Teaching and Practicing Practical Security

Mark Ciampa, Ph.D.
Western Kentucky University
150,000,000

A. Average CEO annual salary in 2010

B. How many cars Toyota will eventually end up recalling

C. Number of computers remotely controlled by attackers
90

A. The number of loose ends that were not resolved in the final episode of *Lost*

B. How old you will feel after sitting through all of these presentations today

C. Percentage of e-mail malware that is phishing
1,500

A. The number of e-mails you receive each week

B. How many mouse clicks are needed to navigate your company’s Web site

C. Number of users who still respond weekly to the “Nigerian General” spam
50%

A. How much your retirement account lost last year

B. Price your new flat panel TV dropped the week after you bought it

C. Percentage of Americans who had their credit card or SSN exposed online
39 Seconds

A. Time took the person sitting next to you this morning at breakfast to inhale that donut

B. How often you keep checking your watch to see when this presentation is finally over

C. Frequency a computer is probed on the Internet
More Bad News

- Web pages that infect by simply looking at them (6,000 new infected pages daily, or 1 every 14 seconds)
- More attacks originate in U.S. than any other country (33%)
- Home users were the most highly targeted sector (93% all targeted attacks)
- An infected U.S. computer average of 8 instances of malware
- U.S. has highest number of infected computers
Infected Computers by Country

- United States: 27%
- Brazil: 17%
- China: 17%
- Germany: 3%
- France: 3%
- United Kingdom: 3%
- Spain: 2%
- Japan: 2%
- Other: 26%
Phishing Attacks

- Phishing attacks remained virtually flat from Jul 2008 - Apr 2009
- May 2009 saw 400% increase in phishing, and increased even more in Jun 2009
- Phishing increase due to large number attacks targeting social networking sites
- Phishers now casting wider net to include gaming sites and portals
Phishing Targets

- January 2009
- February 2009
- March 2009
- April 2009
- May 2009
- June 2009
- July 2009

Categories:
- Other
- Online Services
- E-Commerce Sites
- Social Networking Sites
- Financial Sites
8 Years Ago: *Fame*

- Individual local hackers
- Wanted show off abilities
- Created nuisance worms and viruses
Today: Fortune

- Organized international groups
- Motive is financial gain
- Steal confidential information instead of destroy
- Create customized malware
- Blend multiple attacks
Why Increase In Attacks

- Speed of attacks
- More sophisticated attacks
- Simplicity of attack tools
- Faster detection weaknesses
- Delays in user patching
- Distributed attacks
- User confusion
User Confusion

- Confusion over different **attacks**: Worm or virus? Adware or spyware? Rootkit or Trojan?

- Confusion over different **defenses**: Antivirus? Firewall? Patches?

- Users asked to make security decisions and perform technical procedures
User Confusion

- Will you grant permission to open this port?
- Is it safe to unquarantine this attachment?
- May I install this add-in?
User Confusion

- 88% use their home computer for online banking, stock trading, reviewing personal medical information, and storing financial information, health records, and resumes.
- 98% agree important to be able to know risk level of a web site before visiting it. (But 64% admit don’t know how to.)
- 92% think that their anti-virus software is up to date. (But only 51% have current anti-virus software that been updated within last 7 days.)
User Confusion

- 44% don’t understand firewalls
- 25% have not even heard of the term “phishing”, only 13% can accurately define it
- 22% have anti-spyware software installed, an enabled firewall, and anti-virus protection that has been updated within last 7 days
Microsoft Office Format

- Over half vulnerabilities exploited in Microsoft Office format files already had patches available, some dating back 3 years
- 71.2% of attacks exploited single vulnerability for which security update (MS06-027) been available since 2006
- Most successful attacks affected Office 2003 users who had not applied a single service pack or security update since original release of Office 2003 (October 2003)
User Misconceptions

- I don’t have anything on my computer they want
- I have antivirus software so I’m protected
- My IT person takes care of security here at work
- My Apple computers is safe
## Apple Patches

