Staying Safe & Secure Online

Joseph Guarino
Owner/Sr. Consultant Evolutionary IT
CISSP, LPIC, MCSE 2000, MCSE 2003, PMP
Toastmasters CC, ACB

www.evolutionaryit.com

Objectives

- Detail the fundamentals of Information Security and explain why it matters.
- Arm you with practical tools and knowledge to defend yourself.

Who am I

- Joseph Guarino
- Working in IT for last 15 years: Systems, Network, Security Admin, Technical Marketing, Project Management, IT Management
- CEO/Sr. IT consultant with my own firm Evolutionary IT
- CISSP, LPIC, MCSE, PMP, Toastmasters CC,ACB
- www.evolutionaryit.com

Computer Security

The fundamentals for the everyday users.

Common Misperceptions

- *“I have anti-virus software...”*
- *“I don't personally have anything of value on my computer...”*
- *“I have a firewall...”*
- *“I don't need to backup...”*
- *“There are no major financial risks...”*

Key terms/concepts

Define some key terms...

General Terms

- **Software Bug** – an error, flaw or mistake in a computer program.
- **Vulnerability** – is a weakness in a system that allows an attacker to exploit or otherwise violate the integrity of your system.
- **Patch** – a fix for a software bug or security vulnerability.

Malware Terms

- **Malware** – software designed to infect and damage a user's computer system without the owner's consent. This is the general all encompassing term.
- **Virus** – computer program that infects or copies itself onto a user's computer system without user's permission/consent. Most often a virus delivers a dangerous payload or action.

Malware Terms

- **Spyware** – software installed surreptitiously on a users computer system to intercept, monitor, market.
- **Adware** – software installed surreptitiously which is designed to deliver ads.
- **Badware** – alternative term used to describe spyware, malware and deceptive adware.
- **Grayware** – term used to describe spyware, adware, dialers, remote access kits that harm systems performance.

Malware Terms

- **Bot** – machines infected with worms, trojans or other malware under a centralized control structure.
- **Worms** – network enabled or aware viruses.
- **Rats** – remote access toolkits which allow remote access to a users machine.

Malware Terms

- **Dialer** – an unwanted dial application which connects to pay-rate phone numbers.
- **Rootkits** - program that takes fundamental control of your system without your consent.
- **Key Loggers** – hardware or software means of capturing users keystrokes.
- **Phishing** – attempt via email, IM or other malware to redirect user to fraudulent websites.

Evolution of Malware

- Malware today has evolved beyond the simple virus.
- Malware's evolution will NOT stop and it will be a constant battle to defend against an ever changing threat.
- Profit motive of cyber criminals will always bring new threats.
- Consider that the threats will expand to new technologies.

Software Licensing Terms

- **Commercial Software –** proprietary software that you commonly use. Has very restrictive rights on use.
- **Shareware/Trialware/Nagware** – a trial version of a commercial program. Can sometimes contain malware.
- **Freeware** – free in terms of price. No cost but can sometimes contain malware.

Software Licensing Terms

- **Open Source** – allows anyone the liberty to use, extend and distribute the software as they see fit. No Nag/Grey/Ad/Badware.
- **Free Software** - allows anyone the liberty to use, extend and distribute the software as they see fit. Focus on freedoms/liberty above all else. No Nag/Grey/Ad/Badware.
- **FOSS** – Free and open source software is a term to specify the range of free and open source software.

Who creates this stuff?

- Where does it come from?
- Why do the create it?
- Myth vs. Reality

Hackers?

Hackers

- **Hackers** are not the media tells us they are.
- **White hat** = Good. Often called ethical hackers who help society, law enforcement and government.
- **Grey hat** = Middle of the road, sometimes good sometimes bad.
- **Black hat** = Compromised ethics and often criminally minded.
- **Hacker** in the technical and engineering community really means a person who wants to learn and understand something.

Crackers

Correct term is cracker, black hat or cyber criminal.

Cracking Demo/Psychographic

- Today it is less of teens just “messing around” like the movie War Games.
- Real threats are: criminal syndicates, foreign governments, general thugs.
- These organizations are the “well-source” of most of these activities.

Cracking Demo/Psychographic

- Motive (Money), Opportunity (Unpatched, insecure systems/network), Means (Resources).
- Crackers use increasingly sophisticated software to mount attacks.
- Malware consistently evolves around the attempts to defend against it.
- Evolves around technologies and delivery mechanisms. If SPAM filtering gets too effective they move to IM.

Cracking Demo/Psychographic

- Increasingly - malware have advanced characteristics: distributed, polymorphic, automatically evading detection, encrypted, self-protecting and self-healing.
- Shows all the hallmarks of professional software developments but with a deeply pernicious/evil intent.

The numbers speak...

Statistics.

Cyber Crime Stats

General Stats

FBI Computer Crime Survey 2005

Frequency of attacks. Nearly nine out of 10 organizations experienced computer security incidents in a year's time; 20% of them indicated they had experienced 20 or more attacks.

Types of attacks. Viruses (83.7%) and spyware (79.5%) headed the list. More than one in five organizations said they experienced port scans and network or data sabotage.

Financial impact. Over 64% of the respondents incurred a loss. Viruses and worms cost the most, accounting for $12 million of the $32 million in total losses.

Sources of the attacks. They came from 36 different countries. The U.S. (26.1%) and China (23.9%) were the source of over half of the intrusion attempts, though masking technologies make it difficult to get an accurate reading.

Reporting. Just 9% reported them to law enforcement.

Cyber Crime Stats..

Malware Stats

According to a study from TrendMicro -

It is estimated that PC Viruses cost businesses approximately $55 Billion in damages in 2003.

The same calculations in were done in 2002 and 2001, at $20-30 Billion and $13 Billion, respectively.

According to vendor Sophos -

In 2007, they uncovered 9,500 new infected web pages daily - an increase of more than 1000 every day when compared to April. In total, 304,000 web pages hosting malicious code were identified in May.

According to Anti-malware vendor Panda Labs -

Approximately 11 percent of computers around the world are part of these botnets, and they are responsible for 85 percent of all spam sent. In 2007, PandaLabs uncovered several tools such as Zunker or Barracuda, which were being used by cyber-criminals to administer networks of thousands of infected computers across more than 50 countries.

