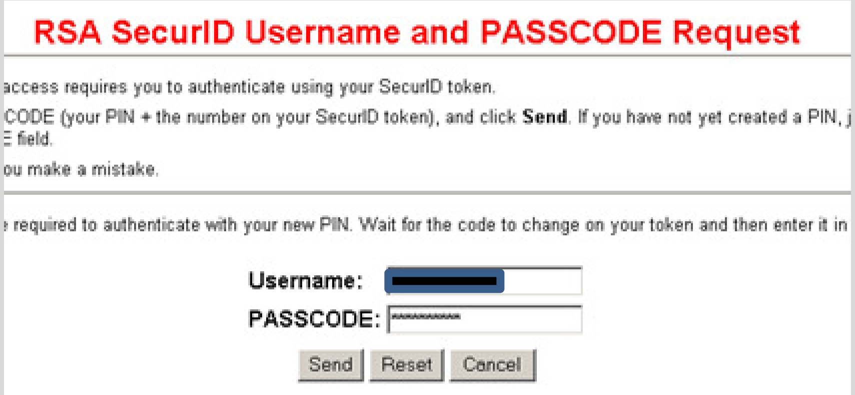


2 Confirm security image and enter password

Is this your security image?

"fritzer"

Enter password



RSA SecurID Username and PASSCODE Request

access requires you to authenticate using your SecurID token.

CODE (your PIN + the number on your SecurID token), and click **Send**. If you have not yet created a PIN, j

E field.

ou make a mistake.

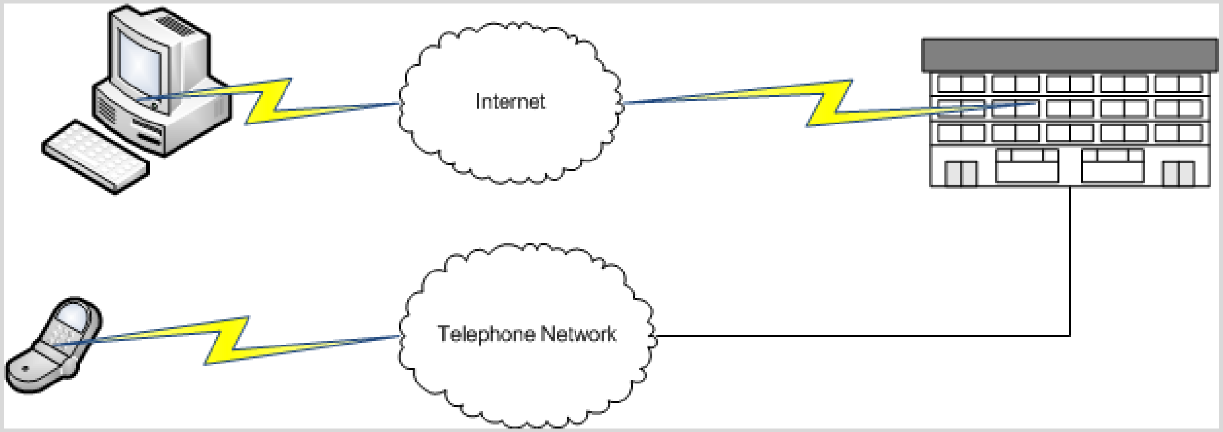
required to authenticate with your new PIN. Wait for the code to change on your token and then enter it in

Username: [redacted]

PASSCODE: **********

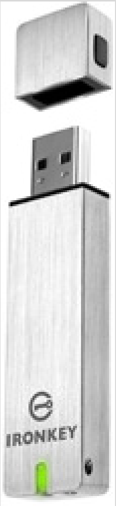
Evolution of Security Methods

- Out of Band Authentication
- Use separate medium to authenticate user

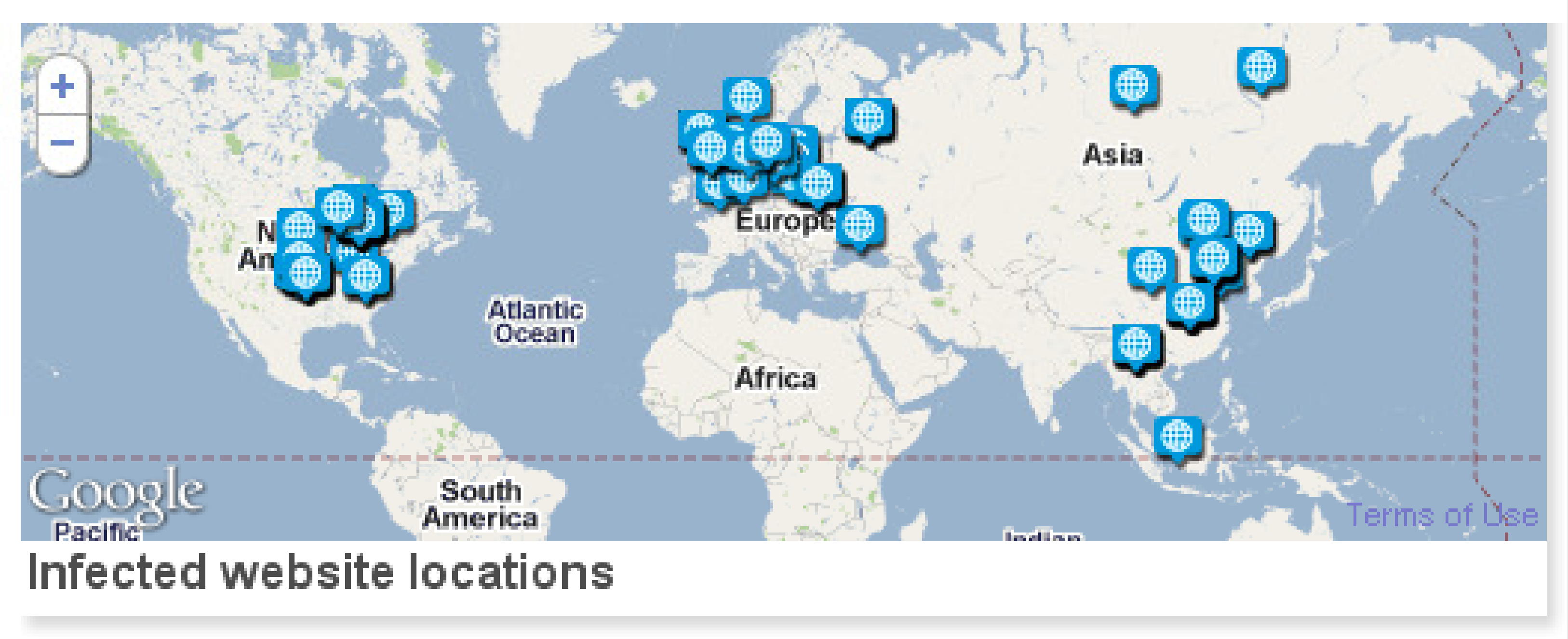


Evolution of Security Methods

- Hardened Portable Virtual Environment
  - Operating System
  - Browser
  - Access only to Approved Websites