### Security updates

<table>
<thead>
<tr>
<th>Name and information link</th>
<th>Released for</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone OS 3.1.3 and iPhone OS 3.1.3 for iPod touch</td>
<td>iPhone OS 1.0 through 3.1.2, iPhone OS for iPod touch 1.1 through 3.1.2</td>
<td>02 Feb 2010</td>
</tr>
<tr>
<td>Security Update 2010-001</td>
<td>Mac OS X v10.5.8, Mac OS X v10.6.2</td>
<td>19 Jan 2010</td>
</tr>
<tr>
<td>Java for Mac OS X 10.5 Update 6</td>
<td>Mac OS X v10.5.8</td>
<td>03 Dec 2009</td>
</tr>
<tr>
<td>Java for Mac OS X 10.6 Update 1</td>
<td>Mac OS X v10.6.2 or later</td>
<td>03 Dec 2009</td>
</tr>
<tr>
<td>Safari 4.0.4</td>
<td>Mac OS X v10.4.11, Mac OS X v10.5.8, Mac OS X v10.6.1 and v10.6.2, Windows 7, Vista, XP</td>
<td>11 Nov 2009</td>
</tr>
<tr>
<td>Mac OS X v10.6.2 / Security Update 2009-006</td>
<td>Mac OS X v10.5.8, Mac OS X v10.6 and v10.6.1</td>
<td>02 Nov 2009</td>
</tr>
<tr>
<td>iTunes 9.0.1</td>
<td>Mac OS X v10.4.11 or later, Mac OS X Server v10.4.11 or later, Windows XP SP2, Vista, Windows 7</td>
<td>22 Sept 2009</td>
</tr>
<tr>
<td>Xsan 2.2</td>
<td>Mac OS X v10.5.8, Mac OS X v10.6</td>
<td>14 Sept 2009</td>
</tr>
<tr>
<td>Security Update 2009-005</td>
<td>Mac OS X v10.4.11, Mac OS X v10.5.8</td>
<td>10 Sept 2009</td>
</tr>
</tbody>
</table>
“Securing your home computer helps you and your family, and it also helps your nation . . . by reducing the risk to our financial system from theft, and to our nation from having your computer infected and then used as a tool to attack other computers”

Janet Napolitano
Department Homeland Security
Calls for Training

- National Strategy to Secure Cyberspace (NSSC) document, created by U.S. President’s National Infrastructure Advisory Council, calls for comprehensive national security awareness program to empower all Americans, including the general population, “to secure their own parts of cyberspace”

- Department of Homeland Security, through the NSSC, calls upon home users to help the nation secure cyberspace “by securing their own connections to it”
Calls for Training

- Action and Recommendation 3-4 of NSSC calls upon colleges and universities to model user awareness programs and materials
- Colloquium for Information Systems Security Education (CISSE), International Federation of Information Processing Working Group 11.8 on Information Security Education (IFIP WISE), and Workshop on Education in Computer Security (WECS) all involved in security training in schools
- National Security Agency (NSA) developed effort aimed at creating larger core of computer security trained professionals known as the National Centers of Academic Excellence in Information Assurance Education, which even provides large numbers of college scholarships under its “Cyber Corps” program.
Calls for Training

- Other researchers state that institutions of higher education (IHEs) should be responsible for providing security awareness instruction, including Crowley (2003), Mangus (2002), Null (2004), Tobin and Ware (2005), Valentine (2005), Werner (2005), and Yang (2001).
- Security instruction and training important not only to meet current demands of securing systems but also to prepare students for employment in their respective fields.
- Location of security awareness instruction and training in a college curriculum should not be isolated in upper-level courses for IT majors, according to Tobin and Ware (2005), Werner (2005), and others.
- Instruction should be taught to all graduates as a “security awareness” course (Valentine, 2005) along with integrating it across through the curriculum (Yang, 2001).
- Long (1999) advocated that security instruction should begin as early as kindergarten.
Defenses

1. Education & awareness
2. Smart behavior
3. Technology
Security Education In Schools

- Brief coverage of security in *Introduction to Computers* courses where teach definitions
- Teach network security to computer majors
- Yet leaving out *practical security awareness* for all students
Security Education Challenge

- Need educate all students about *practical* computer security awareness
- “Security Literacy” – Why and how to make personal systems secure
- “*Users should be as fluent with security literacy as with Office or e-mail*”
Practical Security Topics

- Desktop Security
- Internet Security
- Personal Security
- Wireless Network Security
Teaching and Practicing Practical Security

