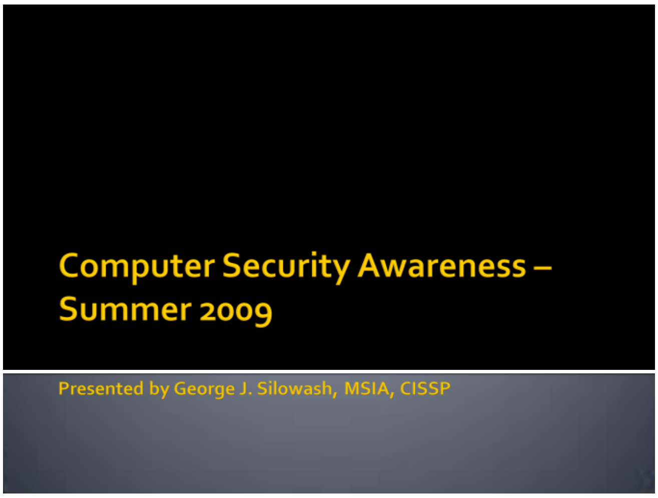
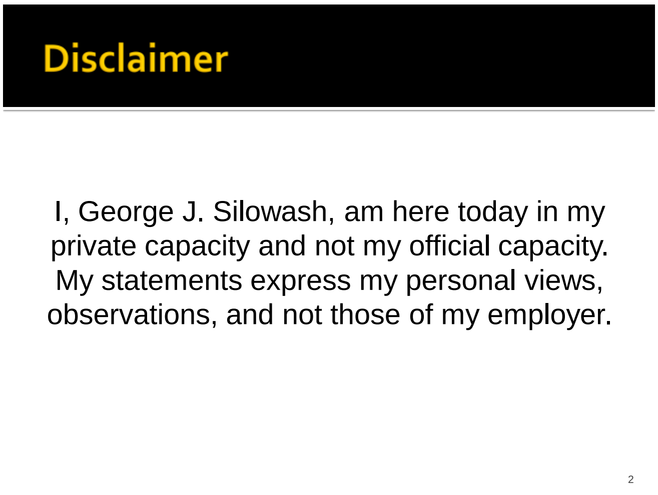


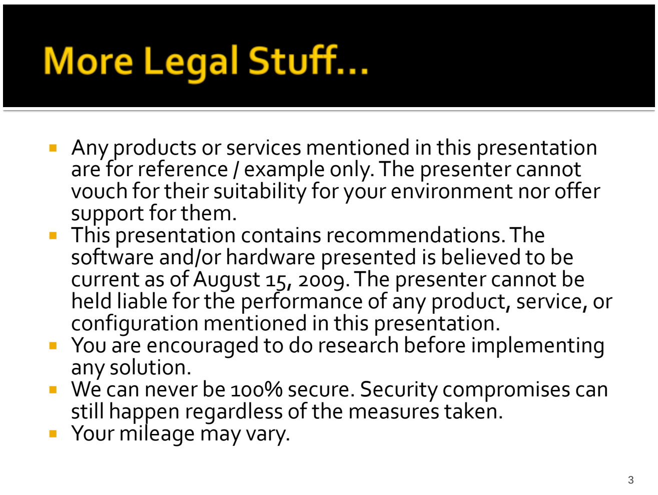
Computer Security Awareness – Summer 2009

Presented by George J. Silowash, MSIA, CISSP



Disclaimer

I, George J. Silowash, am here today in my private capacity and not my official capacity. My statements express my personal views, observations, and not those of my employer.



More Legal Stuff…

- Any products or services mentioned in this presentation are for reference / example only. The presenter cannot vouch for their suitability for your environment nor offer support for them.
- This presentation contains recommendations. The software and/or hardware presented is believed to be current as of August 15, 2009. The presenter cannot be held liable for the performance of any product, service, or configuration mentioned in this presentation.
- You are encouraged to do research before implementing any solution.
- We can never be 100% secure. Security compromises can still happen regardless of the measures taken.
- Your mileage may vary.