Web Activity

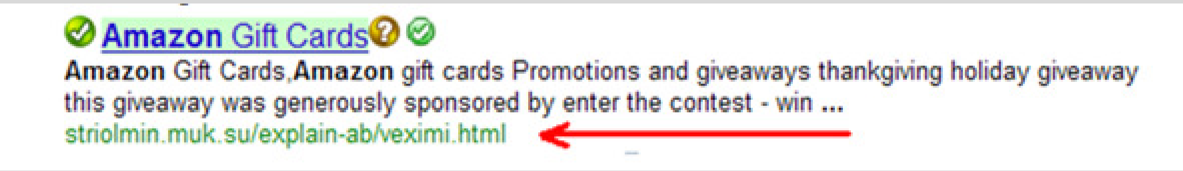


Infected website locations

Sophos Web Threats Dashboard – 6/7/2011

Web Activity

- Search Results to bogus sites
- Indiscriminant searching



✓ Amazon Gift Cards ? ✓

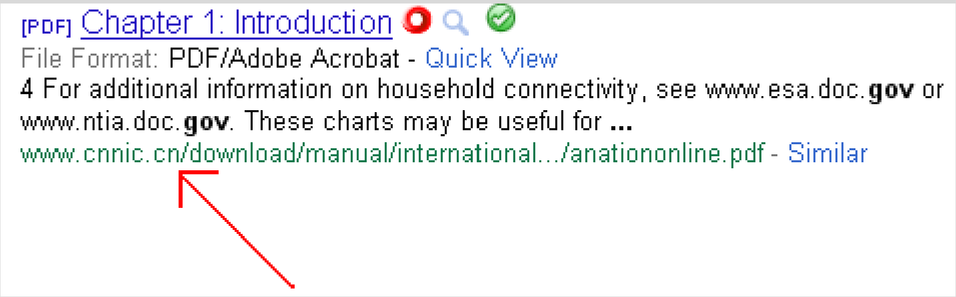
Amazon Gift Cards,**Amazon** gift cards Promotions and giveaways thankgiving holiday giveaway this giveaway was generously sponsored by enter the contest - win ...

striolmin.muk.su/explain-ab/veximi.html

- Visiting compromised or bogus sites leads to downloads to further compromise

Web Activity

- Determining where you are actually going



[PDF] Chapter 1: Introduction

File Format: PDF/Adobe Acrobat - Quick View

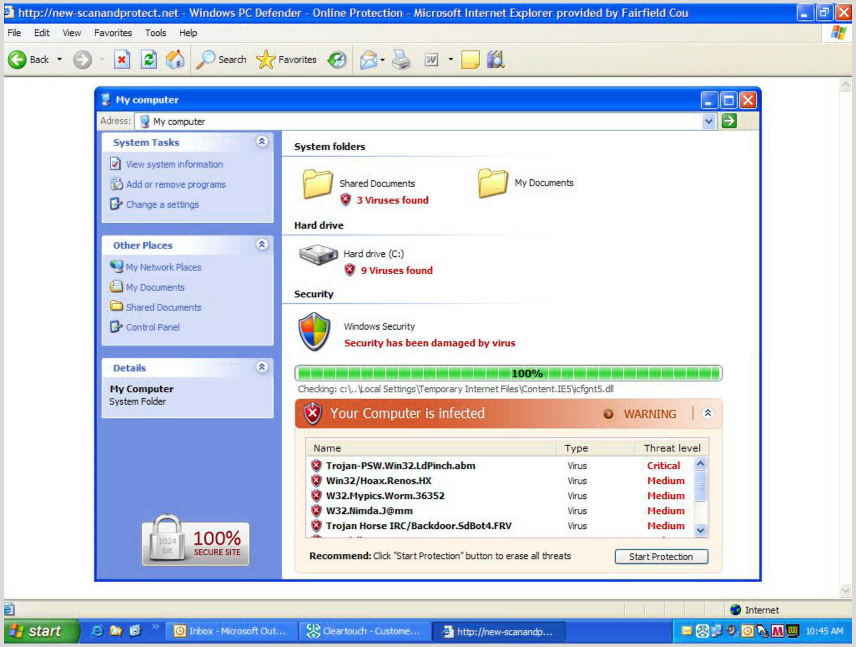
4 For additional information on household connectivity, see www.esa.doc.**gov** or www.ntia.doc.**gov**. These charts may be useful for **...**

www.cnnic.cn/download/manual/international.../anationonline.pdf - Similar

- The domain immediately to the *left* of the first single-slash is your real destination

Web Activity

- **Pop-ups**
  - **Appear to be from anti-virus software**
  - **Click thru leads to download of malicious software**



System folders

Shared Documents
3 Viruses found

My Documents

Hard drive

Hard drive (C:)
9 Viruses found

Security

Windows Security
Security has been damaged by virus

100%

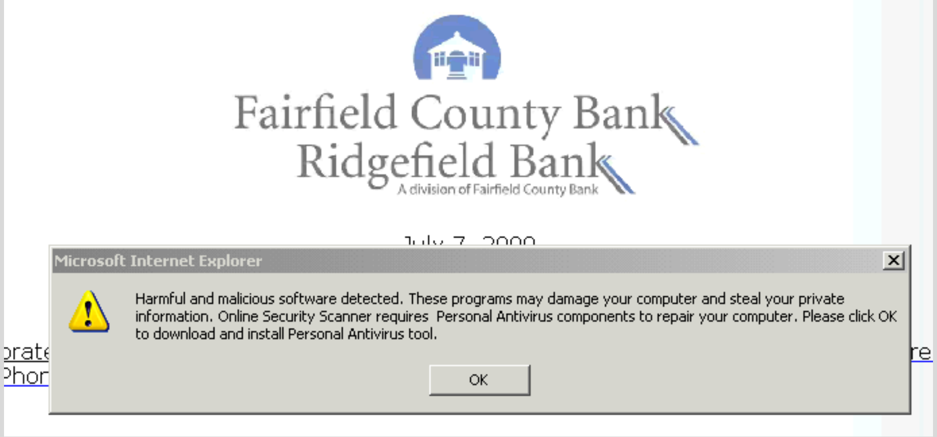
Checking: c:\..\Local Settings\Temporary Internet Files\Content.IE5\jcfgnt5.dll

