Computer & Network Security Awareness
Objectives

• Malicious software can harm your computer
• Phishing and Identity Theft are easily avoidable; if it looks too good to be true, it is.
• Practice your Windows XP Operating System commands and learn your system
• Learn safe networking for you and your kids
• Take passwords seriously and consider using a password wallet (KeePass)
• When your network works, take the time to record its settings
• Consider the use of a hardware and personal software firewall (e.g. Belkin and Symantec)
Threats on the Internet

• Internet use is growing as is the number of incidents
  – An “incident” is an adverse event in an information system, and/or network, or the threat of the occurrence of such an event.
  – Incident implies harm, or the attempt to do harm

• Recorded incidents in the past:
  – 1995 – 1999, 18,300 incidents
  – 2000 – 2003, 294,037 incidents

• How many incidents were not reported?
What is Malicious Code?

- Malicious Code or Malware is attack software and includes:
  - Viruses, Worms, Trojans, Spyware
- Each attack software has specific characteristics, propagation techniques and adware
- Now, let’s review each type of Malware
What is a Virus?

- Programs designed to infect files or operating system & multiply by duplication
- Can spread without your knowledge
  - Needs a host or “living” program
- Considered “greatest damage” attack
  - Destroys operating systems
  - Deletes or corrupts files
  - Sends email to contacts listed in your address book
How Do Viruses Spread?

- Removable Media
  - USB thumb drives
  - Floppies / CD-ROMs
- Mobile Computers - Laptops
- Email Attachments
- Internet Downloads
  - Especially game sites
What kind of an environment is needed for short-range mobile phone viruses to spread rapidly?
A Few Well Known Viruses

• Melissa Virus
  – Spread so rapidly across Microsoft’s infrastructure that Microsoft actually shut down their email systems.

• The ILOVEYOU Virus
  – Was spread to computers all over the world in just six hours causing $7 billion in damage

• SoBig Virus
  – Replicated itself 1,000,000 times in 24 hours.
Antivirus Software

• How does antivirus software work to protect us?
  – Each virus has its own characteristics just like your handwritten signature
  – Antivirus (AV) identifies and tracks virus signatures,
  – Detects, isolates and repairs any damage

• New Viruses, Worms and Trojans

• Solution: Behavioral or Heuristic Antivirus
  – Does not rely on signatures
  – Relies on artificial intelligence technology to detect viruses
  – Seeks abnormal patterns of behavior
Antivirus Updates

- Antivirus software must have up-to-date signatures for maximum protection
- Update your system everyday
  - Most antivirus products can be configured to perform automatic updating
- Antivirus programs will quarantine, delete, or fix infected files found
- Think you have a virus?
  - Update your software and perform a scan
Software Patches

• What are software patches?
  - Patches fix weaknesses in operating systems due to programming errors

• How often do I need to patch?
  - Daily or use WinXP automatic update whenever possible to download (and install) immediately upon release

• Potential risks of patching
  - Review severity of problem; patch may need installation immediately
What is a Worm?

• A virus requires some action on the part of the user such as opening an attachment
• However, a worm runs independently and can replicate a working copy of itself to hosts across a network
• A worm takes advantage of weaknesses in your computer’s networking services and breaks in
• A worm probes the network for other vulnerable computers
A Few Well Known Worms

- **Slammer (Sapphire Worm)**
  - Probed 55+ million hosts per second and infected 90+ % of vulnerable hosts in 10 minutes; $2 billion in damage

- **Code Red**
  - Launched Buffer Overflow attack and infected more than 250,000 systems in just 9 hours

- **MS Blaster - Remote Procedure Call (RPC)**
  - Launched Denial of Service (DOS) attacks against Microsoft Windows Update Web site.
What is a Trojan?

- A Trojan is a program that disguises itself as legitimate, but contains hidden and often malicious functionality.
- The most common way they spread is on porn picture sites. Users click on picture after picture and do not notice the executable software (.exe) files.
- Often included in Internet downloads, pop-ups, or emails.
A Few Well Known Trojans and How They Work

- **SubSeven and BackOrifice**
  - Allow a hacker to gain remote control over a computer
  - Can view your screen, control your mouse, send popup messages, turn Web cam or microphone on or off to see and hear you
  - Special “bot net” software allows hacker to control thousands of Trojans

- **SoBig-E Variants**
  - Mass-mailing Trojan included in later versions of SoBig virus

- **Rbot-GR**
  - Malicious program enables Web cams
  - New Rbot worms appear on the Internet almost every day
What is Spyware?

- Spyware software covertly gathers user information through the user’s Internet connection without their knowledge, usually for advertising purposes.
  - Spyware monitors all activity, even keystrokes, names, passwords, and credit card numbers which can introduce vulnerabilities
- Webroot and Earthlink found over 26 spyware traces on computers over a 6 month period
  - 2 million scans indicated 55 million instances of spyware
- National Cyber Security Alliance
  - June 2003 estimates 9 out of 10 PCs run spyware
Spyware – Why Be Concerned?