About the Presenter

George J. Silowash, MSIA, CISSP
george@msiaguy.com

- Master of Science in Information Assurance, Norwich University '07
- Certified Information Systems Security Professional (CISSP)
- Several awards for Information Security projects / activities

Copyright

Copyright Summary

- **http://creativecommons.org/licenses/by-nc-sa/3.0/**

- ***<u>You are free:</u>***

- to Share — to copy, distribute and transmit the work
- to Remix — to adapt the work

Under the following conditions:

- Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

- Noncommercial — You may not use this work for commercial purposes.

- Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

Today we will discuss…

- Quick Terminology
- Current Threats
- Phishing
- Safe Computing Habits

BONUS:

- Social Network Security Awareness

Some Quick Terms

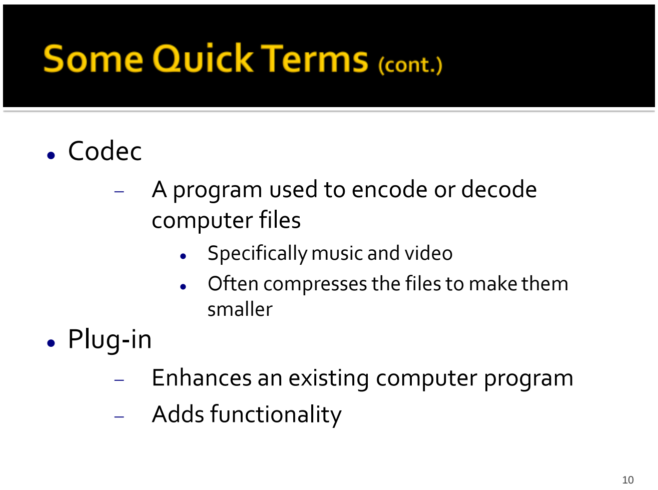
- Virus
  - A malicious software program capable of causing damage to a computer's data, operating system, and/or programs.
  - Requires human intervention to spread to other computers
    - Click a link, open an attachment, etc.

http://wordnetweb.princeton.edu/perl/webwn?s=virus

Some Quick Terms (cont.)

- Worm
  - A malicious software program capable of reproducing itself over a network
  - Requires NO human interaction
    - Computers connected directly to the Internet with no firewall

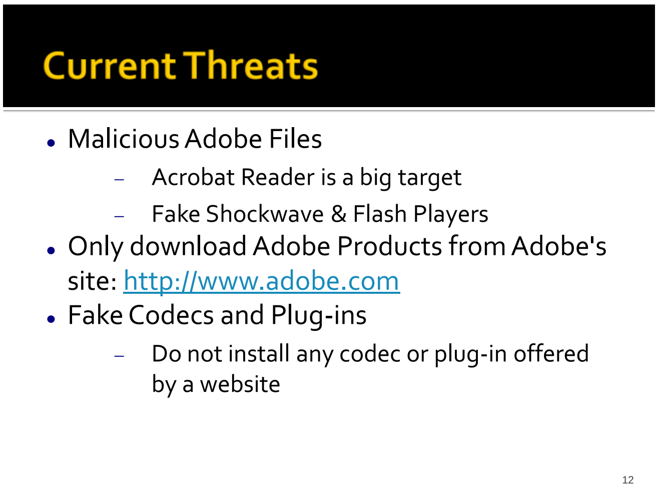
http://wordnetweb.princeton.edu/perl/webwn?s=worm



Some Quick Terms (cont.)

- Codec
  - A program used to encode or decode computer files
    - Specifically music and video
    - Often compresses the files to make them smaller
- Plug-in
  - Enhances an existing computer program
  - Adds functionality

Current Threats



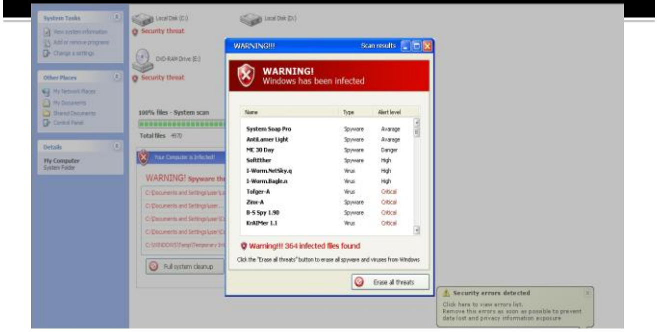
Current Threats

- Malicious Adobe Files
  - Acrobat Reader is a big target
  - Fake Shockwave & Flash Players
- Only download Adobe Products from Adobe's site: http://www.adobe.com
- Fake Codecs and Plug-ins
  - Do not install any codec or plug-in offered by a website

Current Threats (cont.)