Your Computer is infected — WARNING

Name	Type	Threat level
Trojan-PSW.Win32.LdPinch.abm	Virus	Critical
Win32/Hoax.Renos.HX	Virus	Medium
W32.Mypics.Worm.36352	Virus	Medium
W32.Nimda.J@mm	Virus	Medium
Trojan Horse IRC/Backdoor.SdBot4.FRV	Virus	Medium

Recommend: Click "Start Protection" button to erase all threats

Start Protection



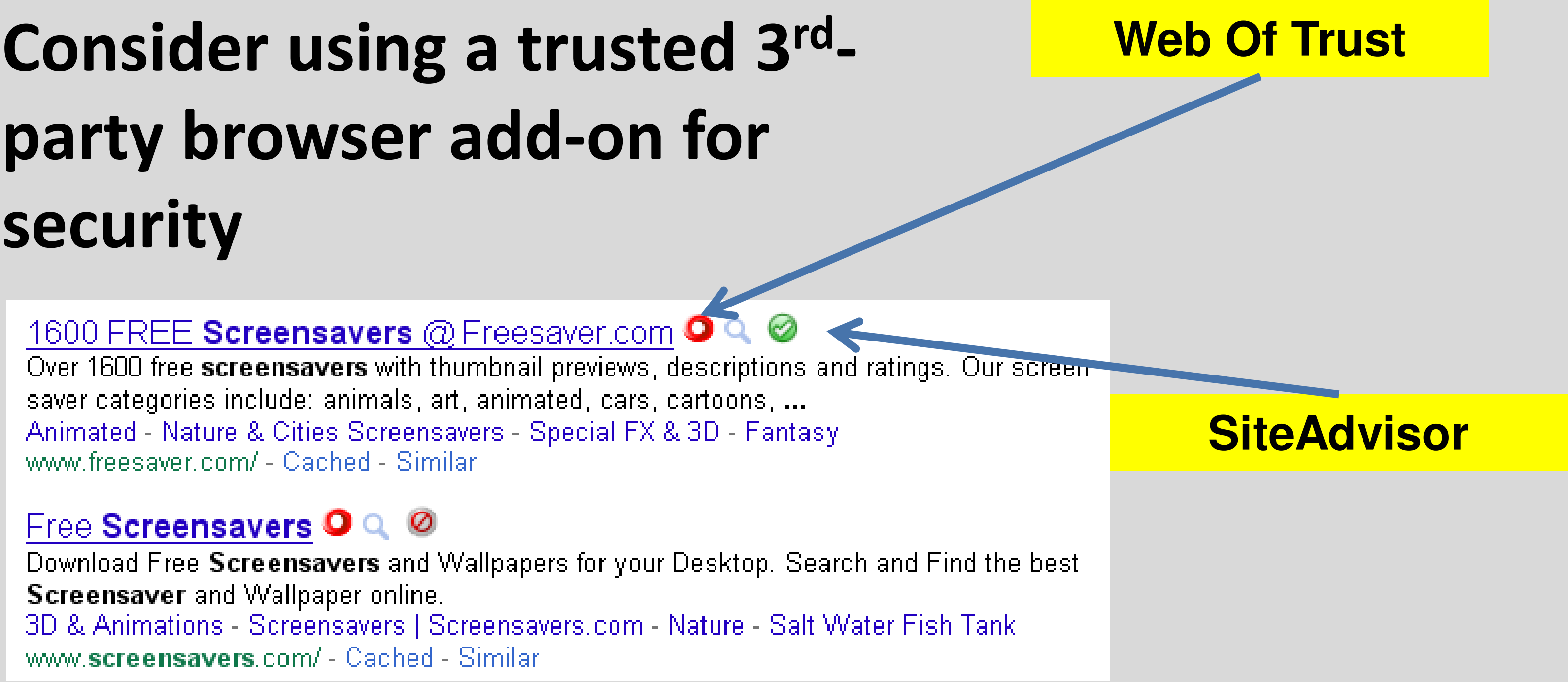
Microsoft Internet Explorer

Harmful and malicious software detected. These programs may damage your computer and steal your private information. Online Security Scanner requires Personal Antivirus components to repair your computer. Please click OK to download and install Personal Antivirus tool.

OK

Web Activity

- Use your search engines search field instead of typing your address in the browser ‘address’ field
- Consider using a trusted 3rd-party browser add-on for security



Web Of Trust

SiteAdvisor

1600 FREE **Screensavers** @ Freesaver.com

Over 1600 free **screensavers** with thumbnail previews, descriptions and ratings. Our screen saver categories include: animals, art, animated, cars, cartoons, **...**

Animated - Nature & Cities Screensavers - Special FX & 3D - Fantasy

www.freesaver.com/ - Cached - Similar

Free **Screensavers**

Download Free **Screensavers** and Wallpapers for your Desktop. Search and Find the best **Screensaver** and Wallpaper online.