• Spyware takes form as tracking cookies, installed applications, or software update programs
• Can create sluggish PC performance, strange emails, and unintended web sessions
• Can correlate web surfing habits, online transactions, email addresses and scan hard drive for personal information
Anti-Spyware

- Anti-Spyware removes spyware similar to antivirus
  - Identifies and tracks signatures
  - Will not detect altered signatures
- Antivirus and Anti-Spyware
  - Best protection is provided by using two separate software processes
- Some Anti-Spyware software is free or very affordable
  - Free Anti-Spyware software: Lavasoft Ad-aware, Spybot Search & Destroy, Microsoft Anti-Spyware
Know if You’ve Been Hacked

• Be alert for signs of strange or unanticipated behavior
  - Strange emails you didn't send
  - Applications YOU did not install
  - Pop-up ads when you are not browsing the Web
  - Odd behavior, you cannot explain

• Take action!
  - Update and run Antivirus and Spyware removal software
  - Update Operating System and installed applications

• If you are unsure about the integrity of your system, unplug it
  - Scans and updates may not remove every infection
  - System backup or reinstall may be needed to fully recover
You’ve Been Hacked…
What Do You Do?

If your PC is hacked, it is crucial to limit or NAIL your financial exposure quickly:

- **Notify**: Technical support, financial institutions, credit card companies
- **Action**: Monitor credit report, change all passwords, place fraud alert on credit report
- **Inspect**: Use a firewall and enable logging to track activity
- **Law Enforcement**: File a police report, contact your state’s Attorney General, report identify theft to FTC
Defending Yourself from Malware

- Home computers have become a common target
- Take steps to protect yourself from loss, damage or attack
  - Operating Systems, email Awareness, Backups, Antivirus, Anti-Spyware, Firewall software, Software Patches and Strong Passwords
- As we progress we will discuss how to defend yourself against the dangers lurking on the Internet.
Emails and Attachments

• July 2004, MSNBC research found 1 of 3 users were unable to recognize fake email
• Email communication use is wide-spread
  – Attachments can contain viruses, worms, and Trojan horses
• Dangers can be hidden in emails even without attachments
• Don’t know the sender? Don’t open it!
• If you receive mail with an attachment from someone you know, call and ask if they sent an attachment before opening it
• With Outlook, you can right click and delete the email and attachment safely
Be Wary of Email W/O Recipient List (i.e. To: or CC:)

While we are at it, be wary of email that promises something for something, if it sounds too good to be true; it is.

Dear Sir,

I have a female client who is interested to invest in your country on partnership basis.
Examine Email Headers to Detect Spoofed Email

View Options or with Outlook 2003 in reading pane: right click, Options

Email Headers
**RCPT TO:** is Destination Mailbox  
**TO:** is Display Mailbox

The ‘Destination’ and the ‘Display’ mailboxes do NOT match and they should.

```
MAIL FROM: sender@somehost.com
RCPT TO: faber@sans.org
DATA
From: spoof@someotherhost.com
To: anyone@anyhost.com
Subject: Test Mail
Date: Mon, 18 Jul 18:00:00 +0100
MIME-Version: 1.0
Content-Type: text/plain
Hello, world
```
Return Path and From

The ‘Return-Path’ and the ‘From’ do NOT match and they should.

Return-Path: <sender@somehost.com>
Delivered-To: faber@mx1.sans.org
Received: 18 Jul 2005 15:52:43 -0400 (EDT)
Received: from mymailserver.net
    by mua.mymailserver.net
    for <faber@sans.org>; Mon, 18 Jul 15:52:43 -0400 (EDT)
From: spoof@wellsfargo.com
To: anyone@anyhost.com
Subject: Test Mail
Date: Mon, 18 Jul 18:00:00 +0100
MIME-Version: 1.0
Content-Type: text/plain
What is Phishing?

- Attempts to steal personal identity and financial information
- Generally, there are two components to attempts
  - Social engineering to trick the unsuspecting user
  - Technical trickery to make them think a fraudulent web site is a trustworthy one like a bank’s
- Common Targets
  - eBay
  - PayPal
  - Banks
  - Credit Unions
  - Credit Cards

Computer & Network Security Awareness - © 2006 SANS
Phishing Example 1

**Date:** Tue, 12 Jul 2005 23:03:22 -0700  
**From:** "Bank Of The West" <security@bankofthewest.com>  
**Subject:** Security Update

Dear Bank Of The West Client,

To provide our customers the most effective and secure online access to their accounts, we are continually upgrading our online services. As we add new features and enhancements to our service, there are certain browsers versions which will not support these system upgrades. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

In order to further protect your account, we have introduced some new important security standards and browsers requirements.

Bank Of The West security custom require that you test your browser new...
Phishing Example 1:
A Closer Look - This Site is Fake

Protect Yourself Against Financial Fraud!
At the Bank of the West, we take the matter of protecting your financial information seriously. We recognize and respect your right to privacy when it comes to your personal financial information. Please attend our request to protect against scam
Phishing Example 2: Your Account Information Has Been Received…
Phishing Example 3

From: Lasalle Bank [unlock@lasallebank.com]
To: press@sans.org
Cc: 
Subject: Unlock your ACCOUNT

Dear LaSalle Bank customer,

We recently noticed one or more attempts to login into your LaSalle Bank online banking account from a suspicious IP address and we have evidence of login failures.

If you recently logged into your account while traveling to a foreign country, or we believe that the login attempts may have been made by unauthorized persons.

However if you are the rightful owner of the account, click the following link to verify the account in digits of your Social Security number as a password.

https://lasallebank.com/online/secure_account.jsp

The login attempt was made from: http://202.145.52.165/www.lasallebank.com/

IP: 82.89.87.55
ISP Host: host55-87.pool8289.interbusiness.it

IF YOU CHOSE TO IGNORE OUR REQUEST, WE HAVE NO CHOICE BUT TO TEMPORARILY SUSPEND YOUR ONLINE BANKING ACCOUNT

URLs do not match

You don’t even have an account with this bank!