Cyber Crime Stats

Malware Stats

- **According to Gardner** - It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million. United States businesses lose an estimated US$2 billion per year as their clients become victims. In 2007 phishing attacks escalated. 3.6 million adults lost US $ 3.2 billion in the 12 months ending in August 2007.

Security is not

All about technology!

It's about what you do.

- Computer security is as much about what you do as it is about technology.
- Being aware of how to safely operate your computer is step one.
- The right technology with proper application of that technology is only part of the equation.

Social Engineering

- Cyber criminals will attempt to manipulate, finesse, trick the information from you in the most conniving and creative ways.
- Comes in the form of calls, emails, IM's, etc.
- Don't trust them. Don't give them information.
- ATT's Anti-social Engineering Training Vid

Web Fundamentals

Fundamental Technical Concepts/Terms

DNS

- Domain name system.
- It translates the underlying IP or numeric addresses of the internet into humanly readable form.
- I.e. www.google.com and not 74.125.47.147
- .com, edu, .gov, .mil. .au (Australia), .de (Germany), .it (Italy).

Domain name

- Domain name locates an organization online.
- GTLD (Generic Top Level Domains). Class of organizations. Ex. .com, .net, .gov.
- CcTLD (Country Code Top Level Domain). Country or territory. Ex. .us (USA), .it (Italy)

Anatomy of web address

- URL – Universal Resource Locator or URI Uniform Resource Identifier.
- Web address
- http://en.wikipedia.org
- Protocol – http, https, ftp, etc.
- Hostname – name of machine.
- Domain name - .org - non-profit

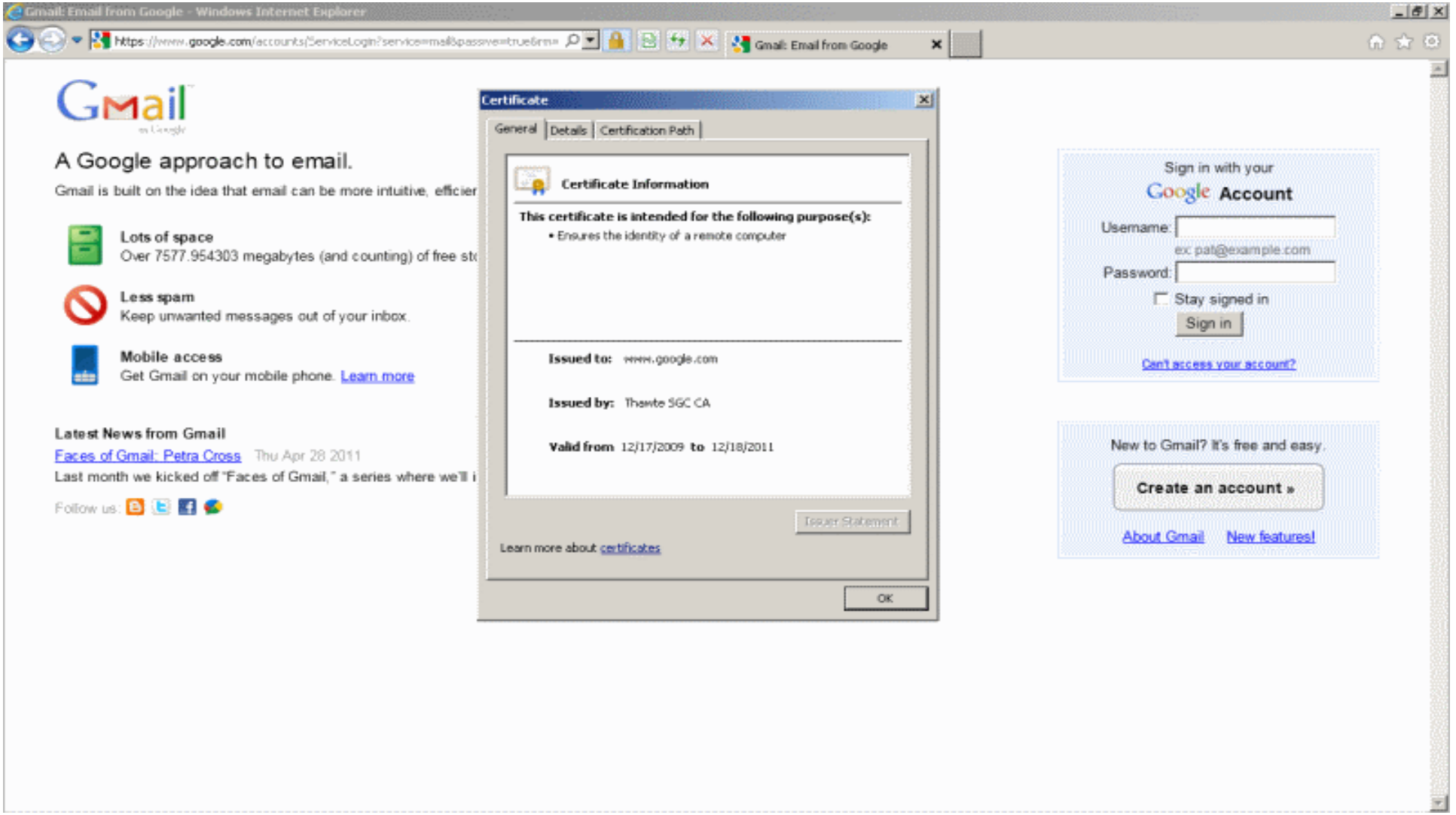
Anatomy of a web address
SSL

- Https
- SSL/TLS
- Secure encrypted web connection. Shows up as a lock in the browser.
- Don't enter in Personal Identifiable Information or engage in commerce without it!