- Fake Antivirus
  - Trusted sites appear to offer Antivirus through ads and links
  - Actual virus that infects your computer
- Phishing
  - Attacker is looking to gain additional information about you
    - Passwords, credit card numbers, banking information
  - Type of social engineering attack
  - Spear Phishing attacks target specific groups of people

Fake Antivirus Example



WARNING!!! Scan results

WARNING!
Windows has been infected

Name	Type	Alert level
System Soap Pro	Spyware	Average
AntiLamer Light	Spyware	Average
MC 30 Day	Spyware	Danger
SoftEther	Spyware	High
I-Worm.NetSky.q	Virus	High
I-Worm.Bagle.n	Virus	High
Tofger-A	Virus	Critical
Zinx-A	Spyware	Critical
B-S Spy 1.90	Spyware	Critical
KrAIMer 1.1	Virus	Critical

Warning!!! 364 infected files found

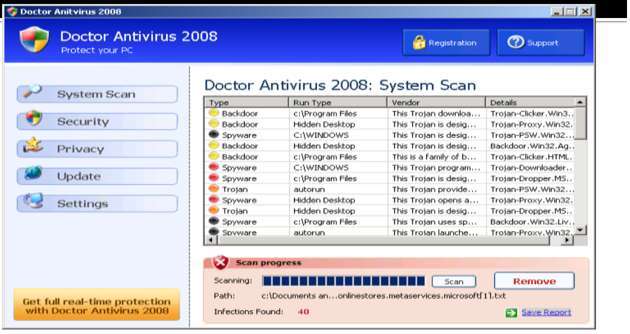
Click the "Erase all threats" button to erase all spyware and viruses from Windows

Erase all threats

Security errors detected
Click here to view errors list.
Remove this errors as soon as possible to prevent data lost and privacy information exposure

http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

Fake Antivirus Example



Doctor Antivirus 2008: System Scan

Type	Run Type	Vendor	Details
Backdoor	c:\Program Files	This Trojan downloa...	Trojan-Clicker.Win3..
Backdoor	Hidden Desktop	This Trojan is desig...	Trojan-Proxy.Win32.
Spyware	C:\WINDOWS	This Trojan is desig...	Trojan-PSW.Win32...
Backdoor	Hidden Desktop	This Trojan is desig...	Backdoor.Win32.Ag..
Backdoor	c:\Program Files	This is a family of b...	Trojan-Clicker.HTML.
Spyware	C:\WINDOWS	This Trojan program...	Trojan-Downloader..
Spyware	c:\Program Files	This Trojan is desig...	Trojan-Dropper.MS..
Trojan	autorun	This Trojan provide...	Trojan-PSW.Win32...
Spyware	Hidden Desktop	This Trojan opens a...	Trojan-Proxy.Win32.
Trojan	Hidden Desktop	This Trojan is desig...	Trojan-Dropper.MS..
Spyware	c:\Program Files	This Trojan uses sp...	Backdoor.Win32.Liv..
Spyware	autorun	This Trojan launche...	Trojan-Proxy.Win32.

Scan progress

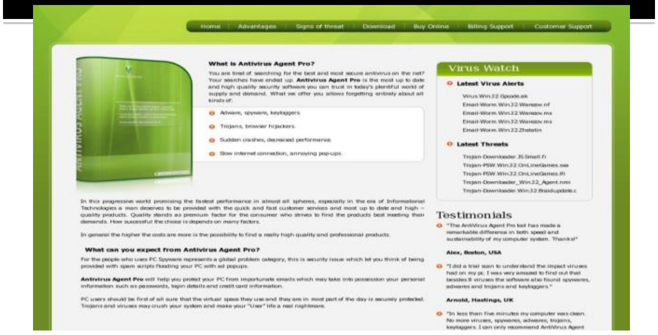
Scanning:

Path: c:\Documents an...onlinestores.metaservices.microsoft[1].txt

Infections Found: 40

http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

Fake Antivirus Websites



What is Antivirus Agent Pro?