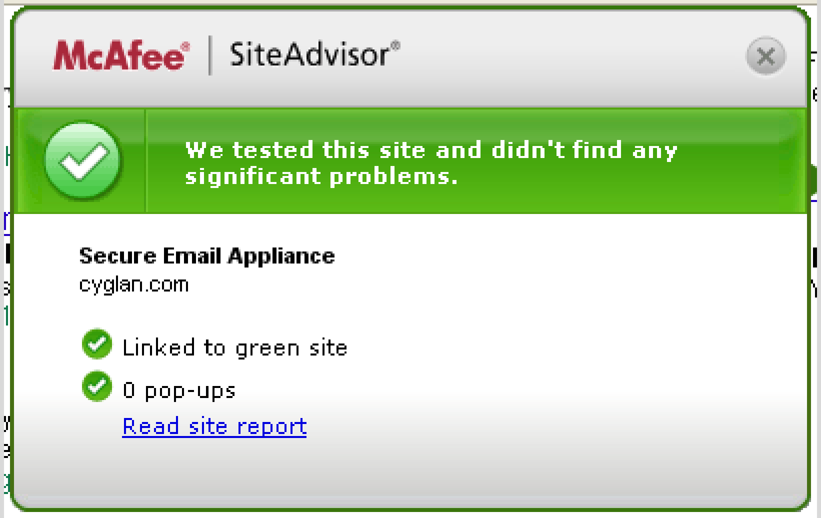
3D & Animations - Screensavers | Screensavers.com - Nature - Salt Water Fish Tank

www.**screensavers**.com/ - Cached - Similar

Web Activity

WOT®

Community-powered tools that boost trust on the web.



McAfee® | SiteAdvisor®

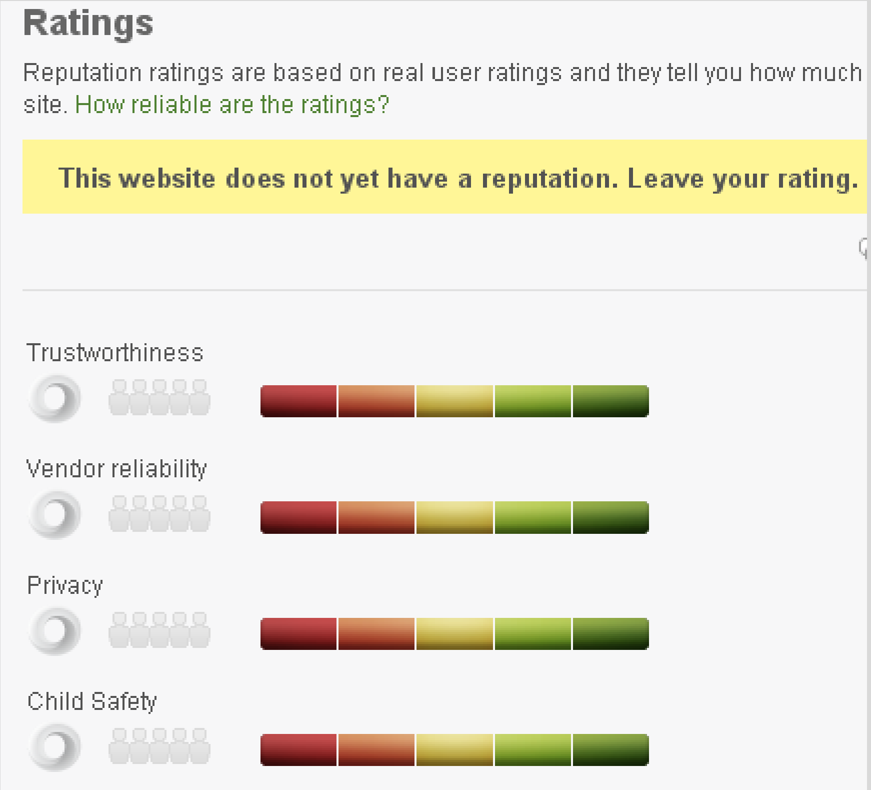
We tested this site and didn't find any significant problems.

Secure Email Appliance
cyglan.com

✓ Linked to green site

✓ 0 pop-ups

Read site report



Ratings

Reputation ratings are based on real user ratings and they tell you how much site. How reliable are the ratings?

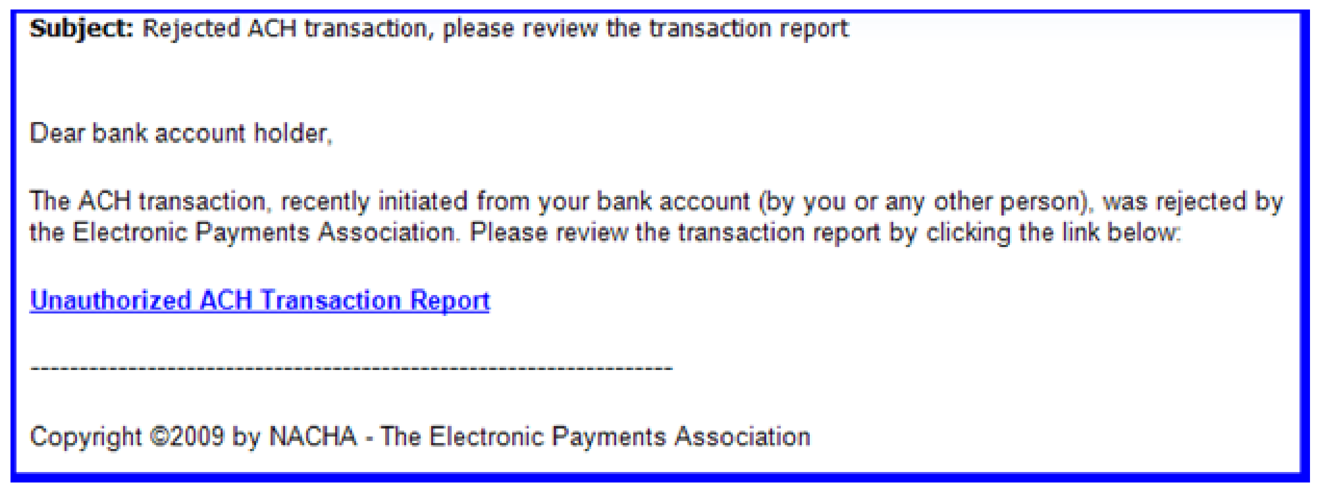
This website does not yet have a reputation. Leave your rating.