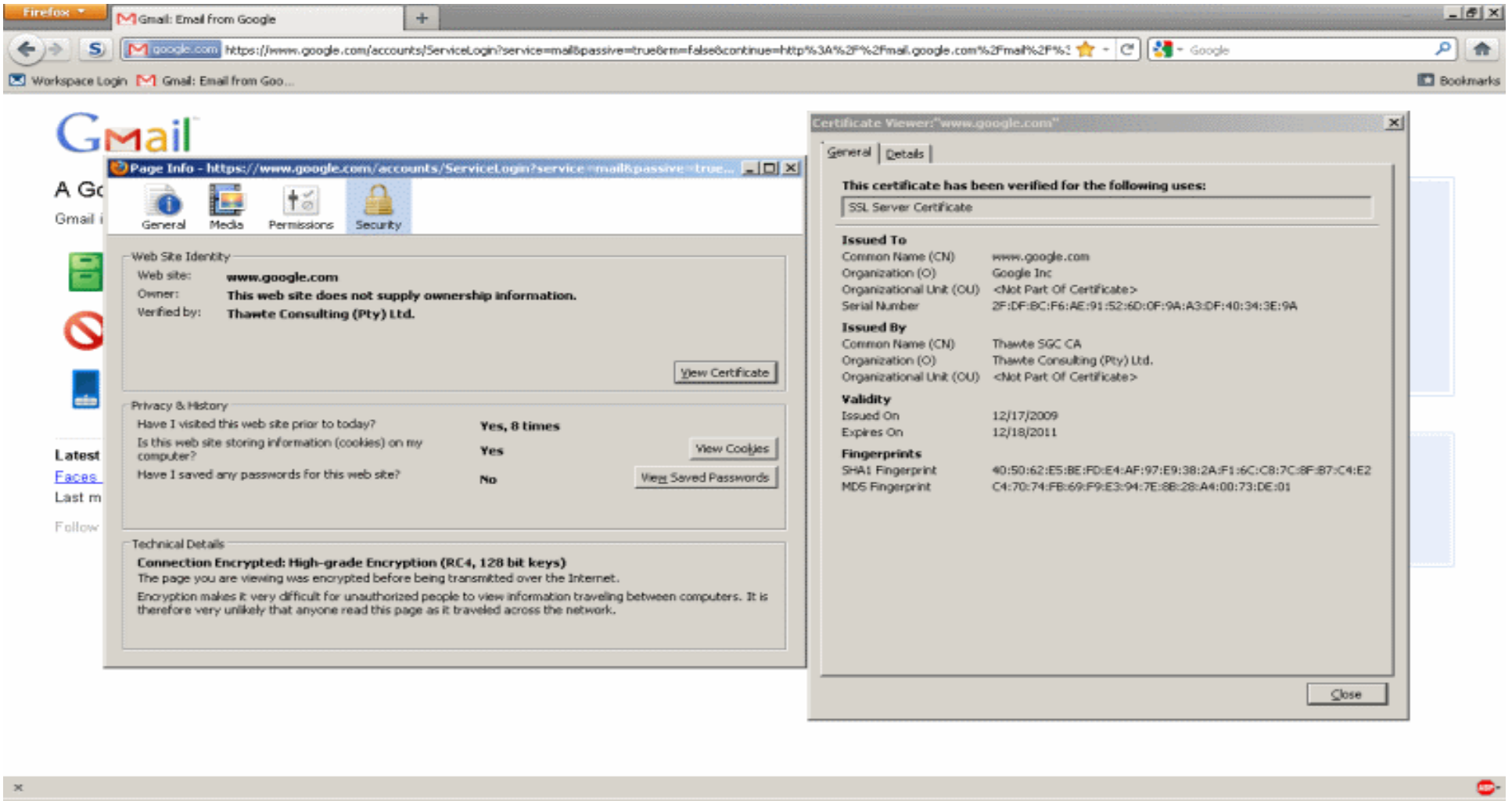
Anatomy of a Digital Certificate

- Much like a drivers license or other form of ID.
- Issued by Certification Authority such as Verisign, Thawte, GeoTrust, Entrust, Comodo or Godaddy.
- Validates that the website you are connected to.
- Look for the Lock!

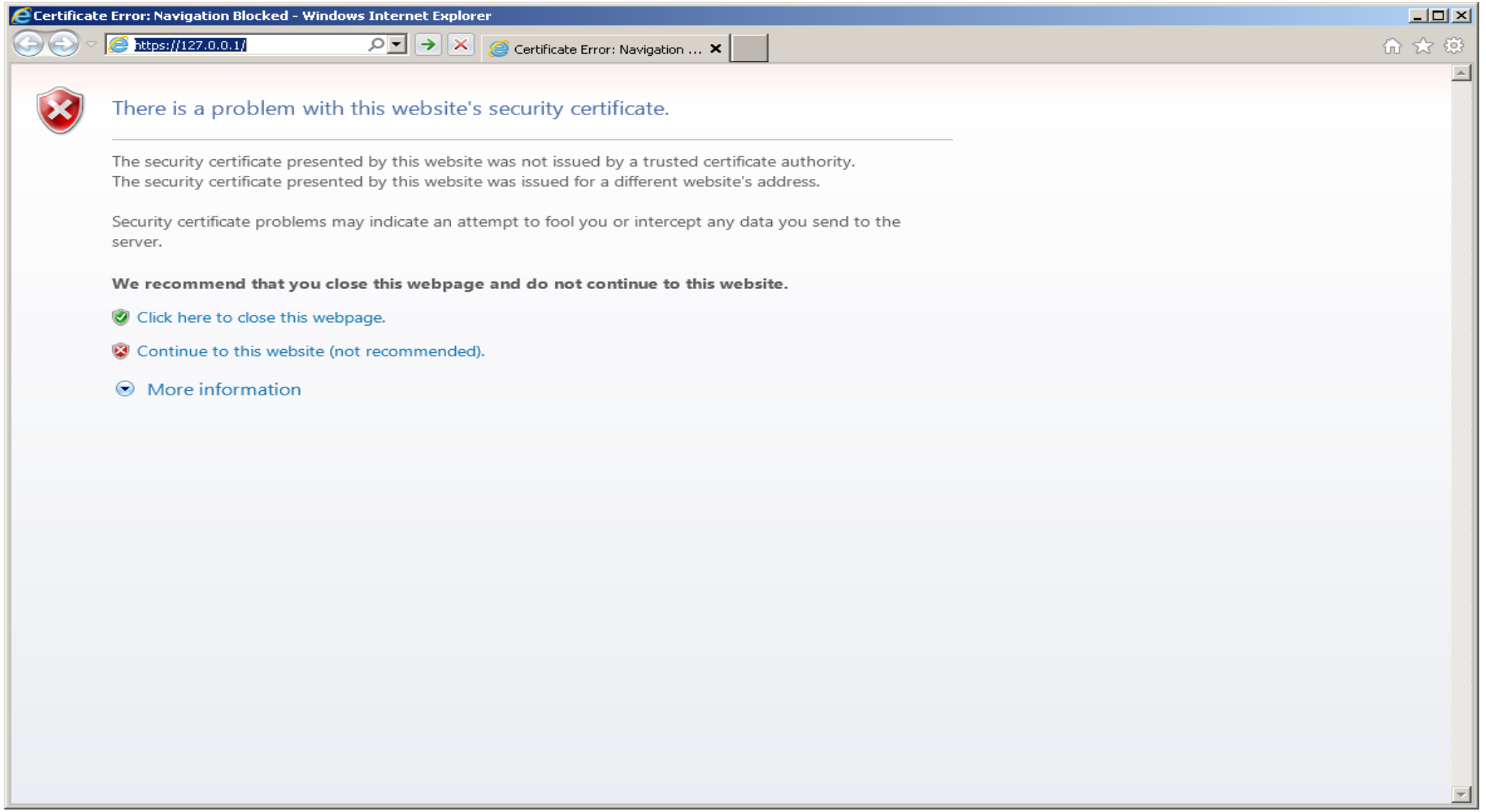
Internet Explorer 9 SSL Example
Valid Certificate