You are tired of searching for the best and most secure antivirus on the net? Your searches have ended up. **Antivirus Agent Pro** is the most up to date and high quality security software you can trust in today's plentiful world of supply and demand. What we offer you allows forgetting entirely about all kinds of:

- Adware, spyware, keyloggers.
- Trojans, browser hijackers.
- Sudden crashes, decreased performance.
- Slow internet connection, annoying pop-ups.

In this progressive world promising the fastest performance in almost all spheres, especially in the era of Informational Technologies a man deserves to be provided with the quick and fast customer services and most up to date and high – quality products. Quality stands as premium factor for the consumer who strives to find the products best meeting their demands. How successful the choice is depends on many factors.

In general the higher the costs are more is the possibility to find a really high quality and professional products.

What can you expect from Antivirus Agent Pro?

For the people who uses PC Spyware represents a global problem category, this is security issue which let you think of being provided with spam scripts flooding your PC with ad popups.

Antivirus Agent Pro will help you protect your PC from importunate emails which may take into possession your personal information such as passwords, login details and credit card information.

PC users should be first of all sure that the virtual space they use and they are in most part of the day is securely protected. Trojans and viruses may crush your system and make your "User" life a real nightmare.

Virus Watch

- **Latest Virus Alerts**
  - Virus.Win32.Gpcode.ak
  - Email-Worm.Win32.Warezov.nf
  - Email-Worm.Win32.Warezov.mx
  - Email-Worm.Win32.Warezov.ms
  - Email-Worm.Win32.Zhelatin
- **Latest Threats**
  - Trojan-Downloader.JS.Small.fi
  - Trojan-PSW.Win32.OnLineGames.saa
  - Trojan-PSW.Win32.OnLineGames.tfi
  - Trojan-Downloader_Win32_Agent.nmi
  - Trojan-Downloader.Win32.Braidupdate.c

Testimonials

- "The AntiVirus Agent Pro tool has made a remarkable difference in both speed and sustainability of my computer system. Thanks!"

Alex, Boston, USA

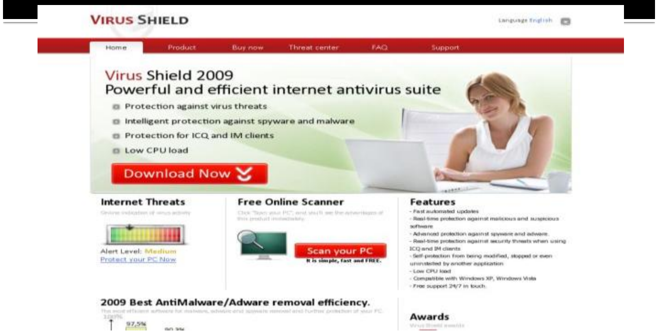
- "I did a trial scan to understand the impact viruses had on my pc. I was very amazed to find out that besides 8 viruses the software also found spywares, adwares and trojans and keyloggers."

Arnold, Hastings, UK

- "In less than five minutes my computer was clean. No more viruses, spywares, adwares, trojans, keyloggers. I can only recommend AntiVirus Agent

http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

Fake Antivirus Websites



Virus Shield 2009
Powerful and efficient internet antivirus suite

- Protection against virus threats
- Intelligent protection against spyware and malware
- Protection for ICQ and IM clients
- Low CPU load

Internet Threats

Online indication of virus activity

Free Online Scanner

Click "Scan your PC", and you'll see the advantages of this product immediately.

Features

- Fast automated updates
- Real-time protection against malicious and suspicious software
- Advanced protection against spyware and adware.
- Real-time protection against security threats when using ICQ and IM clients
- Self-protection from being modified, stopped or even uninstalled by another application
- Low CPU load
- Compatible with Windows XP, Windows Vista
- Free support 24/7 in touch.

2009 Best AntiMalware/Adware removal efficiency.

The most efficient software for malware, adware and spyware removal and further protection of your PC.