© SANS Institute 2006, Author retains full rights.
Phishing Example 4

Dear Wells Fargo customer,

As you may already know, we at Wells Fargo guarantee your online security and partner with you to fight fraud. Due to the newly introduced fraud protection, we urge you to go through the 2 steps Wells Fargo Account Conversion procedures. The operation involves logging into your account at:


After completing the operation, you will be informed whether or not your account has been committed with Comprehensive Quarterly.

Thank you for working with us in combating online fraud and also, for choosing Wells Fargo as your Financial Institution.

URLs do not match.
Phishing Example 5

To fully restore your account, please take the following steps:

1. Login to your BOK Personal Banking account.
2. Review your account history for any unauthorized activity.

To get started, please click the link below:

[Login]

Grammar Error: Login takes you to a game site.
Sehr geehrter Kunde,


Im Zusammenhang mit dem Obenerwähnten bitten wir Sie, eine spezielle Form der zusätzlichen Autorisation auszufüllen.

Diese Maßnahmen werden ausschließlich zur Sicherung der Interessen von unseren Kunden getroffen.

Danke für die Zusammenarbeit,
Administration der Postbank Online Banking
Netcraft Toolbar Helps Warn You About Phishing Web Sites
Phishing Credit Card Scams

Secured Credit Card Marketing Scams

ANYONE CAN QUALIFY FOR A MAJOR CREDIT CARD!
Separated? Divorced? Bankrupt? Widowed?
BAD CREDIT? NO CREDIT? NO PROBLEM!
900-555-1111

* Make the call NOW and get the credit you deserve!
  * Even if you’ve been turned down before, you owe it to yourself and your family.
  * Your major credit card is waiting.
Ignore Credit Card
“Protection” Offers by Email

• Federal Trade Commission Web page says:
  – “If you did not authorize it, do not pay it”
  – “Liability limited to $50 per card”

• Responding to this email offer may disclose account information to scam artist
What is Identity Theft?

- Identity theft is the use of another person’s personal information (ex. name, social security number, credit card number, passport) without that person’s knowledge.
- A Gartner study found that approximately 7 million people were victims of identity theft in 2003.
- The Consumer Sentinel received over 635,000 consumer fraud complaints in 2004. Of those complaints, 39% were identity theft complaints.
Identity Theft

- Lighter side -
  
  • In 1938, wallet maker used a sample “SSN” card to show that such a card fit in the wallet.
  
  • The card was fake, however the SSN number was NOT!

![Social Security Card](image-url)
Over 40,000 People Used That as Their Own Social Security Number

“They started using the number. They thought it was their own. I can’t understand how people can be so stupid. I can’t understand that.”

– Mrs. Hilda Schrader Whitcher

http://www.ssa.gov/history/ssn/misused.html
eBay Statistics

- 168 million registered users worldwide
- eBay estimates that more than 430,000 people in the United States make their living selling items on the site
- “Any given day...millions of items sold”
- Everything from boats, cars, art, electronics, to professional services (web design, accounting, etc.)
eBay Scams

• Non-delivery or Misrepresentation
• “Triangulation” – Seller dealing in goods bought with stolen identities/CC numbers. Buyer purchases stolen goods without knowing
• Be aware of eBay’s rules and policies to protect you
• Hidden Fees for shipping, handling, etc.
• Practice careful bidding!
A bit misleading, the price is in GBP (United Kingdom Pounds). Depending on the dollar's strength, this could be a deal or you could pay more than you expected for this item.

**READ THE FINE PRINT!!!!**

This item costs 65 GBP to ship and had a mandatory requirement of 15 GBP for insurance. Total cost is 109.99 GBP or 193.60 US Dollars. Not quite the deal you thought.

Seller has built a reputation by selling many products and has a positive feedback rating of 98.3%.

© SANS Institute 2006, Author retains full rights.
File an Online Fraud Complaint Report

- Submitting an eBay online Fraud Complaint provides eligibility for Fraud Protection coverage, [http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage](http://crs.ebay.com/aw-cgi/ebayisapi.dll?crsstartpage)
- An eBay Fraud Protection Claim must be filed separately within 90 days of close of listing.
  - Coverage available to winning bidders/buyers for purchases made on eBay via an eBay listing only
  - Claim must be made for each item won
  - Copy of complaint is forwarded to Federal Trade Commission (FTC)
- If claim is approved, maximum coverage is $200 less $25 processing costs.
- You may also file complaints with:
  - Internet Fraud Complaint Center, [http://www.ifccfbi.gov/index.asp](http://www.ifccfbi.gov/index.asp)
What is a Web Browser?

• Software used to browse the World Wide Web
• Some examples of web browsers:
  – Microsoft Internet Explorer, Mozilla Firefox, Netscape Navigator, Safari, Opera
• Browser software must always be kept up-to-date regardless of type
Web Browser Security

- Most commonly used and exploited web browser is Microsoft Internet Explorer
- Firefox is second most commonly used and has been exploited to a lesser degree
- Most browser exploits require “clicking”
- Be aware of patched, unpatched, and behavior-based vulnerabilities
- Maintain a secure environment; become an educated user
Microsoft Internet Explorer (IE) Browser Weakness

- Most problems are due to a programming language called Active X
- Also, users often surf the web as “Administrator” which has power to install software
- Start -> My Computer (right click) -> Manage, Users and Groups, select yourself, double click, Member of
- Sample vulnerability: Status Bar
  - Displays Web site link in status bar that takes you to a different Web site
IE’s Protected Storage Isn’t
Add-ons are programs that extend the capabilities of your Web browser. Some add-ons can interfere with the operation of your browser. You can disable, enable, or update add-ons. Disabling an add-on might prevent some Web pages from working.