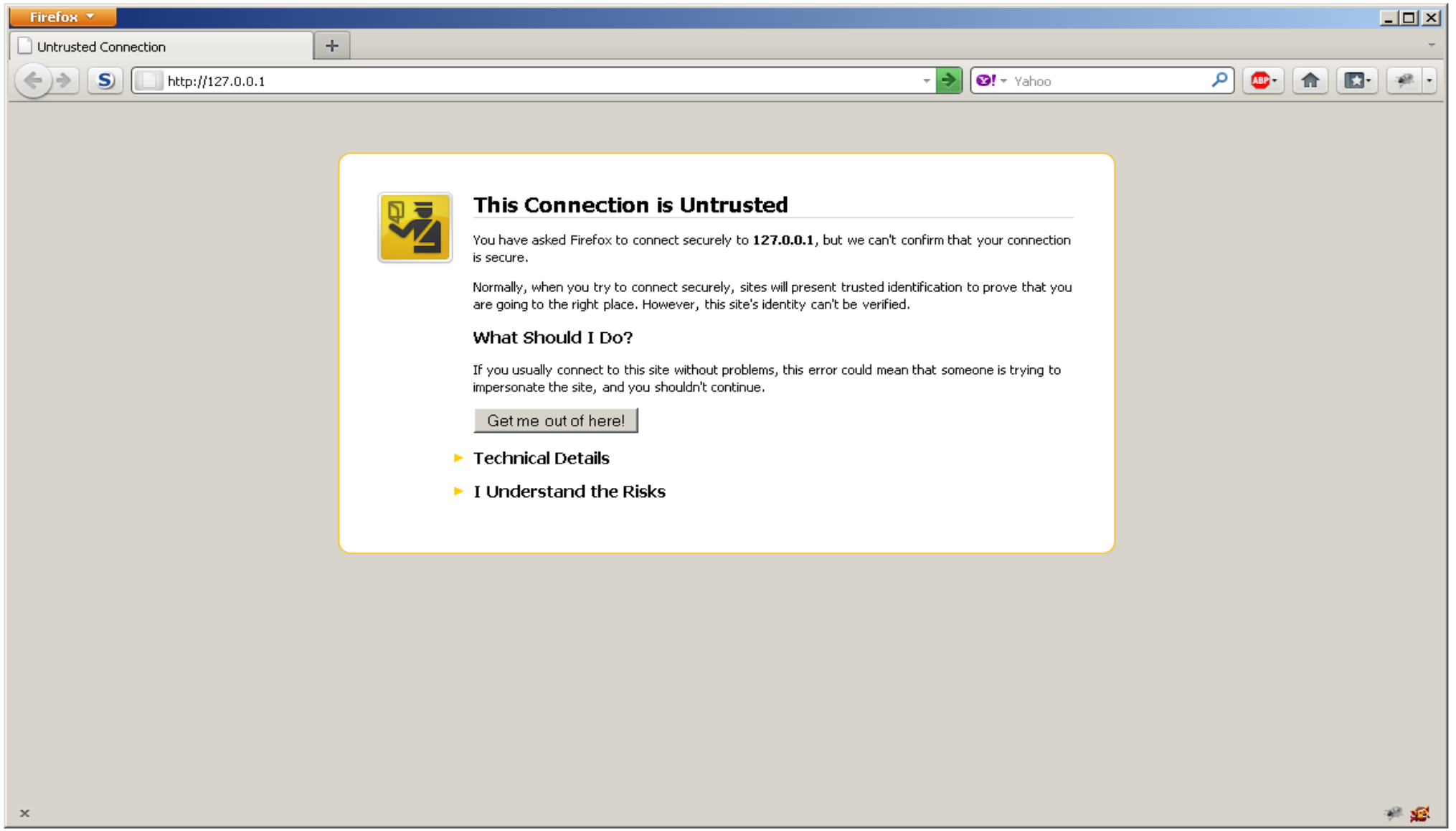
Firefox 4.x SSL Example
Valid Certificate



