



# Computer Security Guide for Students, Faculty, and Staff

## Table of Contents

Section	Page
Computer Support at ECU.....	3
Windows Computer Support.....	3
Apple Computer Support .....	3
Secure Your Computer .....	4
Passwords.....	5
Software—Update and Use Prudently .....	6
Secure Your Browser .....	6
Security for Wireless Networking.....	7
Use Your Head .....	8
Scan for Software Vulnerabilities .....	8
Secure Your Home Network.....	9
Secure Your Data.....	11
Data Ownership and Responsibility .....	11
Data Storage Guidelines .....	11
Data Encryption.....	12
Updating Microsoft Software .....	13
Microsoft Update .....	13
Automating Microsoft Update .....	13
Microsoft Baseline Security Analyzer.....	14
Applying Patches to a New Computer .....	15
When Your Antimalware Software Detects Malware .....	16
Pay Attention.....	16
Appropriate Responses to Notices .....	16
When Your Computer is Infected .....	16
How to Avoid Malware Problems .....	18
Malware Types .....	18
Avoiding Malware.....	19
System Maintenance for the PC.....	21
Check Disk .....	21
Disk Defragmenter.....	21
How Hackers Work.....	22
Technical Hacking .....	22
Social Engineering .....	22
Is My Computer Compromised? .....	25
If Your Campus Computer is Compromised.....	26

React Quickly.....	26
Can't Somebody Just "Clean" My Compromised Computer? .....	26
Identity Theft .....	28
North Carolina Identity Theft Protection Act .....	28
Additional Identity Theft Protection .....	28
Phishing .....	29
Take Action .....	29

---

*This document has been prepared for students, faculty, and staff at East Carolina University, who are supported by ITCS (Information Technology and Computing Services). Contents of this document may also apply to computers that are not supported by ITCS.*

# Computer Support at ECU

ITCS IT Support Services for faculty/staff/students:

- telephone: 328-9866
- website: <http://www.ecu.edu/cs-itcs/ithelpdesk>

Student Help Desk:

- telephone: 328-4968

ACE Student Computer Support Center:

- location: Austin Building, Room 101
- website: <http://www.ecu.edu/ace>

## Windows Computer Support

ITCS supports computers running licensed versions of Microsoft Windows XP and Microsoft Windows 7. Specific instructions in this document apply to Windows XP and Windows 7, although many suggestions can apply to other operating systems and computing platforms.

Microsoft has discontinued support for Windows 2000, Windows Me, Windows 98, Windows 95, and Windows NT 4. ITCS cannot support operating systems that are not supported by their manufacturer. Retired versions of Windows are no longer updated with security patches, so they cannot be secured against hackers and malware and represent a threat to other computers on the ECU campus data network. If your computer runs one of these outdated operating systems, you must upgrade immediately to Windows XP and install the latest Service Pack to ensure the security of your data.

## Apple Computer Support

ITCS supports Apple computers running licensed versions of OS X. Older versions of Apple operating systems are not supported.

# Secure Your Computer

“Required computer maintenance” used to mean “defragment your hard drive and check for viruses.” These two duties are still required to maintain your computer, but your maintenance responsibilities have expanded to add “secure your computer.” If your computer is not secured, it will get compromised—and when it gets compromised, it must be formatted and reloaded before you can trust its security again.

Security threats to your computer can be classified in three groups:

- Hackers, who try to break into your computer without your knowledge or permission. They may claim that they were “just looking around” or that they were “doing you a favor by showing that your security is flawed.” They may also steal your data or use your computer to commit a crime by remote control. In any case, hackers are unethical people who should not be trusted or respected.
- Malware (malicious software), which comes in many forms: viruses, worms, Trojan horses, scripts, rootkits, adware, and spyware. Malware can take control of your computer without your knowledge or permission, delete your data, send your data to an unauthorized recipient, or cause your computer to attack other computers. In the last few years, malware has become professional crimeware—it’s no longer produced by kids trying to impress their friends.
- User error, which includes ignorance, laziness, and gullibility. Computer users need to understand computer security, just as car drivers need to understand the “rules of the road” to avoid unpleasant results. Users must keep their computers up to date, use passwords whenever available, and ensure the passwords are not guessable. Short passwords that are easy to type are also easy to guess. Unwary users can fall prey to con artists like phishers and social engineers, resulting in embarrassment, financial loss, and identity theft.