Phishing

- Typically an official-looking e-mail is sent to potential victims pretending to be from their ISP, retail store, bank, freight carriers, etc.
- Embedded links direct user to malicious website to collect personal information or deliver payload

Phishing

- **Phishing emails are more convincing than ever (the old tell-tale signs are quickly becoming a thing of the past: impertinent emails, poor spelling, malicious attachments…)**



Subject: Rejected ACH transaction, please review the transaction report

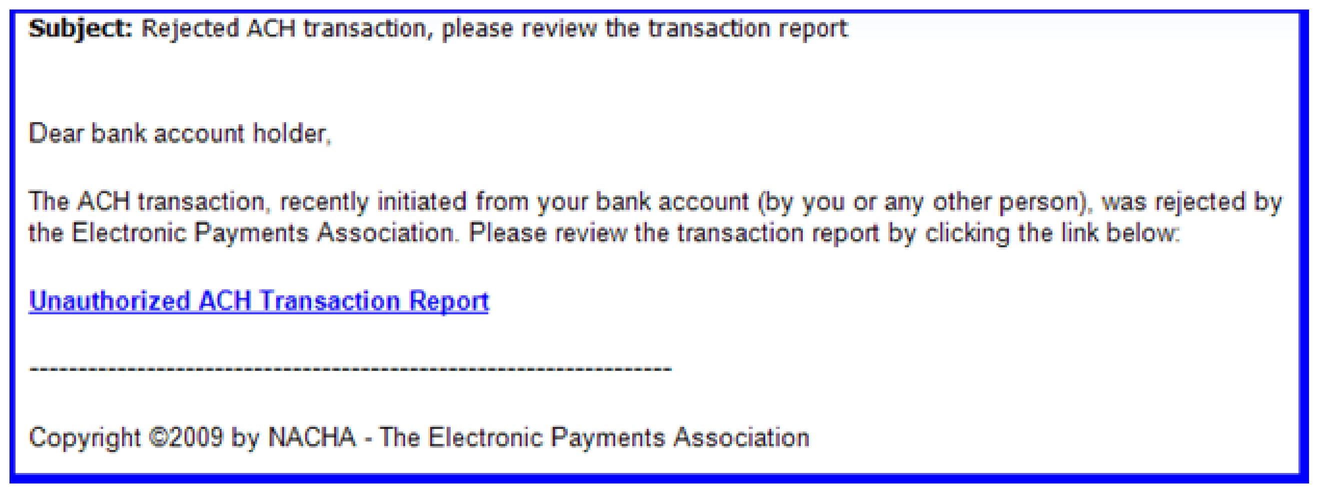
Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any other person), was rejected by the Electronic Payments Association. Please review the transaction report by clicking the link below:

Unauthorized ACH Transaction Report

Copyright ©2009 by NACHA - The Electronic Payments Association

Phishing



Subject: Rejected ACH transaction, please review the transaction report

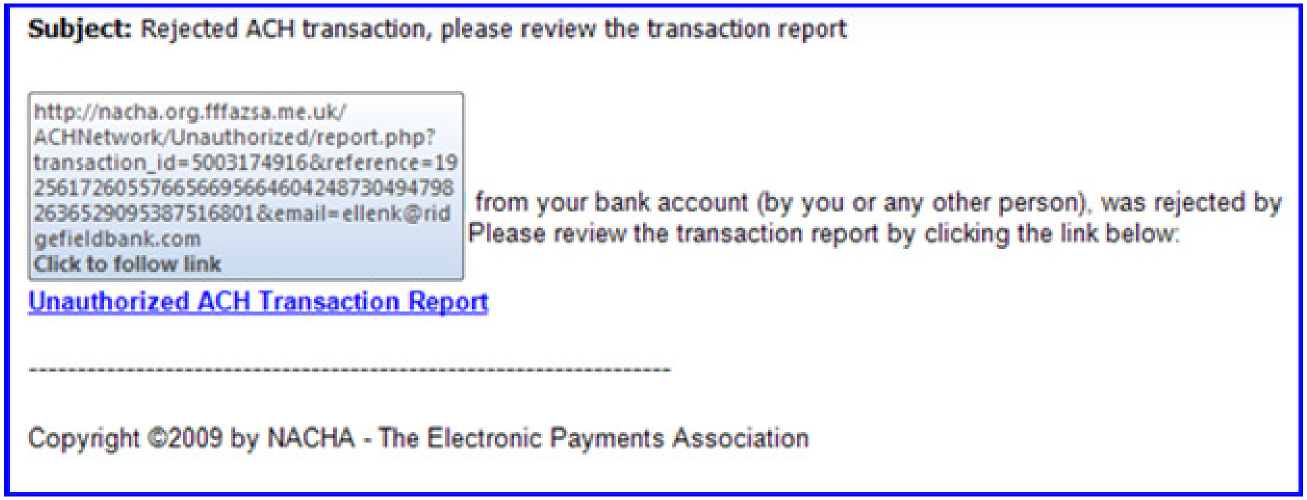
Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any other person), was rejected by the Electronic Payments Association. Please review the transaction report by clicking the link below:

Unauthorized ACH Transaction Report

Copyright ©2009 by NACHA - The Electronic Payments Association

Hover the mouse over the link to reveal the destination



Subject: Rejected ACH transaction, please review the transaction report

http://nacha.org.fffazsa.me.uk/ACHNetwork/Unauthorized/report.php?transaction_id=5003174916&reference=192561726055766566956646042487304947982636529095387516801&email=ellenk@ridgefieldbank.com
Click to follow link

from your bank account (by you or any other person), was rejected by
Please review the transaction report by clicking the link below:

Unauthorized ACH Transaction Report

Copyright ©2009 by NACHA - The Electronic Payments Association

Phishing

Reducing the chances of being tricked

- **Is the arrival of the email expected?**
  - **Unsolicited vs. anticipated communication?**
    - **“Connecting-the-dots” (are you your own “worst enemy” when it comes to security)**

Web Based E-mail

- Offers convenient “access anywhere”
- Often a vector of malware through pop-ups, advertising and scams
- Potential to compromise corporate security environment