Desktop Security
Virus

- Virus – Program with malicious intent
- Similar to biological counterpart but requires 2 “carriers”
  - Document/program - Virus secretly attaches itself and then executes malicious payload when document opened or program launched
  - User - Virus rely on actions by users to spread virus to another computer
Worm

- Program designed to take advantage of vulnerability in application or operating system to enter system

- Once worm has exploited the vulnerability on one system, immediately searches for another computer that has the same vulnerability

- Worm can travel by itself and does not require any user action to begin its execution
Trojan Horse

- Trojan horse (Trojan) - Program advertised as performing one activity but actually does something else (or it may perform both the advertised and malicious activities)
- Typically executable programs that contain hidden code that attacks the computer system
Threat Category Trends
Threat Categories By Nation

- US, UK, France & Italy - Trojans are the largest single category of threat.
- Spain & Korea - Worms dominate, then threats targeting online gamers.
- China - Language-specific browser-based threats.
- Brazil - Malware targeting online banking widespread.
Zombies & Botnets

- One of the more common types of malware today carried by Trojan horses, worms, and viruses
- Program puts infected computer under remote control of an attacker without user’s knowledge
- **Zombie** - Infected “robot” computer
- **Botnet** - Thousands of zombies manipulated under remote control
Zombies & Botnets

- Attackers use Internet Relay Chat (IRC) to remotely control zombies
- IRC an open communication protocol used for real-time “chatting” with other IRC users over Internet
- Once a computer is infected it joined to specific IRC channel on an IRC server and awaits instructions, allowing an attacker to remotely control the zombie
- Once under the control of a bot herder, botnets can be used for many different malicious purposes
Personal Firewall

- Two-way personal software firewall - Inspects network traffic passing through it and denies/permits passage based on rules
- Firewall restricts what can come in and go out of your computer across the network
  - Stops bad stuff from coming in
  - Stops a compromised computer from infecting other computers on network
- Application-aware firewall allows user to specify which desktop applications can connect to the network
Check Firewall Settings
Test Firewall

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

- Open
- Closed
- Stealth

Total elapsed testing time: 69.029 seconds
Test Firewall

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

Total elapsed testing time: 68.029 seconds
Patch Management

- Different types of patches
- How to install patch
- Auto-update feature
Windows Patch Updates

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

Understanding Windows automatic updating

- **Install updates automatically (recommended)**
  - Install new updates:
    - Every day
    - at 7:00 AM

- Download updates but let me choose whether to install them

- Check for updates but let me choose whether to download and install them

- Never check for updates (not recommended)
  - Your computer will be more vulnerable to security threats and performance problems without the latest updates.

Recommended updates

- Include recommended updates when downloading, installing, or notifying me about updates

Update service

- Use Microsoft Update
  - You will receive updates for Windows and other products from Microsoft Update.
Know Your Antivirus

- Know how to update
- Know how to scan device
- Know how to test antivirus
- Know how to disinfect
# Antivirus

![VirusScan Console](image)

<table>
<thead>
<tr>
<th>Task</th>
<th>Status</th>
<th>Last Re</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Protection</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Buffer Overflow Protection</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>On-Delivery E-mail Scanner</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Unwanted Programs Policy</td>
<td>No unwanted program categories are turned on. No user-defined detecti...</td>
<td></td>
</tr>
<tr>
<td>On-Access Scanner</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Quarantine Manager Policy</td>
<td>The quarantine folder contains 0 items</td>
<td></td>
</tr>
<tr>
<td>Full Scan</td>
<td>Not Scheduled</td>
<td></td>
</tr>
<tr>
<td>AutoUpdate</td>
<td>Run at startup</td>
<td></td>
</tr>
</tbody>
</table>

*VirusScan Console*
Antivirus

- Test antivirus settings
- Disinfect
Windows Security Dashboard

- Displays all system security features
- First in Windows XP SP2 to constantly monitor & display status of Windows Firewall, Automatic Updates, anti-virus
- Vista “Windows Security Center (WSC)” expands coverage by adding anti-spyware software, Internet Explorer security settings, User Account Control, and monitoring multiple vendors’ security solutions running and indicate which are enabled and up to date
- Windows 7 renamed to “Action Center”
## Windows Security Center