You must perform all the following tasks (detailed elsewhere in this document) to ensure the proper security and operation of your computer:

- If your computer runs Windows XP or Windows 7, follow the directions in this document to secure your computer. If your computer runs any older version of Windows, upgrade immediately! Older versions of Windows cannot be secured against modern security threats.
- Protect your computer with strong passwords (see the section titled “Secure Your Computer”). Leaving password fields blank or using default passwords will get your computer compromised, sometimes in a matter of minutes.
- Microsoft Update must be run daily to ensure that all Critical Updates have been applied to your computer. You can configure this utility to update your computer automatically (see the section titled “Updating Microsoft Software”). *All available Critical Updates should be installed immediately!*
- Use antimalware software. ECU has a site license for Symantec antimalware software, which is required to be installed on all Windows and Macintosh computers connected to the ECU campus data network. Never turn off or disable antimalware software. If you suspect your computer is infected, don’t wait—do something about it! If your computer is located on the ECU campus, call the ECU Help Desk at 328-9866 and open a service ticket to have your computer checked. Update antimalware definitions daily and scan all your files at least weekly to protect against malware (malicious software) that can destroy your data and render your computer useless.
- Firewalls should be used on any computer that connects to a network or the Internet.
  - Windows XP and Windows 7 contain a built-in firewall.

- If you use a hardware firewall at home (e.g., a wireless router with a built-in firewall), that's good. However, do not bring it to campus and connect it to the campus computer network—it is a networking device prohibited by University policy.
- Whenever you leave your computer, lock it. Press the CTRL, ALT, and DEL keys simultaneously, then release them and choose "Lock Computer." All current processes and active programs will continue to run, but unauthorized individuals can't use your computer until you login again.
- Use a password-protected screen saver and configure it to blank your screen after 10 minutes of inactivity. Use only screen savers included in your Windows operating system. Never use an aftermarket screen saver on your computer.
- Turn off your computer if it will be idle for more than a few hours, especially if it will be idle overnight. A computer can't get compromised while it's turned off—and it doesn't waste electricity!

## Passwords

- Use passwords whenever possible.
  - Never use a blank password.
  - Change all default passwords immediately.
  - Use strong passwords (passphrases).
- Create strong passwords by following these guidelines:
  - at least 8 digits long
  - no repeating digits
  - combination of numbers and letters
  - mix of upper- and lower-case letters
  - special characters (!, @, #, &, %, etc.) *within* the password, not just at the beginning or end
  - Don't use dictionary words (including foreign or archaic languages), your account name, proper names, zip codes, or room numbers.
  - Don't use "password" as your password.
- Keep passwords secret.
  - If someone else uses your userID and password, you will be held accountable for their actions.
  - Use only the unique userid provided to you and change it often.
  - Don't write down your password and hide it under the telephone, under the keyboard, or in a desk drawer.
  - Never reveal your password to anyone, *including your coworkers and superiors*. If your superior or coworker pressures you to reveal your password, they are in direct violation of University policy. Notify ECU Human Resources immediately—your anonymity will be protected.
  - When using a computer or accessing a website, never use any option that offers to "save my password for the next time," "automate my login," or "remember me." These options will store your password, which is just as bad as writing it down. Stored passwords can be stolen and used against you.
  - ITCS will *never* request your password over the phone or via email!
- Change passwords at least every 90 days.
  - Don't re-use old passwords.
  - Don't use the same password for multiple systems.