Awards

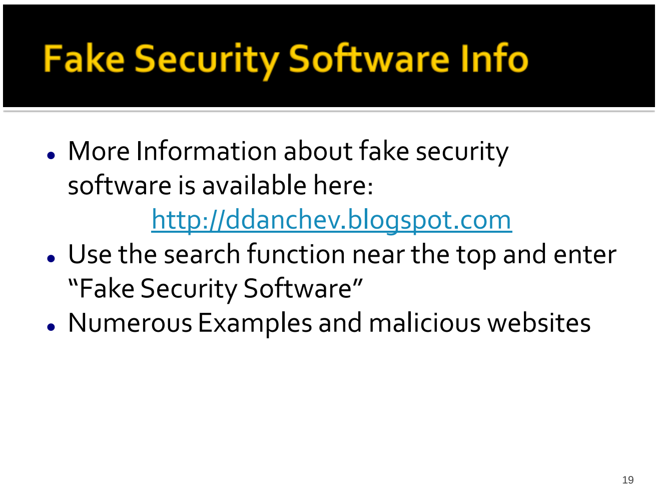
Virus Shield awards

http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

Fake Antivirus Dangers

- Installs other malicious code / Trojans
  - Steal passwords, other sensitive information
- Nags you to pay in order to remove "infections"
  - Infections do not exist or if they do, they were placed by the Trojan & downloads other Trojans
  - What does the software do with your credit card number?
- Some traces back to Russian Business Network to fund illegal activities

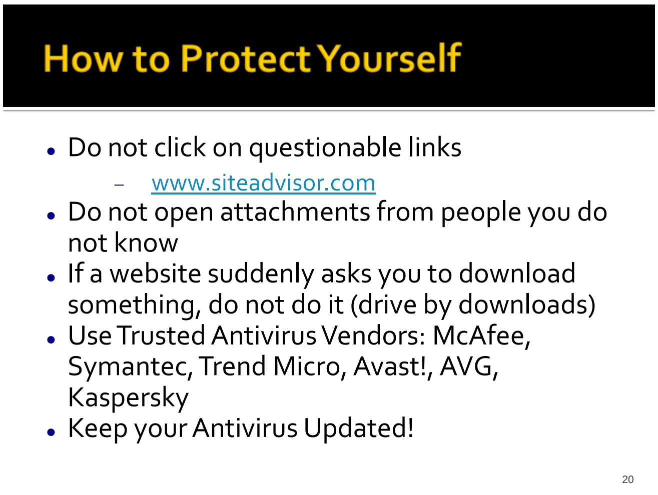
http://www.symantec.com/connect/blogs/misleading-applications-show-me-money



Fake Security Software Info

- More Information about fake security software is available here:
  http://ddanchev.blogspot.com
- Use the search function near the top and enter "Fake Security Software"
- Numerous Examples and malicious websites

19



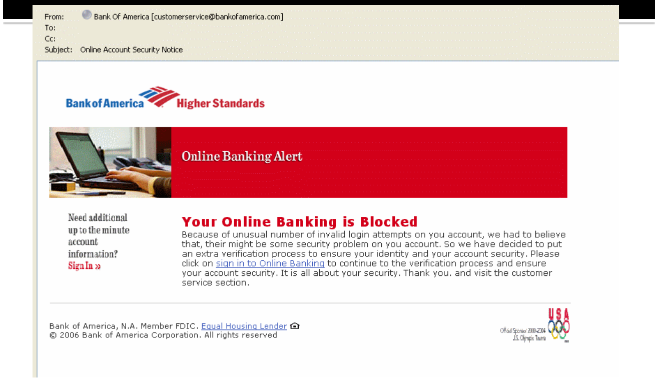
How to Protect Yourself

- Do not click on questionable links
  - www.siteadvisor.com
- Do not open attachments from people you do not know
- If a website suddenly asks you to download something, do not do it (drive by downloads)
- Use Trusted Antivirus Vendors: McAfee, Symantec, Trend Micro, Avast!, AVG, Kaspersky
- Keep your Antivirus Updated!

20

Phishing

Would you fall for this?