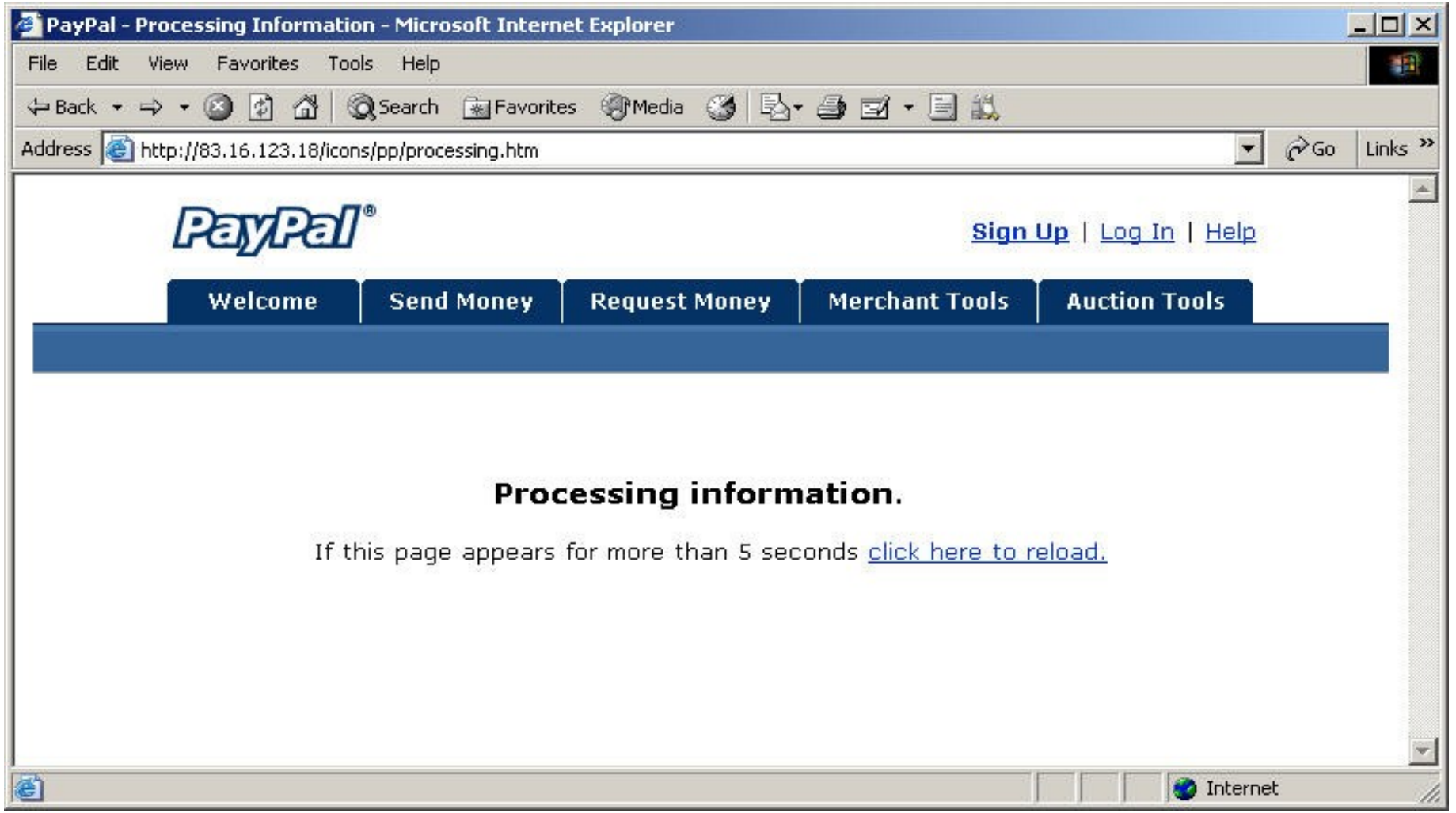
Internet Explorer 9 SSL Example Error!



Firefox 4.x Example Error!



Internet Explorer SSL Example Fraudulent



Web Threats

What are the threats?

Web Surfing Threats

- Malware is often delivered via websites clandestinely without your knowledge or approval.
- Phishing can redirect you to false websites that are used to harvest your login/password, credit card info, general identity information.
- If you don't know how to spell the name of an organization refer to company literature or Google, Yahoo, MSN.
- Browser based attacks are increasingly common. This type of attack pinpoints vulnerabilities in the browser software itself and it associated plug-ins(Flash), or technologies(Java/Javascript). Expect this trend to continue.

Phishing

- SPAM, Social Media Site, brings you messages that seem to be from legitimate parties that send you to phony/look-alike website.
- Your (Personally Identifiable Information) and credit card information is collected and sold in the underground.
- Usually an attempt is also made to infect your machine with malware.
- Best to not even open. Delete.

Phishing Cont.

- Think before you click! Don't open. Delete it!
  - Are you a customer? - If not Mark as SPAM and delete.
  - Did you have any recent interaction with the company involved? - Don't open it. Deleted!
- INSTEAD, go to the official website Validate its certificate.
- Then log on to your account.

Phishing
Professional Criminals

- Phishing attempts are increasingly looking more real and like real legitimate emails.
- The data these criminals possess about you is often legitimately from data breaches and or illegal/illegitimate sources. So increasingly they can accurately make these look real.
- Phishing attempt on Executives.
- IRS Phishing Scheme.

Phishing Email Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Account cancel!
- Social Engineering – Attempt to mislead, persuade,confuse, etc.
- Generic or Targeted Greetings – Hello Distinguished Sirs!?
- Urgent Request for PII – We need to validate your account or you will be terminated from the internet!
- Forged Email. - Email is often not valid and or not from the domain in question.
- Incorrect Link – Link is obviously wrong. https://www.payppal.net/~noway

Phishing General Advice

- Paypal Anti-Phishing Guide
- Ebay Anti-Phishing Guide
- Phish Tank Website
- Anti-Phishing Working Group Archive

Web Surfing Remediation

- Only visit sites you can judge to be legitimate. If you are engaged in Ecommerce make sure certificate is valid.
- Trust not click not.
- Mistyping a URL can lead you to a fake/phishing or even malware site.
- Only go directly to the associated website via typing it in the location or address bar.