### Security essentials
To help protect your computer, make sure the four security essentials below are marked On or OK.

**Using Windows Security Center**

<table>
<thead>
<tr>
<th>Firewall</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Firewall is actively protecting your computer.</td>
<td></td>
</tr>
<tr>
<td>Note: Two or more firewalls running at the same time can conflict with each other.</td>
<td></td>
</tr>
<tr>
<td>How does a firewall help protect my computer?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automatic updating</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>As updates become available, Windows installs them for you (recommended). Automatically installing updates can enhance the security and performance of your computer.</td>
<td></td>
</tr>
<tr>
<td>How does automatic updating help protect my computer?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware protection</th>
<th>Check settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus protection</td>
<td>Not found</td>
</tr>
<tr>
<td>Windows did not find antivirus software on this computer.</td>
<td></td>
</tr>
<tr>
<td>Show me my available options.</td>
<td></td>
</tr>
<tr>
<td>Spyware and other malware protection</td>
<td>On</td>
</tr>
<tr>
<td>Windows Defender is actively protecting your computer.</td>
<td></td>
</tr>
<tr>
<td>How does anti-malware software help protect my computer?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other security settings</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet security settings</td>
<td>OK</td>
</tr>
<tr>
<td>All Internet security settings are set to their recommended levels.</td>
<td></td>
</tr>
<tr>
<td>How do Internet security settings help protect my computer?</td>
<td></td>
</tr>
<tr>
<td>User Account Control</td>
<td>On</td>
</tr>
<tr>
<td>User Account Control is turned on.</td>
<td></td>
</tr>
<tr>
<td>How does User Account Control help protect my computer?</td>
<td></td>
</tr>
</tbody>
</table>
User Account Control (UAC)

- User attempts to perform task that requires administrative access then prompted for approval or administrator password if standard user
- Displays authentication dialog box must be answered before continuing
- Administrators - Click Continue or Cancel
- Standard users - Enter admin password
User Account Control (UAC)

Windows needs your permission to continue.

If you started this action, continue.

User Accounts Control Panel
Microsoft Windows

Details

User Account Control helps stop unauthorized changes to your computer.
User Account Control (UAC)

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.  
Tell me more about User Account Control settings

- Always notify me when:
  - Programs try to install software or make changes to my computer
  - I make changes to Windows settings

- Never notify

Recommended if you routinely install new software and visit unfamiliar websites.

[OK] [Cancel]
## View security report

### Security Update Scan Results

<table>
<thead>
<tr>
<th>Score</th>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>Windows Security Updates</td>
<td>4 security updates are out of date or could not be confirmed.</td>
</tr>
<tr>
<td></td>
<td>Media Player Security Updates</td>
<td>No critical security updates are missing.</td>
</tr>
<tr>
<td></td>
<td>IIS Security Updates</td>
<td>IIS is not running on this computer.</td>
</tr>
<tr>
<td></td>
<td>SQL Server Security Updates</td>
<td>SQL Server is not installed on this computer.</td>
</tr>
<tr>
<td></td>
<td>Exchange Server Security Updates</td>
<td>Exchange Server is not installed.</td>
</tr>
</tbody>
</table>

### Windows Scan Results

#### Vulnerabilities

<table>
<thead>
<tr>
<th>Score</th>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>Administrators</td>
<td>More than 2 Administrators were found on this computer.</td>
</tr>
<tr>
<td></td>
<td>Local Account Password Test</td>
<td>No user accounts have blank or simple passwords.</td>
</tr>
<tr>
<td></td>
<td>File System</td>
<td>All hard drives (1) are using the NTFS file system.</td>
</tr>
<tr>
<td></td>
<td>Guest Account</td>
<td>The Guest account is not disabled on this computer.</td>
</tr>
</tbody>
</table>

© 2002-2003 Microsoft Corporation, Shavlik Technologies, LLC. All rights reserved.
Desktop Summary

- Check your firewall
- Turn on automatic updates
- Know your antivirus
- Watch UAC
- Use automated inspectors
Teaching and Practicing Practical Security

Internet Security
Internet Attacks

- Downloaded browser code
  - JavaScript
  - Java
  - ActiveX
- Privacy attacks
  - Cookies
  - Adware
Internet Attacks

- Attacks while surfing
  - Redirected Web traffic
  - Drive-by downloads
- E-mail attacks
  - Spam
  - Malicious attachments
  - Embedded hyperlinks
Internet Defenses

- Defenses through browser settings
  - Advanced security settings
  - Security zones
  - Restricting cookies
- Defenses through applications
  - Popup blockers
  - Spam filters
  - E-mail security settings
- E-mail defenses through good practices
Popup Blockers

![Popup Blocker Settings Dialogue Box](image)
Spam Filters

Outlook can move messages that appear to be junk e-mail into a special Junk E-mail folder.