## Software—Update and Use Prudently

- Patch your software (operating system and applications). Hackers will use newly-discovered security flaws against you within a matter of hours! Check for updates to your operating system and applications on a daily basis. Whenever possible, automate the checking. Apply security patches as soon as they become available.
  - See the “Updating Microsoft Software” section of this document for details on updating Microsoft products.
  - If you use non-Microsoft software, check the software manufacturers’ websites regularly and apply all available updates. Automate the process if the applications support this option.
- Use email prudently. Never open any e-mail attachment, regardless of its source. Save the file to your computer’s hard drive and scan it for malware. Follow the directions in “How to Use Antimalware Software—Your Responsibilities.”
- Avoid software you don’t need. If you don’t need it, don’t install it. If you’ve installed it and you don’t use it, uninstall it. If you don’t know how to uninstall it, call the Help Desk. Examples of software to avoid:
  - Peer-to-peer (P2P) file sharing software. (e.g., Kazaa, gnutella, BearShare, Grokster, Morpheus, Napster, LimeWire, BitTorrent, Skype, etc.). Many forms of malware target P2P users exclusively.
  - Instant messaging software (AOL, Yahoo, etc.) and chat software. Many forms of malware are designed to spread using these inherently unsecured channels, which do not have the antimalware protection of a proper email system.
  - Add-on browser toolbars
  - Aftermarket screen savers (especially those that automatically download pictures from the Internet)
  - Non-Microsoft add-ons to Outlook (e.g., “cute” icons, emoticons)
  - Weather-monitoring software
  - News-monitoring software
  - Stock market-monitoring software
  - Non-Microsoft media players (e.g., Quicktime, RealPlayer)
  - Aftermarket desktop search engines capable of sharing your data with other computers
  - Alternative email clients
  - Web server software
  - Shopping or coupon software (e.g., Claria, formerly named Gator)
  - Password-caching software (stores your userids/passwords at remote location)
  - Online gambling software
  - Remote control and remote access software.

## Secure Your Browser

- Your browser has a “popup blocker” that prevents popup windows from cluttering your screen. Some programs require you to disable this function temporarily. If you disable the popup blocker, remember to enable it when you’re finished.
- When using a computer or accessing a website, never use an option to “remember my password the next time.” This option will store your password in a standard location on the computer, which is the same as writing it down—and just as bad. If your password is stored, it can be found and used against you.
- If you use Internet Explorer, your browser has an option to save encrypted web pages to your hard drive. Since encrypted web pages usually require a password, this means you could be saving a copy of your password to your hard drive, which is a bad idea. To turn off this feature:
  - Start Internet Explorer
  - Select “Tools” from the menu bar

- Select the “Advanced” tab
- Go to the Browsing section of the window and deselect “Use inline AutoComplete”
- Go to the Security section of the window and
  - Select the box in front of “Do not save encrypted pages to disk.”
  - Select the box in front of “Empty Temporary Internet Files folder when browser is closed.”
  - Deselect the box in front of “Use SSL 2.0” The boxes to use SSL 3.0 and TLS 1.0 should be checked.
- Click OK to enter the options manager.
- If you use Firefox
  - Go to Tools, Options, Privacy
    - In the History section, deselect all options.
    - In the Cookies section, use the drop-down box to keep cookies until “I close Firefox.”
    - In the Private Data section, select “Always clear my private data when I close Firefox.” Then click the Settings button and ensure that every entry in the list is checked.
  - Go to Tools, Options, Security.
    - In the Passwords section, deselect all choices.
  - Click OK to exit the options manager.

### Security for Wireless Networking

Wireless networks should never be considered secure. You need to take extra security precautions when using a wireless network, especially if it’s a public “hot spot” located in a motel or cyber café.

- Disable Wi-Fi ad-hoc mode. Wi-Fi runs in two modes: infrastructure mode (when you connect to a network) and ad hoc mode (when you connect directly to another PC). If you’ve enabled ad hoc mode, someone near you could establish a connection to your computer without your knowledge, and they’ll have free reign on your PC. To turn off ad hoc mode:
  - Right-click the wireless icon in the System Tray.
  - Choose Status.
  - Click Properties.
  - Select the Wireless Networks tab.
  - Select your current network connection.
  - Click Properties, then click the “Association” tab.
  - Uncheck the box next to “This is a computer-to-computer (ad-hoc) network.”
  - Click OK until the dialog boxes disappear.
- Encrypt your data. ITCS recommends you use the fully licensed version of WinZip Pro to encrypt any sensitive data on a computer that will be connected to a wireless network. If your data is encrypted and somebody gets into your PC (either remotely or by stealing it), they won’t be able to read or alter any of your data.
- Use a personal firewall. Windows XP contains a firewall—consult the built-in Windows Help documentation for information on its configuration.
- Turn off file sharing. It’s fine to enable file sharing on your home network, but doing it at a public hotspot invites everyone else to peruse your data. To turn off file sharing:
  - Start Windows Explorer.
  - Right-click on the drive or folders you normally share.
  - Choose “Sharing and Security,” and uncheck the box next to “Share this folder on the network.”
- Ensure the network is legitimate. One of the latest scams is for someone to set up a network (hotspot) themselves in a public location or cyber café and steal your personal information when you connect. Before connecting at a hotspot, ask an employee for the name of the hotspot because someone may have set up a rogue to take advantage of you.