From: Bank Of America [customerservice@bankofamerica.com]
To:
Cc:
Subject: Online Account Security Notice

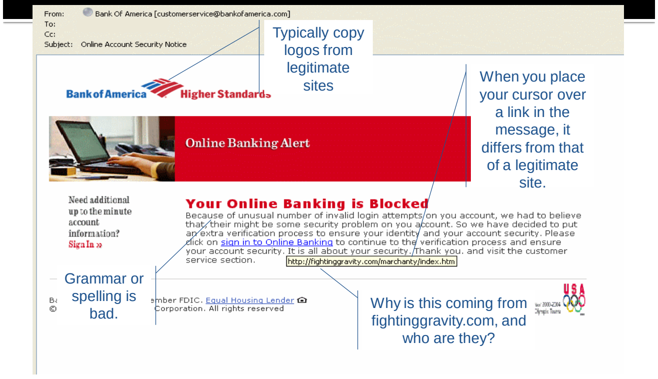
Need additional up to the minute account information?
Sign In »

Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you. and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2006 Bank of America Corporation. All rights reserved

Spotting the Phish



From: Bank Of America [customerservice@bankofamerica.com]
To:
Cc:
Subject: Online Account Security Notice

Need additional up to the minute account information?
Sign In »

Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you. and visit the customer service section.

http://fightinggravity.com/marchanty/index.htm

Ba ember FDIC. Equal Housing Lender
© Corporation. All rights reserved

Typically copy logos from legitimate sites

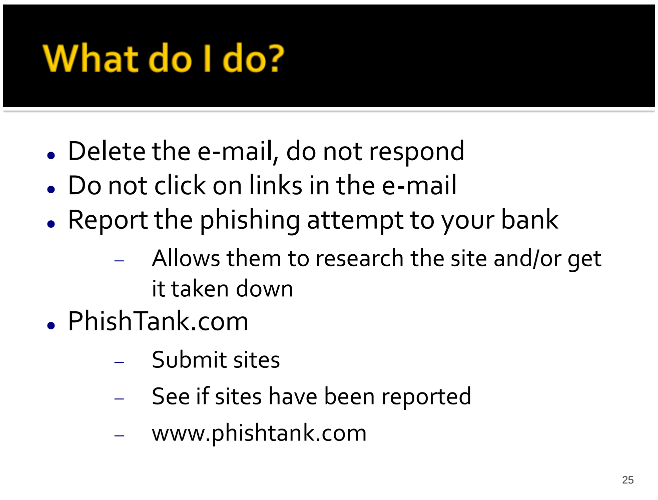
When you place your cursor over a link in the message, it differs from that of a legitimate site.

Grammar or spelling is bad.

Why is this coming from fightinggravity.com, and who are they?

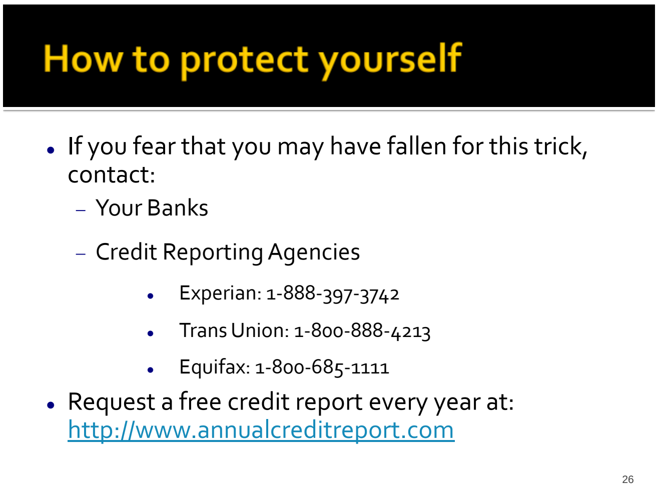
Other Phishing Flags

- Banks will not e-mail you to update account information
  - Never provide personal / sensitive information via e-mail
- If you receive an email from someone you do not do business with
- If it doesn't look or feel right, something is probably wrong



What do I do?