### Name
- **AcroIEHprObj Class**: Adobe Systems, Incorporated
- **AcroIETFoolbarHelper Class**: Adobe Systems, Incorporated
- **Adobe PDF**: Adobe Systems, Incorporated
- **CNavExtBho Class**: Symantec Corporation
- **DriveLetterAccess**: (Not verified) Sonic Solutions
- **Norton AntiVirus**: Symantec Corporation
- **Real.com**: Symantec Corporation
- **Spybot-SD Internet Explorer**: Safer Networking Ltd.
- **Sun Java Console**: (Not verified) Sun Microsystems
- **Windows Messenger**: Symantec Corporation

### Status
- **Enabled**: Adobe Systems, Incorporated
- **Enabled**: Adobe Systems, Incorporated
- **Enabled**: Adobe Systems, Incorporated
- **Enabled**: Symantec Corporation
- **Enabled**: (Not verified) Sonic Solutions
- **Enabled**: Symantec Corporation
- **Enabled**: Symantec Corporation
- **Enabled**: Safer Networking Ltd.
- **Enabled**: (Not verified) Sun Microsystems
- **Enabled**: Symantec Corporation

### Type
- **Browser Helper Object**: Adobe Systems, Incorporated
- **Browser Helper Object**: Adobe Systems, Incorporated
- **Toolbar**: Adobe Systems, Incorporated
- **Toolbar**: Adobe Systems, Incorporated
- **Browser Helper Object**: Symantec Corporation
- **Browser Helper Object**: (Not verified) Sonic Solutions
- **Browser Helper Object**: (Not verified) Sun Microsystems
- **Browser Helper Object**: Safer Networking Ltd.
- **Browser Extension**: Symantec Corporation
- **Browser Extension**: (Not verified) Sun Microsystems

### Select an add-on from the list above to perform the following actions:

**Settings**
- To disable an add-on, click it and then click Disable. To update an ActiveX control, click it and then click Update ActiveX.

**Enable**

**Update**
- Click here to update this add-on.

**OK**
Mozilla Firefox Browser

- Firefox does not support Microsoft ActiveX
- Sample vulnerability: Spoofed Link in early version
  - “Save Link As” function will save wrong destination link
Keep Your Browser Patched

• Run Windows Update automatically
• Run Office Update - office applications
• To download Firefox updates
  - Check your current version
    • Help → About Mozilla Firefox
  - Check for Software updates
    • Tools → Options → Advanced: Scroll down to “Software Update” and click “Check Now”
Keep Your Browser In Check

• Test to ensure patches have been applied, by:
  – Attempting vulnerability exploit after patch
Protecting Children

Tools like K9 can prevent kids from surfing offensive or dangerous Web sites.

Computer & Network Security Awareness - © 2006 SANS
Chat, Myspace.com, etc.

Kids can give too much information away. Also, the new trend of blogging and posting personal photos can attract predators. This photo is shot from above and the subject appears not to be alert. What kind of person will this appeal to?
Trouble Signs for Kids

- Computers used by kids should never be in a private place, be concerned if they ask for the computer to be in their bedroom
- Too much time spent on computer
- Irritated if not able to access Internet, or other changes in behavior
- They touch the keyboard if you enter the area: `alt tab` switches to last application used, `alt F4` closes an application immediately
- Mysterious about where they are going
Online Music Downloads and Software Piracy

• Be aware of illegal downloading of music or pirated copies of software
• Digital Millennium Copyright Act (DMCA), took effect in 1998 to protect CDs, DVDs and other digital media
• Ensure you are downloading music legally, over $70M in penalties reportedly collected
Think Before You Click…

• Change your web browsing habits to:
  – Prevent unknown installed malware
  – Prevent phishers from obtaining your personal information

• Create a list of general guidelines for you and other end users’ reference

• Apply your new browsing behavior
Principle of Least Privilege

- You are far safer not surfing the Web as the Windows Administrator since the Administrator has the right to install software.
- Mac Operating Systems (OS X) requires Administrative privileges and password.
- Windows users choose “Run As” to enter administrative credentials.
- DropMyRights software launches your browser with minimal privilege - Demonstration.
Firefox Software Install Option

![Firefox Options Window]

- Block Popup Windows
- Load Images
- Enable Java
- Enable JavaScript
Operating Systems (OSes)

- Modern OSes are ‘user’ friendly
  - Example, Windows XP Professional provides: File sharing, printer sharing, Internet firewalling, Internet connection sharing, personal web server, remote desktop connectivity, home movie creating, just to name a few services

- Services are features accessible to non-local users

- Your OS can be too friendly
  - Protected Storage Explorer
  - What sensitive information is stored about you?
NET SHARE

Always check NET SHARE before taking a computer on travel.
Net Statistics Workstation

C:\Documents and Settings\Owner>net statistics workstation
Workstation Statistics for \CRASH6

Statistics since 8/22/2005 7:32 AM

Bytes received 0
Server Message Blocks (SMBs) received 3
Bytes transmitted 0
Server Message Blocks (SMBs) transmitted 0
Read operations 0
Write operations 0
Raw reads denied 0
Raw writes denied 0

Network errors 0
Connections made 0
Reconnections made 0
Server disconnects 0

Sessions started 0
Hung sessions 0
Failed sessions 0
Failed operations 0
Use count 0
Failed use count 0

The command completed successfully.
Net Accounts

C:\Documents and Settings\Owner>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 42
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.