Choose the level of junk e-mail protection you want:

- **No Automatic Filtering.** Mail from blocked senders is still moved to the Junk E-mail folder.
- **Low.** Move the most obvious junk e-mail to the Junk E-mail folder.
- **High.** Most junk e-mail is caught, but some regular mail may be caught as well. Check your Junk E-mail folder often.
- **Safe Lists Only.** Only mail from people or domains on your Safe Senders List or Safe Recipients List will be delivered to your Inbox.

- Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder
- Disable links and other functionality in phishing messages. (recommended)
- Warn me about suspicious domain names in e-mail addresses. (recommended)
- When sending e-mail, Postmark the message to help e-mail clients distinguish regular e-mail from junk e-mail
E-Mail Security Settings

- **Read messages using a reading pane** - Most e-mail clients contain a reading pane that allows the user to read an e-mail message without actually opening it.

- **Preview attachments** - When an attachment is received with an e-mail message, some e-mail clients will permit the user to view the contents of the attachment without saving and then opening it.

- **Block external content** - E-mail clients can be configured to block external content, such as hyperlinks to pictures or sounds, in HTML e-mail messages that are received.
You can control whether Outlook automatically downloads and displays pictures when you open an HTML e-mail message.

Blocking pictures in e-mail messages can help protect your privacy. Pictures in HTML e-mail can require Outlook to download the pictures from a server. Communicating to an external server in this way can verify to the sender that your e-mail address is valid, possibly making you the target of more junk mailings.

- Don't download pictures automatically in HTML e-mail messages or RSS items
- Permit downloads in e-mail messages from senders and recipients defined in the Safe Senders and Safe Recipients Lists used by the Junk E-mail filter
- Permit downloads from Web sites in this security zone: Trusted Zone
- Permit downloads in RSS items
- Permit downloads in SharePoint Discussion Boards
- Warn me before downloading content when editing, forwarding, or replying to e-mail
Treat E-Mail Like A Postcard

- **Anybody can read it** – Just as anybody who’s nosy can read what’s written on a postcard, e-mail likewise can be read as it weaves it way through the Internet. A good idea is to not put anything private in an e-mail that you wouldn’t want a stranger to read.

- **You can only read it** – The only thing you can do with a postcard is read it and then stick it on the refrigerator; it doesn’t have a return envelope so you can respond back to the sender. E-mail should also be seen as “read only”, so don’t click on embedded links or provide requested information.

- **It has nothing else with it** – While a letter in an envelope may also contain other documents a postcard cannot, and e-mail should be treated in the same way. It’s a good idea not to accept any e-mail attachments unless the sender has notified you (and not by e-mail!) to expect it.
Your Capital One statement is ready

The statement for your account ending in 0448 is available online. For your convenience you can log in to Online Account Services (OAS) from this e-mail to review your statement.

Check Out Our Competitive Rates

- Auto Loans
  - New/Used
  - Refinance
  - Motorcycle

- Direct Banking
  - High Yield Money Market
  - Business Money Market
  - CDs

- Home Loans
  - Home Equity
  - Refinance
  - Purchase

- Small Business
  - Credit Cards
  - Loans
  - Line of Credit

Security and simplicity—Capital One® is the place to come to:

- Pay your credit card bill online for free*
- View your statements and transactions
- Check your credit limit and available credit
- Update your personal information

More than credit cards
Did you know that we offer auto loans, home loans, medical financing, a variety of savings products, and more? Visit www.capitalone.com to check our rates, use interactive financial tools, and to find out about all our innovative products.
. . . you can <a href="http://www.capitalone.com">log in to Online Account Services (OAS) </a> from this e-mail

. . . you can <a href="http://www.steal-your-number.net">log in to Online Account Services (OAS) </a> from this e-mail
Check Certificate
Internet Summary

- Use popup blockers
- Turn on spam filters
- Configure e-mail security settings
- Use good e-mail practices
- Check that certificate
Teaching and Practicing Practical Security