Web Surfing Remediation

- Install an up to date anti-malware suite.
- Use the existing anti-phishing tools in Windows Smart Screen Vista/7 (IE9) or OSX (Safari).
- Alternatively use such as Netcraft Toolbar.
- Keep you system patched!
- Stay away from the “underbelly” of the Internet

Websurfing
Secure your browser

- Microsoft Internet Explorer
  - Set up trusted zones.
  - Internet Explorer has anti-phishing filter.
- Mozilla Firefox
  - Optimally use Mozilla Firefox with AdblockPlus.
  - NoScript to block all executable content unless explicitly allowed.
- CERT Recommendations on Securing Browsers.

IM/Chat Threat

- Instant Messaging spammers send bulk IM (SPIM) with executables (programs), links and images.
- Threats to the Instant messenger software itself are common.
- Black Hat/Crackers/Cyber Criminals often send malware files, links, programs in chat rooms.
- Trusting people whom you have not met or know.

IM/Chat Remediation

- Don't click/open/execute messages, links, executables (programs) from sources you don't know or can validate EVER!
- Lock down your Instant Messenger settings to allow you only to receive messages from existing friends and or show you offline to all others. Granularity exists so use it.
- Update your Instant Messenger client when updates occur.
- Trust only those you truly can.

SPAM

Not that deliciously dubious “meat.”

SPAM Threats

- Spam is often a carrier/propagator of malware.
- Social Engineering is a common thread in SPAM.
- Spam and Phishing are interrelated activities.
- Spam contains beacons which spammers use to validate your email address.

SPAM Characteristics

- Grammatical/Typographical Errors – You purchases Ebay Item and late payment. Validate NOW!
- Social Engineering – Attempt to mislead, persuade, confuse, etc.
- Generic or Targeted Greetings – Good day sir!? Hello Mr. Joseph Guarino.
- Urgent Request for PII – We need to validate your account or you will be terminated from the Internet!
- Forged Email. - Why would an @aol email be sending you a Paypal or Ebay notice?
- Incorrect Link – Link is obviously wrong. https://www.payppal.edu/~noway

Spam Example Themes

- **Lotto Scams** – You have won 4mill Pounds!
- **Job Offers** – Work at home 1/hr a day and make millions!
- **Ponzi schemes** – Pyramid schemes.
- **Found money** – Found $10/million US!
- **Stock scams** – Buy this great penny stock!
- **Education scams** – Scholarships and diploma mills.
- **Romance scams** – Foreign dating sites, you have a secret admirer. Olga really does love you, even though you have never met!
- **Financial scams** – Phony IRS communications, phony bank query, free credit report, free financial seminars.

SPAM Remediation

- Don't post your email address online on websites, forums, chatrooms, etc.
- Don't open spam! Use your email software to mark it as spam and delete it.
- Never respond to SPAM.
- Never EVER buy from SPAMMERS.

SPAM Remediation

- Most standalone email clients such as Outlook, Thunderbird and OS X Mail offer built-in SPAM filtering.
- Optimally shut off or limit; Images, Javascript, Java, Flash etc in your email client or web browser if you use web based email.
- Shut off HTML mail and use plain text.
- If you are getting lots of SPAM in your Inbox, switch to another email provider that does a better job filtering.

Social Networking Threats

- Sites such as Myspace, Facebook, YouTube, Orkut, Xing, Ryze, LinkedIN.
- Cyber criminals use social networking sites as a delivery mechanisms for malware. Spammers and Malware purveyors use these sites features (email, IM, chat room) to “promote” less than reputable software and websites.
- Anonymous access to your account.
- Third party add-on applications may have security concerns.
- Fake accounts and spam content abound on some of these sites.
- Comment spam is a major problem on some of these sites.