C:\Documents and Settings\Owner>
Net Users

C:\Documents and Settings\Owner>net users
User accounts for \CRASH6

-------------------
Administrator       Guest
Lynn               SUPPORT_388945a0
HelpAssistant

The command completed successfully.

C:\Documents and Settings\Owner>
Net Localgroup

```
C:\Documents and Settings\Owner>net localgroup
Aliases for \CRASH6

*Administrators
*Backup Operators
*Guests
*HelpServicesGroup
*Network Configuration Operators
*Power Users
*Remote Desktop Users
*Replicator
*Users
The command completed successfully.
```

C:\Documents and Settings\Owner>
Genuine Windows Validation - Windows Piracy Check

http://www.microsoft.com/resources/howtotell/ww/windows/default.mspx
Environmental Controls

- Temperature should range between 41-80 degrees °F
- Humidity range between 20-60%
  - High: cause rusting
  - Low: cause static electricity
- Dust affects computer fans
- Food, drinks and smoke causes damage
- Uninterruptible Power Supply
Clean Power

- Computers need a source of clean power
  - Constant and level flow of electricity
- Danger = power surges, spikes, brownouts
  - Brownouts – Short term drop in voltage
  - Blackouts – Total loss of power
  - Spikes – Instantaneous massive boost in voltage
  - Surges – Momentary rise in voltage
  - Noise – Electromagnetic fluctuation
Case Study

- A surge protector can save your computer and invested money.
- A computer not plugged into a surge protector can result in loss of motherboard.
- Never plug in your computer without some protection.
- Ensure your product is tested, has fuse protection and clamping voltage for the best protection against surges.
File System Integrity

C:\> chkdsk /f

![ CHKDSK command output ]
Start > All Programs > Accessories > System Tools > Disk Defragmenter
Belarc can tell you a lot about your computer including the programs installed - www.belarc.com

Computer Profile Summary
Computer Name: D8826v71 (in MSHOME)
Profile Date: Monday, December 05, 2005 4:41:43 PM
Advisor Version: 7.0t
Windows Logon: snorthcutt

The license associated with the Belarc Advisor product allows for free personal use only. Use on multiple computers in a corporate, office, or school setting is prohibited. See the license agreement for details. The information on this page was created locally on your computer by the Belarc web server. Click here for more info.
Backups

• Protects against computer crashes, theft, loss of important data
• Create a regular schedule of backups
• WinXP Pro provides a backup utility called Ntbackup.exe, that can back up your settings or the entire disk, **Start - Run -> ntbackup**
• Burning a CD or DVD of important information can be quicker than configuring backup software
• External Hard Drives can backup your entire system
Usernames and Passwords

- How do I effectively choose, use, and protect my password?
- Your username and password authenticates your log in
- Your password is your first line of defense
- Your password is also your last line of defense if firewalls fail
Weak Passwords

• What constitutes a weak password?
  - Contains less than eight characters
• Examples of weak passwords include:
  - Username +1
  - Cowboys or Redskins
• Take a moment now to evaluate your password characteristics
• The following slide will help you take steps to strengthen your password
Strong Passwords

• What constitutes a strong password?
  – Length and several character types
  – 12 characters, mixture of upper/lower case letters, numeric and punctuation symbols

• Meet minimum length

• Use upper and lower case letters and numbers

• Use special symbols like punctuation

• Use song titles or catch phrases strengthened by one or more of the above
# Longer Passwords are Harder to Break

<table>
<thead>
<tr>
<th>Password Basis</th>
<th># Of Options</th>
<th># Of Possibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>English words</td>
<td>~ 234,000</td>
<td>~ 234,000</td>
</tr>
<tr>
<td>4 Case-insensitive letters</td>
<td>26 ^ 4</td>
<td>456,976</td>
</tr>
<tr>
<td>6 Case-insensitive letters</td>
<td>26 ^ 6</td>
<td>308,915,776</td>
</tr>
<tr>
<td>8 Case sensitive letters</td>
<td>52 ^ 8</td>
<td>53,459,728,531,456</td>
</tr>
<tr>
<td>10 Case sensitive letters with numbers</td>
<td>62 ^ 10</td>
<td>839,299,365,868,340,224</td>
</tr>
<tr>
<td>12 Case sensitive letters with numbers and punctuation</td>
<td>95 ^ 12</td>
<td>540,360,087,662,636,962,890,625</td>
</tr>
</tbody>
</table>
Cain, NTLMv2

• Cain from www.oxid.it is a popular password cracker
• The best way to protect your computer is to disable Lan Man hashes
• Use regedit to allow NTLMv2 only
Password Management

• Should I write it down?
  – Try not to write down a password
  – Write “hints” instead
  – Consider KeePass password wallet
Multiple Account Passwords

- Exercise separate passwords for separate accounts
- If a hacker successfully compromises your password; would he have access to all of your accounts?
- It is vital to select unique passwords for each account
- Why would “qwerty” be a poor choice of password?
Wireless Basics