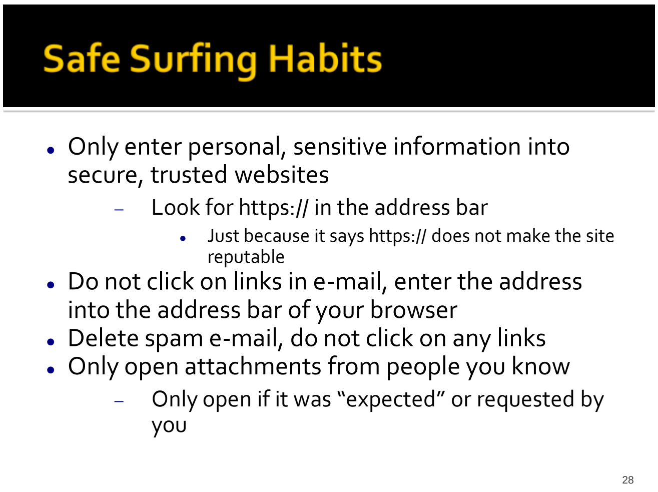
- Delete the e-mail, do not respond
- Do not click on links in the e-mail
- Report the phishing attempt to your bank
  - Allows them to research the site and/or get it taken down
- PhishTank.com
  - Submit sites
  - See if sites have been reported
  - www.phishtank.com



How to protect yourself

- If you fear that you may have fallen for this trick, contact:
  - Your Banks
  - Credit Reporting Agencies
    - Experian: 1-888-397-3742
    - Trans Union: 1-800-888-4213
    - Equifax: 1-800-685-1111
- Request a free credit report every year at: http://www.annualcreditreport.com

Safe Computing Habits



Safe Surfing Habits

- Only enter personal, sensitive information into secure, trusted websites
  - Look for https:// in the address bar
    - Just because it says https:// does not make the site reputable
- Do not click on links in e-mail, enter the address into the address bar of your browser
- Delete spam e-mail, do not click on any links
- Only open attachments from people you know
  - Only open if it was "expected" or requested by you

28

Safe Computing Habits (cont.)

- Keep Microsoft Windows & Office updated with the latest patches
  - http://update.microsoft.com
  - "Patch Tuesday" is the second Tuesday of every month
- Apply Adobe updates ASAP
  - Many vulnerabilities targeting Adobe products recently

29

Social Networking

Social Networking Awareness

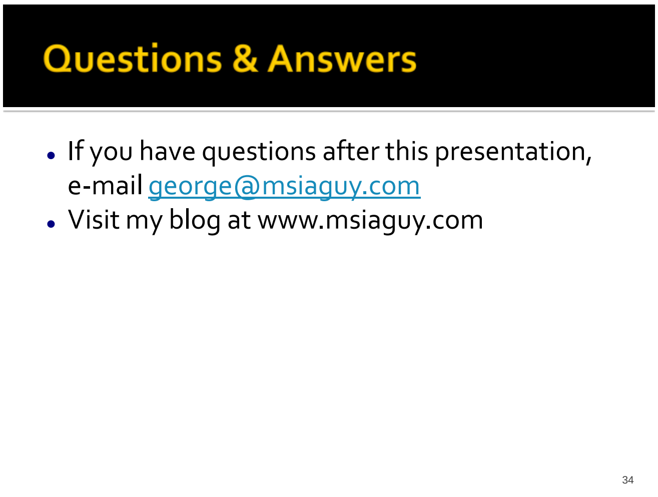
- What is social networking?
  - A way of connecting with people online
  - May be friends, professionals, etc that you know personally or have an indirect relationship with
  - People create a profile and request to be friends with others
    - Request is approved or denied
- Big Names in Social Networking:
  - Facebook, LinkedIn, Myspace, Twitter

Social Networking Privacy & Security

- Be careful what you post online
  - Can information gleamed from your profile be used to guess your passwords?
    - Facebooks users circulate "notes" that ask various questions about yourself
  - Can information you post be used against you in seeking business contracts, employment, etc.?
  - Do you really need to let people know exactly what you are doing?
    - "I am at the movies with my family."
    - I know no one is at home right now, or better yet, I know where I can find you.