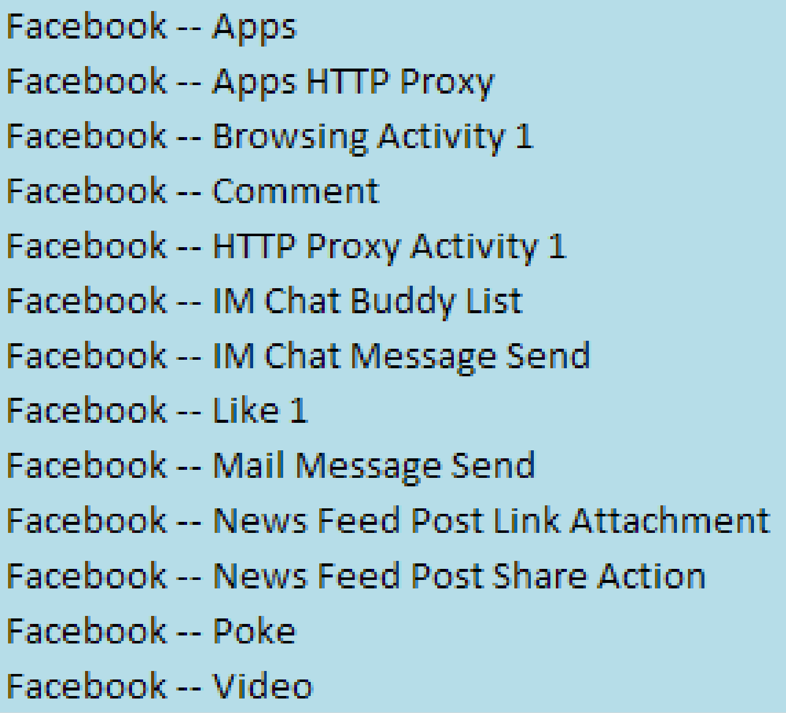
YAHOO! MAIL

Windows Live™ Hotmail

Gmail™ by Google

Social Networking

- Social Networking – not just your garden-variety web traffic
- Facebook, and similar sites, employ “Applications” that can pose serious security risks
- Should these sites be successfully blocked? Can they be allowed in a controlled manner?

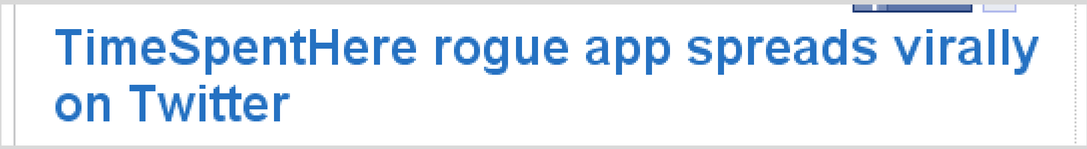


Facebook -- Apps
Facebook -- Apps HTTP Proxy
Facebook -- Browsing Activity 1
Facebook -- Comment
Facebook -- HTTP Proxy Activity 1
Facebook -- IM Chat Buddy List
Facebook -- IM Chat Message Send
Facebook -- Like 1
Facebook -- Mail Message Send
Facebook -- News Feed Post Link Attachment
Facebook -- News Feed Post Share Action
Facebook -- Poke
Facebook -- Video

Social Networking

Free Tube Hub hot sexy girls links spread virally on Facebook

Rihanna and Hayden Panettiere sex video spreads Mac malware on Facebook



TimeSpentHere rogue app spreads virally on Twitter

IMF boss rape video? Mac malware spreads via Facebook links

World funniest condom commercial? Facebook hit by viral likejacking attack

Wireless Networking

- ***Private Wi-Fi needs to be secured***
  - ***Change the default administration password immediately***
  - ***Implement a Service Set Identifier (Network name) and a strong network access code***
  - ***Use WPA2 encryption***
  - ***Consider MAC address filtering***

Wireless Networking

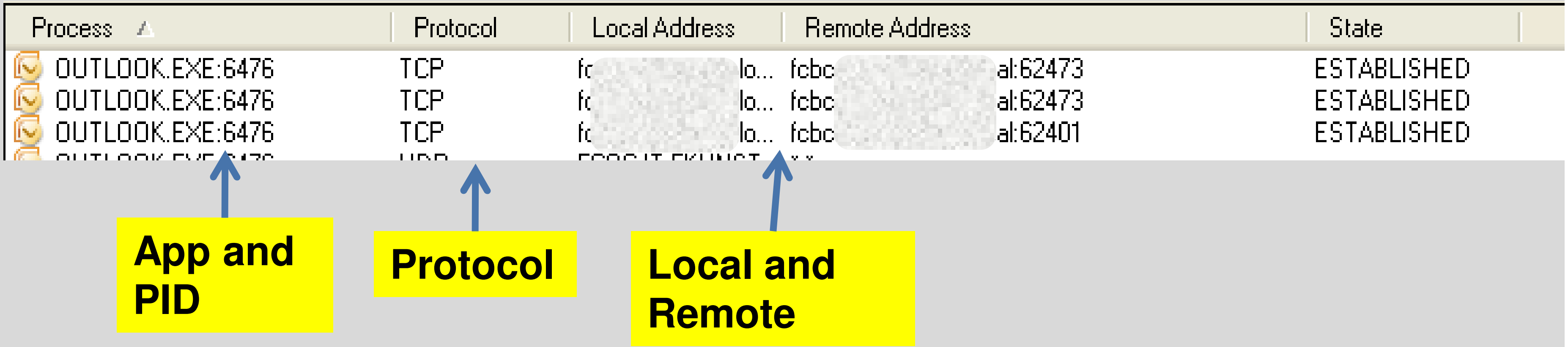
- ***Public Wi-Fi Tips***
  - ***Use HTTPS***
    - ***HTTP sessions can be captured***
  - ***Enable Firewall***
  - ***Disable File Sharing***
  - ***Do not use for sensitive transactions***
  - ***Consider use of a VPN***

Encryption

- ***Data Encryption***
  - ***Laptops***
  - ***Sensitive data***
    - ***Credit cards for payment***
    - ***Credit Applications***
    - ***Personally identifiable information***

Who’s Talking?