Personal Security
Password Paradox

- Password paradox – For password to remain secure never written down but committed to memory
- Password also be of sufficient length and complexity that attacker cannot easily guess
- Paradox: although lengthy and complex passwords should be used and never written down, very difficult to memorize these types of passwords
- Users have multiple accounts for computers at work, school, and home, e-mail accounts, banks, online Internet stores, and each account has its own password
Weak Passwords

- Common word (*Eagles*)
- Short passwords (*ABCD*)
- Personal information (name of a child or pet)
- Write password down
- Predictable use of characters
- Not change password
- Reuse same password
## Top Ten Passwords

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Number of Users with Password (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>290731</td>
</tr>
<tr>
<td>2</td>
<td>12345</td>
<td>79078</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>76790</td>
</tr>
<tr>
<td>4</td>
<td>Password</td>
<td>61958</td>
</tr>
<tr>
<td>5</td>
<td>iloveyou</td>
<td>51622</td>
</tr>
<tr>
<td>6</td>
<td>princess</td>
<td>35231</td>
</tr>
<tr>
<td>7</td>
<td>rockyou</td>
<td>22588</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>21726</td>
</tr>
<tr>
<td>9</td>
<td>12345678</td>
<td>20553</td>
</tr>
<tr>
<td>10</td>
<td>abc123</td>
<td>17542</td>
</tr>
</tbody>
</table>
Strong Passwords

- Strong passwords – Passwords are difficult to break
- Passwords should optimally have at least 15 characters
- Passwords should be a random combination of letters, numbers, and special characters
- Passwords should be replaced with new passwords at least every 60 days
- Passwords should not be reused for 12 months
- The same password should not be duplicated and used for multiple accounts
# Strong Passwords

<table>
<thead>
<tr>
<th>Password Example</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I8anhterYee59</td>
<td>Non-dictionary combination of alphabetic and numeric characters</td>
</tr>
<tr>
<td>68!eEiWob*2ukk</td>
<td>Non-dictionary combination of alphabetic, numeric, and punctuation characters</td>
</tr>
<tr>
<td>135LeEeEngtH31i34!@</td>
<td>Non-dictionary long combination of alphabetic, numeric, and punctuation characters</td>
</tr>
<tr>
<td>ØAr87&amp;535!hhtrr460o0o0€</td>
<td>Non-dictionary long combination of alphabetic, numeric, punctuation characters, and non-keyboard characters</td>
</tr>
</tbody>
</table>
Test Passwords

- All passwords should be as long as possible, using a mix of characters, and not contain any dictionary words
- Develop naming convention
- Online password creators
- Online password graders
Use Special Characters

- Make passwords stronger with special characters not on keyboard
- Created by pressing ALT key while typing number on numeric keypad (not top of the keyboard); ALT + 0163 produces £.
- View list available non-keyboard characters click Start and Run and enter charmap.exe; click on character and the code ALT + 0xxx will appear in lower-right corner if can be reproduced in Windows
Password Management Program

- Password management program – Allow user to enter account information such as username and password, along with other account details
- Storage program is itself protected by single strong password, and can require presence of a file on USB flash drive before program open
- Allows user to drag and drop usernames and passwords into these fields without typing
Phishing

- Social engineering - Relies on deceiving someone to obtain secure information
- Phishing - Common form of social engineering is sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information
- User asked respond to an e-mail or is directed to a Web site where instructed to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information for which the legitimate organization already has a record
- However, Web site is actually a fake and is set up to steal the user’s information
Recognize Phishing Attacks

- *Deceptive Web links*—Link to Web site embedded in e-mail should not have an @ sign in the middle of the address
  - Users should never log on to a Web site from a link in an e-mail but instead should open new browser window and type legitimate address
- *E-mails that look like Web sites*—Phishers often include the logo of the vendor and otherwise try to make the e-mail look like the vendor’s Web site as a way to convince the recipient that the message is genuine
  - Presence of logos does not mean that e-mail is legitimate.
Recognize Phishing Attacks