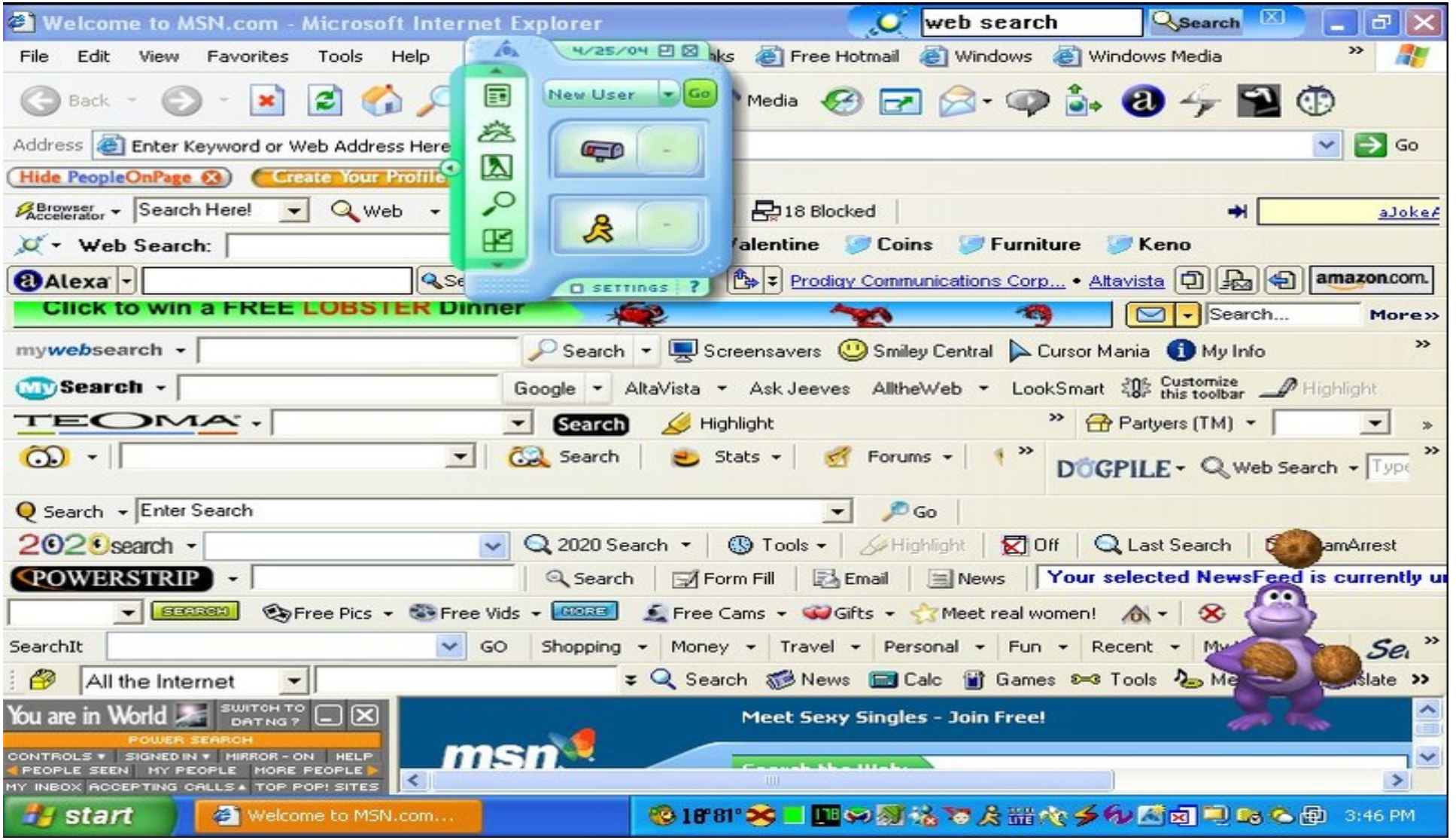
Social Networking Remediation

- If you don't know the person and have established a relationship with them then do NOT add them to your network.
- Delete or mark as SPAM, emails, IM's or comments that illegitimately advertise, or otherwise violate the sites terms of service.
- Don't click on content in people profile as it may redirect you to somewhere you don't want to go and or infect your computer with malware.

Social Networking Remediation cont.

- Don't use third party add-ons. You can't validate these applications behavior, privacy policy, etc.
- Block anonymous access to your account.
- Shut off HTML and multimedia comments in your page.
- Report fake accounts so they can be removed. Community policing works!

Spyware/Adware/Badware/Greyware



Spy/Ad/Bad/Greyware

- Programs are shareware/freeware or arrive in spam, phishing, social network site, IM, etc.
- Trust not click not!
- Be in the habit of being skeptical!
- Research before you click or install.

Shareware/Freeware Threats

- Some shareware, Freeware are not technically free at all. Make sure to validate or research it first.
- They sometimes contain Adware, Spyware other programs that could damage your system, violate your privacy, cause data loss, or otherwise annoy you to tears.
- Ex. Wild Tanget, Bonzi Buddy, Weather Bug.
- Read the fine print.

Shareware/Freeware Remediation

- If you really need the program, buy from a respectable vendor.
- If you want a truly free program that has none of these problems - then get Free Software or Open Source Software.
- Read the fine print, EULA (End User License Agreement), Privacy Policy.

Other Threats

Other threats in cyberspace.

Cyber stalking

- Cyber stalking – misuse of information or communications technologies to harass another person, group or organization.
- Can involve threats, identity theft, monitoring, false accusations, damage to property or generalized harassment.
- Keep a digital log of all harassing communications.

Cyber stalking

- Lock the user out with your software settings. Block them.
- Report them to the website in question as a violation of the Terms of Service.
- Contact law enforcement if the problem persists.

Cyber stalking help

- WiredSafety.org
- National Center for Victims of Crime
- Working to Halt Online Abuse

Cyber bullying

- Targeted harassment or bullying using communication or information technology.
- Threats, pejorative labels, sexual remarks with intent to cause emotional/psychological distress.
- Lock the user out with your software settings. Block them.

Cyber bullying

- Report them to the website in question as a violation of the Terms of Service.
- Contact law enforcement if the problem persists.
- Kids should be encouraged to talk to their parents, guidance councilor, whoever they can trust.

Cyber bullying help

- Cyberbullying.org
- Cyberbullying.us
- Center for Safe & Responsible Internet Use

Parental Controls

General Advice for Parents
Parental Control Software

- Web Watcher -
- http://www.webwatcherkids.com/
- Spectator Pro – PC/Mac -
- http://www.spectorsoft.com/index.html
- Net Nanny -
- http://www.netnanny.com/
- General List -
- http://en.wikipedia.org/wiki/List_of_Content_Control_Software

General Advice for Parents
Parental Control

- Both Windows Vista and OS X have built in Parental Control.
- All of these tools are relatively effective but not perfect.
- Optimally you should additionally block at the network level.
- Make sure your firewall/wireless access point supports parental controls as well.

Data Remanence & Recycling/Disposing of Your Digital Devices

Your digital trash

- When you recycle your old computer or (any other digital device) don't do it without securely erasing the data.
- When you delete data its not gone. It can be easily recovered.
- Same goes for all other digital devices such as cell phones, smart phones, personal assistants, etc. that have personal information on it.
- USB Thumb drive/Key, CD/DVD.

Secure Erasure Applications

- Deleting files or even formatting a drive is not enough. Wipe them.
- Eraser(Windows) Open Source
- Dban (Live CD) Open Source
- ShredIt (Mac) Commercial

Secure Erasure Applications

- Microsoft Windows -
  - Eraser - http://www.heidi.ie/eraser/
  - Sysinternals - SDelete
  - East Tec – Eraser 2008
- Apple -
  - Apple – Secure Empty Trash/ Secure Erase
  - Smith Micro – Internet Cleanup
  - Apple OS X - SRM

Secure Erasure – Cell/Smart Phones

- Remember Cell/Smart Phones have much information on them:
- Applications, Appointments, Contacts, Email, Email Attachments, Log Information, Pictures, SMS Messages, Videos, Voice Recordings, Email Password, Banking Information, Wireless Networks, Company VPN Connections, Social Media Accounts/Passwords.
- Data may be on the SIM (subscriber identity module) card or MicroSD.

Secure Erasure – Cell/Smart Phones

- Remove and destroy the SIM (subscriber identity module) card.
- Check for delete or reformat instructions at:
  - Cellphone Manual
  - Cellphone Manufacturers Website
  - Cell Carriers Website
  - Cell Eraser Instruction Lookup

General Security Recommendations

Best Defense

Defense in depth – Using many layers, technologies, techniques and processes to help mitigate/reduce the risk of any one component of an information systems being compromised.