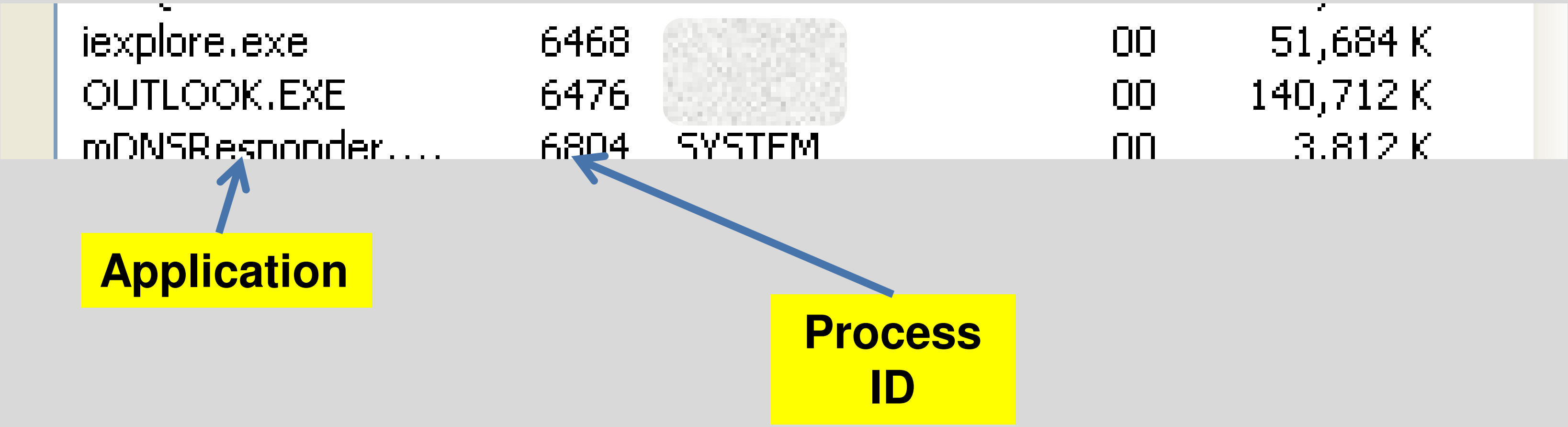
- ***Applications and Processes are constantly communicating***
- ***TCPView displays the processes, protocols, source and destination***



Process	Protocol	Local Address	Remote Address	State
OUTLOOK.EXE:6476	TCP	fc[redacted]lo...	fcbc[redacted]al:62473	ESTABLISHED
OUTLOOK.EXE:6476	TCP	fc[redacted]lo...	fcbc[redacted]al:62473	ESTABLISHED
OUTLOOK.EXE:6476	TCP	fc[redacted]lo...	fcbc[redacted]al:62401	ESTABLISHED

Who’s Talking?

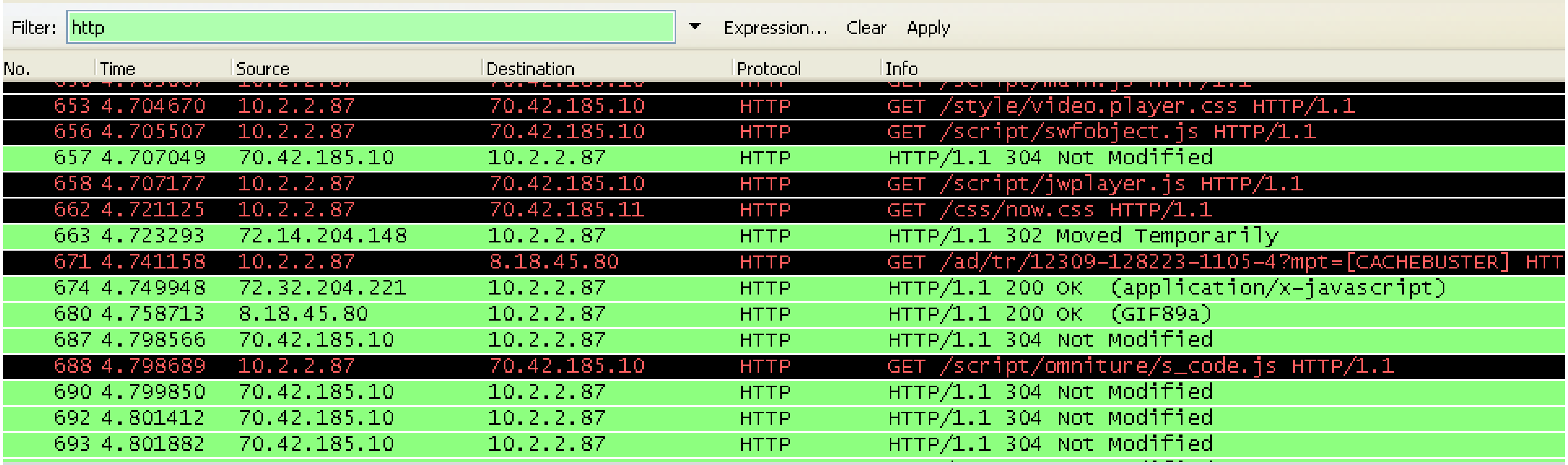
- ***Task Manager displays the processes and applications***



```
iexplore.exe        6468   [redacted]        00     51,684 K
OUTLOOK.EXE         6476                     00    140,712 K
mDNSResponder....   6804   SYSTEM            00      3,812 K
```

Who’s Talking to Whom?

- ***Wire Shark is a packet capture and analysis tool***



```
No.     Time      Source          Destination     Protocol  Info
653 4.704670  10.2.2.87       70.42.185.10    HTTP      GET /style/video.player.css HTTP/1.1
656 4.705507  10.2.2.87       70.42.185.10    HTTP      GET /script/swfobject.js HTTP/1.1
657 4.707049  70.42.185.10    10.2.2.87       HTTP      HTTP/1.1 304 Not Modified
658 4.707177  10.2.2.87       70.42.185.10    HTTP      GET /script/jwplayer.js HTTP/1.1
662 4.721125  10.2.2.87       70.42.185.11    HTTP      GET /css/now.css HTTP/1.1
663 4.723293  72.14.204.148   10.2.2.87       HTTP      HTTP/1.1 302 Moved Temporarily
671 4.741158  10.2.2.87       8.18.45.80      HTTP      GET /ad/tr/12309-128223-1105-4?mpt=[CACHEBUSTER] HTT
674 4.749948  72.32.204.221   10.2.2.87       HTTP      HTTP/1.1 200 OK  (application/x-javascript)
680 4.758713  8.18.45.80      10.2.2.87       HTTP      HTTP/1.1 200 OK  (GIF89a)
687 4.798566  70.42.185.10    10.2.2.87       HTTP      HTTP/1.1 304 Not Modified
688 4.798689  10.2.2.87       70.42.185.10    HTTP      GET /script/omniture/s_code.js HTTP/1.1
690 4.799850  70.42.185.10    10.2.2.87       HTTP      HTTP/1.1 304 Not Modified
692 4.801412  70.42.185.10    10.2.2.87       HTTP      HTTP/1.1 304 Not Modified
693 4.801882  70.42.185.10    10.2.2.87       HTTP      HTTP/1.1 304 Not Modified
```