- **Fake sender’s address**—Because sender addresses can be forged easily, an e-mail message should not be trusted simply because the sender’s e-mail address appears to be valid (such as tech_support@ebay.com).
- **Generic greeting**—Many phishing e-mails begin with a general opening such as “Dear e-Bay Member” and do not include a valid account number.
- **Popup boxes and attachments**—Legitimate e-mails from vendors never contain a popup box or an attachment.
- **Urgent request**—Many phishing e-mails try to encourage the recipient to act immediately or else their account will be deactivated.
Phishing Tests

- Mailfrontier
- Antiphishing.org
- Antiphishing Phil
- Paypal
Social Networking Attacks

- Grouping individuals and organizations into clusters or groups based on affiliation called social networking
- Web sites that facilitate linking individuals with common interests like hobbies, religion, politics, or school contacts are called social networking sites and function as an online community of users
- User who is granted access to a social networking site can read the profile pages of other members and interact with them
- Social networking sites increasingly becoming prime targets of attacks
Social Network Defenses

- **Consider carefully who is accepted as a friend** – Once person has been accepted as friend that person will be able to access any personal information or photographs.

- **Show "limited friends" a reduced version of your profile** - Individuals can be designated “limited friends” who only have access to a smaller version of the user’s profile.

- **Disable options and then reopen them only as necessary** - Disable options until it becomes apparent that option is needed, instead of making everything accessible and restricting access later after it is too late.
<table>
<thead>
<tr>
<th>Option</th>
<th>Recommended Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Only my friends</td>
<td>Facebook networks can contain hundreds or thousands of users and there is no control over who else joins the network to see the information.</td>
</tr>
<tr>
<td>Photos or photos tagged of you</td>
<td>Only my friends</td>
<td>Photos and videos have often proven to be embarrassing. Only post material that would be appropriate to appear with a resume or job application.</td>
</tr>
<tr>
<td>Status updates</td>
<td>Only my friends</td>
<td>Because changes to status such as “Going to Florida on January 28” can be useful information for thieves only approved friends should have access to it.</td>
</tr>
<tr>
<td>Online status</td>
<td>No one</td>
<td>Any benefits derived by knowing who is online are outweighed by the risks.</td>
</tr>
<tr>
<td>Friends</td>
<td>Only my friends (minimum setting)</td>
<td>Giving unknown members of the community access to a list of friends may provide attackers with opportunities to uncover personal information through friends.</td>
</tr>
<tr>
<td>Mobile phone, landline, current address</td>
<td>Opt-out (decline to enter)</td>
<td>Users can contact other subscribers through the online features of Facebook; there are serious security risks to publishing personal contact information.</td>
</tr>
<tr>
<td>Website</td>
<td>Only my friends</td>
<td>A Web site may contain photos or private information that could be used by attackers to identify the user.</td>
</tr>
<tr>
<td>Contact e-mail address</td>
<td>No one</td>
<td>Because messages can be sent through Facebook itself it is not necessary to reveal an e-mail address.</td>
</tr>
</tbody>
</table>
## Backups

![Macrium Reflect interface for disk and partition management.](image)

<table>
<thead>
<tr>
<th>Disk 1</th>
<th>ST3000105AS 3.5ADH</th>
<th>74.506 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partitions</td>
<td>Type</td>
<td>Capacity</td>
</tr>
<tr>
<td>1 - &lt;NO NAME&gt; (C:)</td>
<td>Active</td>
<td>74,497 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk 2</th>
<th>Hitachi HDS721010KLA330 GKA0D0A</th>
<th>931.513 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partitions</td>
<td>Type</td>
<td>Capacity</td>
</tr>
<tr>
<td>1 - Storage (F:)</td>
<td>Primary</td>
<td>400,201 GB</td>
</tr>
<tr>
<td>2 - New Volume (G:)</td>
<td>Primary</td>
<td>443,230 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disk 4</th>
<th>Maxtor OneTouch II 023</th>
<th>279.461 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partitions</td>
<td>Type</td>
<td>Capacity</td>
</tr>
<tr>
<td>1 - Maxtor External USB 300 GB HD (I:)</td>
<td>Primary</td>
<td>279,464 GB</td>
</tr>
</tbody>
</table>
Personal Summary

- Use a password manager
- Recognize phishing attacks
- Practice good social networking skills
- Do regular backups
Does Wireless Security Matter?