• Most wireless products are based on industry standards.
• People use wireless Local Area Network (LAN) technology for many different purposes.
  – Mobility
  – Low Implementation Costs
  – Installation and Network Expansion
  – Scalability
  – Inexpensive Solution
Wireless Networking

- Popularity of Wireless Local Area Networks (WLAN) use is growing due to convenience, mobility and affordable prices.
- If you are using DSL and wireless for business consider a backup DSL from a different provider.
- Obtaining and downloading the latest patches and firmware for all your wireless network hardware is very important.
- Be aware that 2.4 GHz phones, microwaves and some baby monitors may disrupt wireless services temporarily due to the similar wave range of most wireless devices.
Wireless Security

Common security features now include:

- **Wi-Fi Protected Access (WPA)** - or Wired Equivalent Privacy (WEP) allow you to give your network a password required for access
- **Pre Shared Key (PSK)** mode
  - Strength of WPA-PSK is based on the PSK used
- **WPA2**: WPA that uses Advanced Encryption Standard (AES)
  - Will probably require new hardware to support the encryption
Wireless MAC Filter
Standard-Based Technology

• Most common Wireless Broadband Routers utilize the new 802.11g standard with a data rate up to 54Mbps.

• Most 802.11g wireless broadband routers are backwards compatible with 802.11b devices, but if both b and g devices are present, the network switches to b protection mode, slowing everyone down.
Installation Considerations

• Keys to maximizing wireless range basic guidelines:
  - Keep the number of walls and ceilings between your wireless router and other network devices to a minimum.
  - Be aware of the direct line between network devices.
  - Building materials can impede the wireless signal.
  - Keep your product away from electrical devices.
What Networks Am I Connected To?
Networking Using Wizard

Welcome to the Network Setup Wizard

This wizard will help you set up this computer to run on your network. With a network you can:

• Share an Internet connection
• Set up Windows Firewall
• Share files and folders
• Share a printer

To continue, click Next.
Windows XP
Address Resolution Protocol - ARP

If there are no ARP entries, your network interface is not talking to your network.
Route Print - Run This While Your Network is Running Properly and Store in a File for Troubleshooting

C:\Documents and Settings\Owner>route print

Interface List
0x1: 0e 35 93 56 b8 0e 35 93 56 b8 MS TCP Loopback interface
0x2: 00 0e 35 93 56 b8 Intel(R) PRO/Wireless 2200BG Network Connection
- Packet Scheduler Miniport
0x3: 0e 0b 5b 3d cd Intel(R) PRO/1000 MT Desktop Adapter - Packet Scheduler Miniport

Active Routes:
Network Destination  Netmask  Gateway      Interface     Metric
   0.0.0.0          0.0.0.0  192.168.1.1  192.168.1.101  25
   127.0.0.0       255.0.0.0  127.0.0.1  127.0.0.1     1
  192.168.1.0     255.255.255.0  192.168.1.101  192.168.1.101  25
  192.168.1.101 255.255.255.255  127.0.0.1  127.0.0.1     1
  192.168.1.255 255.255.255.255  127.0.0.1  127.0.0.1     1
  224.0.0.0       240.0.0.0  192.168.1.101  192.168.1.101  25
  224.0.0.0       240.0.0.0  127.0.0.1  127.0.0.1     1
  255.255.255.255 255.255.255.255  192.168.1.101  192.168.1.101  3
  255.255.255.255 255.255.255.255  192.168.1.101  192.168.1.101  1

Default Gateway: 192.168.1.1

Persistent Routes:
None

C:\Documents and Settings\Owner>route print > routeaug2005.txt

Computer & Network Security Awareness - © 2006 SANS
Assigning a Static IP Address

- Connect using:
  - Intel(R) PRO/Wireless 2200BG Netw
- This connection uses the following items:
  - AEGIS Protocol (IEEE 802.1x) v2.2.1.0
  - WLAN Transport
  - Internet Protocol (TCP/IP)
- Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Ipconfig /release /renew
Needed if There are Two Computers with the Same IP Address

C:\Documents and Settings\Owner>ipconfig /renew *wireless*

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

- Connection-specific DNS Suffix .: dsl-verizon.net
- IP Address . . . . . . . . . . . . . . : 192.168.1.101
- Subnet Mask . . . . . . . . . . . . . : 255.255.255.0
- Default Gateway . . . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection:

- Media State . . . . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Owner>
Ipconfig /all
Very Handy When Troubleshooting Your Computer’s Networking Situation
Netstat -ao
One Way to See Your Listening Processes and Established Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>CRASH6:epmap</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>1296</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:microsoft-ds</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:1027</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>1916</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:1028</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>780</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:1063</td>
<td>localhost:1064</td>
<td>ESTABLISHED</td>
<td>3232</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:1064</td>
<td>localhost:1063</td>
<td>ESTABLISHED</td>
<td>3232</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2025</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>616</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2110</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>616</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2143</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>616</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2143</td>
<td>localhost:2619</td>
<td>ESTABLISHED</td>
<td>616</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2619</td>
<td>localhost:2143</td>
<td>ESTABLISHED</td>
<td>1004</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:netbios-ssn</td>
<td>CRASH6:0</td>
<td>LISTENING</td>
<td>4</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2615</td>
<td>webmail.sans.org:5223</td>
<td>ESTABLISHED</td>
<td>560</td>
</tr>
<tr>
<td>TCP</td>
<td>CRASH6:2618</td>
<td>charlie1.giac.net:22</td>
<td>ESTABLISHED</td>
<td>616</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:microsoft-ds</td>
<td><strong>:</strong></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:isakmp</td>
<td><strong>:</strong></td>
<td></td>
<td>1036</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1025</td>
<td><strong>:</strong></td>
<td></td>
<td>488</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1051</td>
<td><strong>:</strong></td>
<td></td>
<td>1528</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1067</td>
<td><strong>:</strong></td>
<td></td>
<td>1528</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1069</td>
<td><strong>:</strong></td>
<td></td>
<td>1528</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1070</td>
<td><strong>:</strong></td>
<td></td>
<td>1528</td>
</tr>
<tr>
<td>UDP</td>
<td>CRASH6:1072</td>
<td><strong>:</strong></td>
<td></td>
<td>1528</td>
</tr>
</tbody>
</table>
FPOR-T – The Best Tool to Map Listening Ports to the Program Doing the Listening