Account Hijacking

- ***Information theft***
  - ***Phishing -> Malware, Keyloggers***
  - ***Hacking the FI or service provider***
  - ***Theft from hard copy documents***
  - ***Insiders***
- ***Targets***
  - ***High value, low tech (private education, religious organizations, non-profits)***

Account Hijacking

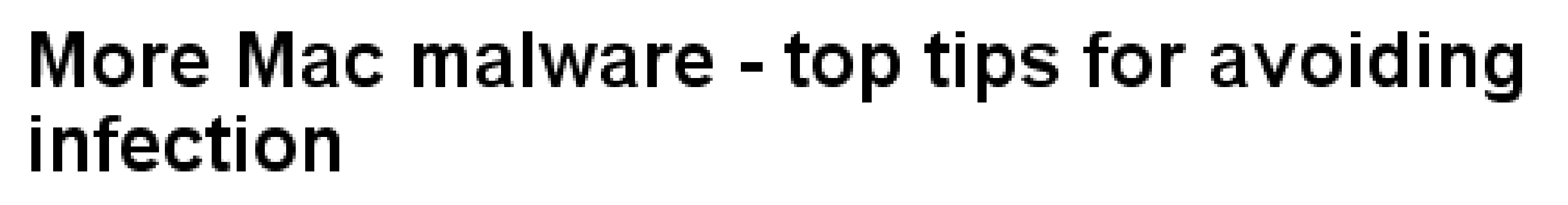
- ***Recruitment of Money Mules***
  - ***Job Offers***
- ***Execution***
  - ***Synchronized activity of draining victim's account***
  - ***Rapid movement of money from mules to criminal enterprise***

MAC Users Beware!!

MAC Video

Courtesy: Sophos

MAC Users Beware!!



More Mac malware - top tips for avoiding infection

- **If you use Safari, turn OFF the *open "safe" files after downloading* option.**
- **Don't rely on Apple's built-in XProtect malware detector.**
- **Install genuine anti-virus software.**
- **Refuse any anti-malware software which offers a free scan but forces you to pay for cleanup.**

Courtesy: Sophos

Mobile Device Security

- Threat is small relative to Windows computers but is GROWING!
- Risks
  - Data theft - Disruption of networks
  - Hijacking of phone to send revenue generating SMS
  - Windows and Symbian OS most targeted
- Over 200 examples of malicious code

Courtesy: Sophos

Mobile Device Security

- Vectors
  - Email
  - MMS
  - External Memory Cards
  - PC Synchronization
  - Bluetooth

Courtesy: Sophos

Software Toolchest

- *Anti-Virus*
  - *AVG*
  - *Avast*
  - *Check with your ISP*
- *Encryption*
  - *TrueCrypt*
  - *GPG*
- *Firewall*
  - *Comodo*
  - *Zone Alarm*
- *Password Vault*
  - *Keepass*
- *Anti-Malware*
  - *Malwarebytes*
  - *SuperAntiSpyWare*
  - *Prevx*
- *Communications*
  - *TCPView*
  - *Wireshark*
- *Browser Add-ons*
  - *SiteAdvisor (McAfee)*
  - *WOT*
  - *NoScript*

Protection of Payments

- Payments
  - Checks
  - Debit/Credit Cards
  - Automated Clearing House
  - Wires

Protection of Payments

- *Checks*
  - *Easily created, replicated and modified*
  - *Blank checks should be secured*
  - *Opt out of receiving presented checks*
    - *Use online banking for check retrieval*
  - *Positive Pay for businesses*
  - *Frequently review your account for invalid transactions*
  - *Report errors promptly (generally 60 days)*

Protection of Payments

- *Cards*
  - *Subject to electronic theft (malware, skimming)*
  - *Promptly report loss or theft of a card*
  - *Issuers (VISA/Mastercard) frequently minimize risk of loss*
- *Fraud Countermeasures*
  - *Neural Network Transactional Profiling*
    - *Location/Vendor/History*
  - *Alerts*
  - *Restrictions on Overseas Transactions or vendors*

Protection of Payments

- *Automated Clearing House (ACH)*
  - *Unauthorized debiting of accounts*
  - *Small dollar amount*
  - *TEL or WEB*
- *Difficult to detect systematically*
  - *Promptly report loss*
  - *Review your account frequently*

Protection of Payments

- *Online Bill Payment*
  - *Similar to a fraudulent check or ACH*
  - *New Payee is added*
  - *Payment is sent*
- *New Biller Alert*
  - *Email notification when a new biller is added*
  - *Review your account frequently*

Protection of Payments

- ***Wires***
  - ***Customer Identification***
  - ***Transaction history***
  - ***Two Person Integrity/Dual Controls***
  - ***Technical restrictions***

Payments in Transition

- ***Mobile Payments***
  - *Many players/industries*
  - *Telco, Retailers*
  - *Starbuck's Mobile Payment*
- ***Person to Person Payments***
  - *Can be delivered to e-mail address or cell phone number*
  - *Back ends to bank account*
  - *Uses ACH to deliver funds*

Parting Thoughts

- ***Security is a System of Shared Responsibility***
  - ***End users***
  - ***Operators***
  - ***Technology***
  - ***Processes***
- ***Tips***
  - ***Subscribe to Alerts if available***
  - ***Note the last login times when accessing systems***
  - ***Do not share that which you don’t want stolen***
  - ***Don’t be a stranger to your online banking site***

Questions

???

References and Resources

- *Consumer Banking Information*
  - *http://www.fdic.gov/consumers/consumer/information/shopprot.html*
- *Antiphishing Working Group*
  - *http://www.antiphishing.org/index.html*
- *Website Trust Ratings*
  - *http://www.mywot.com/*
  - *http://www.siteadvisor.com/*
- *IT Security Blog*
  - *http://nakedsecurity.sophos.com/*
- *Internet Crimes Complaint Center*
  - *http://www.ic3.gov/default.aspx*