General Recommendations - Systems

- **Backup** your data to external disk, CD, DVD and or internet backup (encrypted in transit and at rest).
- **Patch** your system. Windows (Windows Update), Apple OSX (Systems Update). Set to auto update!
- **Patch third party applications**. Currently there is no common patch framework.
- **Least privilege**. Run as regular user not Administrator/Root. Windows (Standard User), OSX (Standard User).
- **Use strong passwords**. >8 alphanumeric characters, not a word in any language.

General Recommendations - Systems

- **Buy an Anti-malware scanner.** Make sure it covers ALL malware threats! Buy a new one annually.
- **Don't run EOL (End of Life) software**. Ex. Windows 95/ME or Apple OS 8/9.
- **Trust not, click not**. Trust nothing unless you can validate its source.
- **Don't read/open/click** on spam, phishing emails, IM's, websites, content that you do not know or trust.
- **Encrypt** where required on any sensitive data (especially portable devices).

General Recommendations - Networks

- Deploy both software/hardware firewall. Most anti-malware suites have a software firewall in them.
- Hardware firewalls from Netgear, Linksys, D-Link, are inexpensive and generally effective.
- Many of these offer “content control” or “parental control” features to block objectionable content, etc.
- Update your firmware. See vendor site for details.

General Recommendations – Public Access Wifi – at home

- If you have wireless at home don't use WEP, use WPA or WPA-2.
- Change the password to access web interface.
- Set up WPA/WPA2 PSK (pre shared key) at the very least with a very long PSK (>33 characters).
- Update your firmware (software on the device). See vendor site for details.

General Recommendations
Public Access Wifi

- Check with the hotel, conference, coffee shop for the valid SSID or network name.
- Validate that you are connected to the right network. Check the certificate.
- Don't connect to random access points for “free internet” as you may become a victim of cyber criminals.
- Use a VPN (Virtual Private Network) if the information resource you are connecting to is of any importance.

General Recommendations
Mobile Devices

- Mobile devices store a treasure trove of personal information.
- Applications, Appointments, Contacts, Email, Email Attachments, Log Information, Pictures, SMS Messages, Videos, Voice Recordings, Email Password, Banking Information, Wireless Networks, Company VPN Connections, Social Media Accounts/Passwords.

General Recommendations
Mobile Devices

- Setup password
- Encrypt where you can
- Use tracking software
- Anti-malware software (none on IPhone)
- Remote wipe

General Recommendations
Mobile Devices

- Apple iPhone 4 – Find my phone - Tracking and remote wipe.
- Lookout – Android, Windows Mobile, Blackberry. Anti-malware, backup, tracking & remote wipe.
- Kaspersky Mobile Security - Android, Windows Mobile, Blackberry, Symbian. Anti-malware, tracking & remote wipe.

Core Things To Do To Improve Your Security @ Home & Elsewhere

(Bare Minimum)

Get a Anti-malware Suite

The Word on Anti-Malware Suites

- Buy only from vendors that offer a comprehensive suite of tools to combat todays multitudinous threats.
- Anti-Malware suites are based on engine (brain) and DAT files (signatures).
- Behavior based are a step ahead because they look for anomalous (strange) behavior.
- An old anti-malware tool is a good as no anti-malware tool.

Anti-Malware Vendors

- Kaspersky
- Trend Micro
- Eset
- Symantec
- AVG
- Microsoft Security Essentials

Patch!

Patch Your Machine

- **Patch** your system. Windows (Windows Update), Apple OSX (Systems Update). Set to auto update!
- **Patch third party applications**. i.e. Browsers, Email Applications, Adobe Reader, Adobe Flash, Java, etc.
- Besides reducing your risks, your machine will be more stable.

Use Strong Passwords & Password Manager

On P@$sw0rDz~

- Choose strong passwords. >8 alphanumeric, not a word in any language. Use mnemonics or “memory device”.
- Strong passwords for you systems, websites, network devices, etc.
- There are also simple biometrics or a password management applications such as Robo Form or KeePass.
- http://www.us-cert.gov/cas/tips/ST04-002.html

Password Management Apps

- RoboForm - Windows, OSX, Mobile
- KeePassX - Open Source - Windows, OSX, Linux, Mobile, etc.
- KeePass - Open Source - Windows, OSX, Linux, Mobile, etc.
- 1Password - Windows, OSX, Mobile

Encryption Technologies Securing Your Data

~Especially Relevant for Portable Digital Devices~

Encryption Choices

- Both Windows Vista/7 (Depends on version i.e. Professional/Enterprise/Ultimate) and OS X support disk encryption.
- This provides encryption of the data at rest on your computer only.
- Microsoft BitLocker
- Apple File Vault

Encryption Choices Commercial

- PGP Desktop
- http://www.pgp.com/
- Veridis – Filecrypt
- http://www.veridis.com/
- Seganos Privacy Suite
- http://www.steganos.com/en/

Encryption Choices
Open source

- True Crypt
- http://www.truecrypt.org/
- GNU Privacy Guard
- http://www.gnupg.org/

Get a Hardware Firewall

Hardware Firewall

- Firewall feature exists in many forms in many devices.
- I.e. Wireless routers have generally have firewall features, some modems even have them now.
- NAT Firewall at the very least.

Hardware Firewall

- Netgear
- D-Link
- Linksys

Backup
Local & Online

Local Backup

- Microsoft & Apple have built in backup technologies for local backup.
- Get external USB hard drives for backing up local machine (local backup).
- External hard drives often have simple backup software.
- A local backup is NOT enough!

Online Backup

- Online backup offers additional protection to data loss.
- Ensure the data is encrypted in transit and at rest.
- Pre encrypt.

Online Backup

- Mozy
- Carbonite
- Dropbox
- IBackup

Conclusion

- Staying secure is a critical issue you can do something about.
- Its not all about technology. Its our choices and activities **and** the technology.
- Practice safe computing and create a safer Internet.

Big Thanks to:

- Cambridge Science Festival
- All of you!