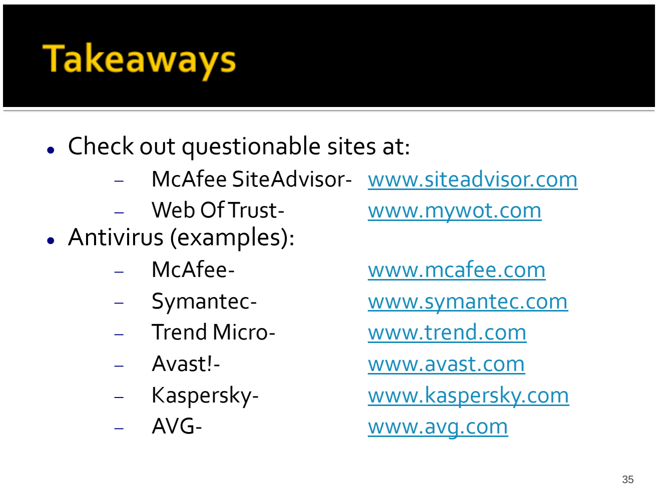
Security Issues

- Koobface virus
  - Spread by malicious links on websites
    - Headline Example: "My friend catched you on hidden cam"
    - Linked to malware or fake video requiring you to download a "codec" to view the file
    - Stole sensitive information (credit card numbers, passwords, etc.)
- Links may not take you where you think they are going to take you



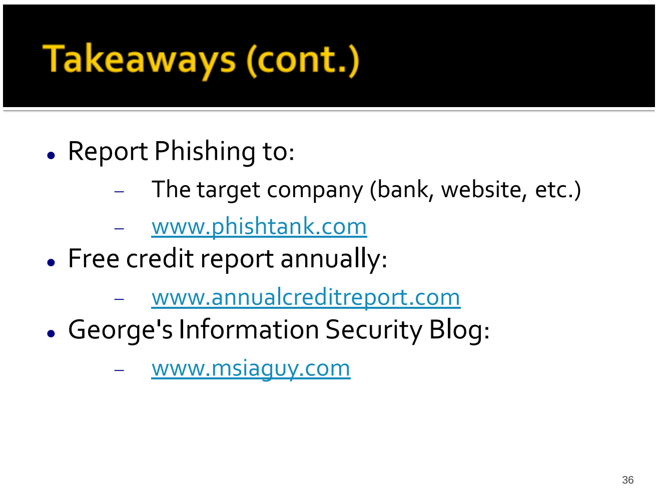
Questions & Answers

- If you have questions after this presentation, e-mail george@msiaguy.com
- Visit my blog at www.msiaguy.com



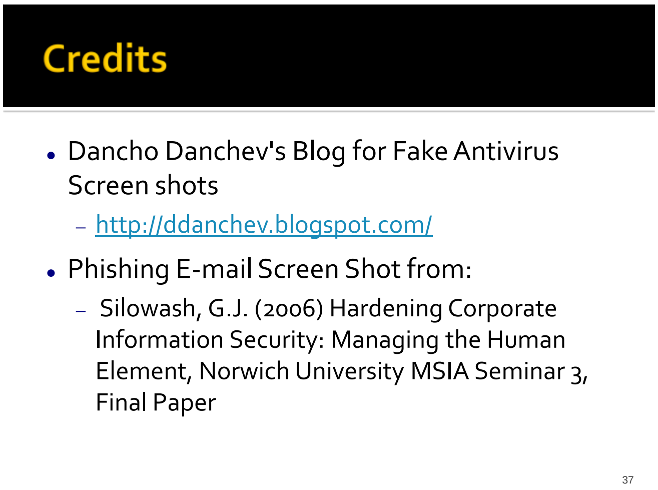
Takeaways

- Check out questionable sites at:
  - McAfee SiteAdvisor- www.siteadvisor.com
  - Web Of Trust- www.mywot.com
- Antivirus (examples):
  - McAfee- www.mcafee.com
  - Symantec- www.symantec.com
  - Trend Micro- www.trend.com
  - Avast!- www.avast.com
  - Kaspersky- www.kaspersky.com
  - AVG- www.avg.com



Takeaways (cont.)

- Report Phishing to:
  - The target company (bank, website, etc.)
  - www.phishtank.com
- Free credit report annually:
  - www.annualcreditreport.com
- George's Information Security Blog:
  - www.msiaguy.com



Credits

- Dancho Danchev's Blog for Fake Antivirus Screen shots
  - http://ddanchev.blogspot.com/
- Phishing E-mail Screen Shot from:
  - Silowash, G.J. (2006) Hardening Corporate Information Security: Managing the Human Element, Norwich University MSIA Seminar 3, Final Paper