C:\Documents and Settings\Administrator\My Documents\Computer\Foundstone\Fport-2.0\fport
FPOR-T v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

<table>
<thead>
<tr>
<th>Pid</th>
<th>Process</th>
<th>Port</th>
<th>Proto</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1200</td>
<td></td>
<td>135</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>1200</td>
<td>System</td>
<td>139</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>1200</td>
<td>System</td>
<td>445</td>
<td>TCP</td>
<td></td>
</tr>
<tr>
<td>608</td>
<td>ccApp</td>
<td>1027</td>
<td>TCP</td>
<td>C:\Program Files\Common Files\Symantec Shared\ccApp.exe</td>
</tr>
<tr>
<td>3032</td>
<td></td>
<td>1031</td>
<td>TCP</td>
<td>C:\Program Files\Exodus\Exodus.exe</td>
</tr>
<tr>
<td>1272</td>
<td>putty</td>
<td>1042</td>
<td>TCP</td>
<td>C:\Program Files\PuTTY\PuTTY\putty.exe</td>
</tr>
<tr>
<td>3212</td>
<td>thunderbird</td>
<td>1043</td>
<td>TCP</td>
<td>C:\Program Files\Mozilla Thunderbird\thunderbird.exe</td>
</tr>
<tr>
<td>3212</td>
<td>thunderbird</td>
<td>1044</td>
<td>TCP</td>
<td>C:\Program Files\Mozilla Thunderbird\thunderbird.exe</td>
</tr>
<tr>
<td>3212</td>
<td>thunderbird</td>
<td>1071</td>
<td>TCP</td>
<td>C:\Program Files\Mozilla Thunderbird\thunderbird.exe</td>
</tr>
<tr>
<td>3212</td>
<td>thunderbird</td>
<td>1080</td>
<td>TCP</td>
<td>C:\Program Files\Mozilla Thunderbird\thunderbird.exe</td>
</tr>
</tbody>
</table>

Computer & Network Security Awareness - © 2006 SANS
Tracert – How to Find the Path From Your Computer to a Server on the Internet

```
C:\Documents and Settings\Owner>tracert www.sans.org
Tracing route to www.sans.org [64.112.229.132]
over a maximum of 30 hops:

1    3 ms    1 ms    1 ms 192.168.1.1
2    20 ms   20 ms  18 ms  4.16.84.1
3    20 ms   18 ms  18 ms  4.24.5.237
4    21 ms   20 ms  21 ms  ge-1-3-0.mpls1.Honolulu2.Level3.net [4.68.124.22]
5    83 ms   82 ms  82 ms  as-2-0.bbr2.SanJose1.Level3.net [4.68.128.157]
6    83 ms   81 ms  84 ms  so-7-0-0.edge1.SanJose1.Level3.net [209.244.3.14]
7    83 ms   84 ms  82 ms  Qwest-Level3-oc48.SanJose1.Level3.net [209.245.1.46,230]
8    83 ms   81 ms  84 ms  svx-core-02.inet.qwest.net [205.171.214.137]
9    85 ms   84 ms  85 ms  svi-core-03.inet.qwest.net [205.171.14.81]
10   111 ms  111 ms 110 ms  pdx-core-01.inet.qwest.net [205.171.130.91]
11   115 ms  116 ms 116 ms  egn-core-02.inet.qwest.net [205.171.5.130]
12   114 ms  113 ms 114 ms  eug-edge-02.inet.qwest.net [205.171.150.22]
13   116 ms  116 ms 116 ms 207.109.243.74
14   110 ms  110 ms 111 ms 64-112-224-3-ips-eug-or-core02.tcpipservices.net [64.112.224.3]
15   114 ms  112 ms 110 ms 64-112-227-69-ips-eug-or-lb01-2.tcpipservices.net [64.112.227.69]
16  maverick32.sans.org [64.112.229.132] reports: Destination host unreachable
```
Ping – The Ideal Way to See if Another Computer is Working, but Personal Software Firewalls May Interfere

C:\Documents and Settings\Owner>ping www.sans.org

Pinging www.sans.org [64.112.229.132] with 32 bytes of data:

Reply from 64.112.229.132: Destination host unreachable.
Reply from 64.112.229.132: Destination host unreachable.
Reply from 64.112.229.132: Destination host unreachable.
Reply from 64.112.229.132: Destination host unreachable.

Ping statistics for 64.112.229.132:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Owner>
What is a Firewall?