- Get into any folder set with file sharing enabled
- See wireless transmissions
- Access network behind firewall can inject malware
- Download harmful content linked to unsuspecting owner
1. Lock Down AP

- Create strong Password (>12 characters with 1 number and mixed case)
- Disable *Wireless Web Access* (cannot access AP settings via wireless device, must be connected with cable)
- Disable *Remote Management* (cannot access AP settings via Internet)
- Access server via HTTPS (must use [https://192.168.1.1](https://192.168.1.1)) if access AP settings via Internet
- Disable *UPnP*
2. Limit Users By MAC

- Edit MAC Filter List by entering MAC addresses of approved PCs
- Permit only PCs listed to access wireless network
- Enable *Wireless MAC Filter*
- Be sure to “Edit”, “Permit” then “Enable” or else cannot let yourself in!
Wireless MAC Filter

MAC Address Filter List

Enter MAC Address in this format: xxxxxxxxxxxxxxxx

Wireless Client MAC List

<table>
<thead>
<tr>
<th>MAC 01 :</th>
<th>MAC 11 :</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0E:35:36:31:2C</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 02 :</th>
<th>MAC 12 :</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0F:66:78:27:71</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 03 :</th>
<th>MAC 13 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 04 :</th>
<th>MAC 14 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 05 :</th>
<th>MAC 15 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 06 :</th>
<th>MAC 16 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 07 :</th>
<th>MAC 17 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 08 :</th>
<th>MAC 18 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 09 :</th>
<th>MAC 19 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 10 :</th>
<th>MAC 20 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 21 :</th>
<th>MAC 31 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 22 :</th>
<th>MAC 32 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC 23 :</th>
<th>MAC 33 :</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Turn on WPA2

- On AP Security Mode set as **WPA2 Personal**
- WPA Algorithms set as **TKIP+AES**
- WPA Shared Key set minimum 24 characters
- Group Key Renewal should not be set to less than **300 seconds** (5 minutes)
4. Other

- Turn on VLAN
- Limit by DHCP settings
- Disable SSID beaconing
Beware of Imposters

Attacker ad hoc network

Free Airport Wireless

Nashville Airport Wireless

Legitimate wireless network
Wireless Summary

- Configure for security
- Be aware of imposters
Teaching and Practicing Practical Security
User Confusion

- Confusion over different attacks: Worm or virus? Adware or spyware? Rootkit or Trojan?
- Confusion over different defenses: Antivirus? Firewall? Patches?
- Users asked to make security decisions and perform technical procedures
Calls for Training

- National Strategy to Secure Cyberspace (NSSC) document, created by U.S. President’s National Infrastructure Advisory Council, calls for comprehensive national security awareness program to empower all Americans, including the general population, “to secure their own parts of cyberspace”

- Department of Homeland Security, through the NSSC, calls upon home users to help the nation secure cyberspace “by securing their own connections to it”
Security Education In Schools

- Brief coverage of security in Introduction to Computers courses where teach definitions
- Teach network security to computer majors
- Yet leaving out practical security awareness for all students
Security Education Challenge

- Need educate **all** students about *practical* computer security awareness
- “Security Literacy” – Why and how to make personal systems secure
- “Users should be as fluent with security literacy as with Office or e-mail”
New Approaches

- Adding practical security to Introduction to Computers course
- Content added to freshman orientation course
- Adding 1 hour ethics & practical course
- Substitute practical security course for introductory Office applications course
URL References

- Test firewall - www.grc.com “Shields UP!!”
- Test antivirus settings - www.eicar.org/anti_virus_test_file.htm
- Disinfect - www.symantec.com/norton/security_response/removaltools.jsp
- Software inspector - secunia.com/vulnerability_scanning/personal/
- Online password creators - www.grc.com/passwords.htm
- Online password graders - www.microsoft.com/protect/yourself/password/checker.mspx
- Password manager – keepass.info
- Phishing tests:
  - survey.mailfrontier.com/survey/quiztest.cgi
  - www.antiphishing.org/phishing_archive.html
  - cups.cs.cmu.edu/antiphishing_phil/
Resources

- **Security Awareness: Applying Practical Security In Your World**
  (978-1-4354-5414-9)
- [Community.cengage.com/infosec](http://Community.cengage.com/infosec)
- Mark.Ciampa@wku.edu
Teaching and Practicing Practical Security

Mark Ciampa, Ph.D.
Western Kentucky University