• A traffic cop. Personal hardware and software firewalls monitor and control traffic allowed in or out of your network.
• The goal is to keep hackers and malicious code away (viruses, worms, trojans).
• Two types of firewalls – hardware & software.
Hardware Firewalls

• A device between the Internet and your network, the simplest example is a DSL router

• Protect networks by one of two methods:
  - Packet Filtering hardware firewalls block traffic initiated from the Internet to your network (e.g. DSL router)
  - Stateful Inspection hardware firewalls maintain information about who started conversations, generally if the computers inside your network initiate, it is considered OK
Software Firewalls

- Software-based firewalls use computer’s resources and is usually cheaper
- Examples of Software Firewalls
- Only run one software firewall at a time
Symantec Software Firewall Set Up

No security issues are detected on your computer

- Norton AntiVirus is on
- Norton Internet Security is on
- Windows Automatic Updates is on

Do not display Windows Security Center (Recommended)

Open LiveUpdate | Learn more about the latest security information | About

Close
Symantec Firewall Setting

[Image of the Symantec Firewall interface]

Computer & Network Security Awareness - © 2006 SANS
Symantec Program Control

Look for programs that you do not recognize.

Then use Google to see if they are unnecessary or malicious.
ZoneAlarm Software Firewall
ZoneAlarm Configuration

Firewall
The firewall protects you from dangerous traffic. It has two Zones:

Internet Zone: For protection from unknown computers.

Trusted Zone: For sharing with trusted computers.

The Internet Zone contains all of the computers on the Web by default. Use the Zones tab to add computers to the Trusted Zone.

For more advanced control of Zones, including networking, privacy controls, and creation of a Blocked Zone, choose ZoneAlarm Pro.

Internet Zone Security

High: Stealth mode. Your computer is hidden and protected from hackers. Sharing is not allowed. This setting is recommended for the Internet Zone.

Trusted Zone Security

Medium: Sharing mode. Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone only.
ZoneAlarm Pro
Lines of Defense

Computer & Network Security Awareness - © 2006 SANS
Microsoft Windows SP2
Software Firewall General Tab

Windows Firewall is helping to protect your PC

On (recommended)
This setting blocks all outside sources from connecting to your computer through the Internet or a network.

Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?
Microsoft Windows SP2
Firewall Exceptions

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

- ActiveSync Application
- Connection Manager
- File and Printer Sharing
- Internet Explorer
- MSN Messenger 6.2
- Remote Assistance
- Remote Desktop
- Skype
- UPnP Framework
- Windows Media Player
- Windows Messenger

Display a notification when Windows Firewall blocks a program.

What are the risks of allowing exceptions?

OK Cancel
Microsoft Windows SP2
Firewall Log Settings
### Microsoft Windows SP2 Firewall Logging

![Window Firewall Log](image)

**Version:** 1.5  
**Software:** Microsoft Windows Firewall  
**Time Format:** Local  
**Fields:** date time action protocol src-ip dst-ip dst-port size tcpflags tcpseq tcpack tcpwin icmptype icmpcode info path

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Action</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Size</th>
<th>Flags</th>
<th>Seq</th>
<th>Ack</th>
<th>Win</th>
<th>Type</th>
<th>Code</th>
<th>Info</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-07-01</td>
<td>06:59:47</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>179.19</td>
<td>4598</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:11</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4600</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:11</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4600</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:13</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4601</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:13</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4601</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:46</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>107.124</td>
<td>4602</td>
<td>1863 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:32</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>107.124</td>
<td>4602</td>
<td>1863 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:32</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>39.141</td>
<td>4603</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:32</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>39.141</td>
<td>4603</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:32</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>5.7</td>
<td>4604</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:33</td>
<td>DROP TCP</td>
<td>107.124</td>
<td>139.189</td>
<td>1863</td>
<td>4602 40 R 1423837557 0 0 -- -- RECEIVE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:33</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>79.192</td>
<td>4606</td>
<td>443 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:34</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>179.192</td>
<td>4606</td>
<td>443 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:34</td>
<td>DROP TCP</td>
<td>79.192 6</td>
<td>39.189</td>
<td>443</td>
<td>4606 40 A 7740099375 2229582245 16722 -- -- RECEIVE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:34</td>
<td>DROP TCP</td>
<td>79.192 6</td>
<td>39.189</td>
<td>443</td>
<td>4606 40 A 7740099375 2229582245 16722 -- -- RECEIVE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:57</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>61.4607</td>
<td>80 -- -- -- - - --</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:57</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>5.61</td>
<td>4607</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:00:58</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>5.61</td>
<td>4608</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:01:10</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4609</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:01:10</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4609</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:01:12</td>
<td>OPEN TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4610</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:01:12</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>139.185</td>
<td>4610</td>
<td>5678 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2005-07-01</td>
<td>07:01:14</td>
<td>CLOSE TCP</td>
<td>139.189</td>
<td>179.19</td>
<td>4598</td>
<td>80 - - - - - -</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary

- Malicious software can harm your computer and can be avoided with care
- Phishing and Identity Theft are easily avoidable; if it looks too good to be true, it is.
- Remember that surfing the web can be dangerous if you are administrator and keep kid safety in mind
- Practice your Windows XP Operating System commands and learn your system
- Take passwords seriously and consider using a password wallet (KeePass)
- When your network works, take the time to record its settings
- Consider the use of a hardware and personal software firewall (e.g. Linksys and Zonealarm)
References

- Virus FAQ for New Users, www.faqs.org
- Spyware Definition, www.webopedia.com
- http://www.cybercrime.gov/crimes.html#IXa

Computer & Network Security Awareness - © 2006 SANS