- If you want to work offline, disable or remove your wireless adapter. Remove your external wireless card or disable the wireless network adaptor built into your computer.
- Look over your shoulder. Advanced techniques aren't required for someone to steal your user name and password. A "shoulder surfer" only needs to peer over your shoulder to watch what you're typing.
- Never leave your laptop alone. A thief could even snatch your laptop while you're using it. Some hotspots have ports to which you can lock your laptop via a laptop lock.

### Use Your Head

Responsibility for security rests with everyone connected to the network. Network security is only as strong as its weakest link. Be a strong link!

- Be suspicious—don't believe unknown visitors or phone calls. Confirm identities.
- Use your locks on doors, drawers, and computers.
- Never reveal your password to anybody, including your superiors.
- Never reveal confidential information. Use a cross-cut shredder or hire a shredding service to shred all documents containing confidential information. When in doubt, shred!
- Never install unauthorized or pirated software.
- Never install software from an unknown source.
- If your computer has been compromised, use another (secure) computer to change all your passwords—NOW!
- Microsoft and Symantec do not communicate directly with end users, unless you have subscribed to their official electronic newsletters. If you receive an email purporting to originate from one of these companies, but haven't subscribed to anything, just delete it. You've been spammed with a falsified correspondence (phishing).
- Don't get fooled by the following security fallacies:
  - "I run antimalware software, so I'm secure." Antimalware software doesn't protect against hackers exploiting unpatched security flaws in your software.
  - "I run a firewall, so I'm secure." Firewalls can't protect your computer if your operating system and applications don't have all available patches installed.
  - "I don't care about security because I backup my data daily." That may be convenient for you, but what happens when your computer gets compromised and attacks other computers on which the data isn't backed up? If your computer gets hacked, you will not be able to use it until it is reloaded.
  - "Responsibility for security rests with the IT Security staff."

### Scan for Software Vulnerabilities

Use a verified online tool to scan your computer for software vulnerabilities (e.g., outdated versions of software that need to be updated). Be very careful which tool you use! Many online vulnerability scanners have been posted by hackers to compromise your computer with malware instead of detecting vulnerabilities.

- Secunia Software Inspector works well: [http://secunia.com/software\\_inspector](http://secunia.com/software_inspector)

# Secure Your Home Network

If you have a home network with a broadband connection to the Internet, you must take steps to protect your computer(s) from Internet-based attacks. Remember that your broadband connection is always “on,” so any computer connected to your network is connected to the Internet whenever the computer is running. If you’re not using your home computer, turn it off—nobody can hack a computer when it’s turned off.

If you have a broadband home network, your ISP probably provided you with either a cable modem (for cable TV customers) or a DSL modem (for telephone customers). To further secure your broadband home network, purchase your own router with a built-in hardware firewall that performs Network Address Translation (NAT) to protect your networked computers from Internet-based attacks.

Why you need a router:

Maybe there was a time, in the distant-past, when it was okay to plug your broadband modem (cable or DSL or fiber or satellite, whatever you've got) directly into your computer. Maybe. But doing that today is tantamount to leaving your front door wide open for malicious jerks to deposit trash in your foyer while stealing your hard-earned cash. There should always be something between you and your broadband for protection: a router. Here's why you need one for safety, plus all the other benefits a router provides.

- It’s an Internet splitter. First and foremost, you have multiple devices. They all need Internet connectivity. The router is the “splitter” that makes it happen. By plugging the broadband into the WAN port, you can then get Internet out to all the other devices, both wired and wireless.
- It networks all devices. The ultimate reason to have a router: you have multiple computers, phones, and other devices, not to mention multiple peripherals (printers, etc.). Wouldn’t it be nice if they all talked to each other? The router is the heart of all that communication. The modern “wireless router” does more than handle only Internet traffic. It has a built in Ethernet switch (those are the Ethernet ports for the wired devices on the network) as well as an access point for wireless connections. The AP is the part that handles all the Wi-Fi traffic and security. A wireless router just ties all these functions into one neat package. Even without broadband, the switch/AP can still get every device on the network talking.
- It provides PC safety. Routers typically have two built in firewalls. The first is simple NAT for network address translation, which isn't so much for protection as it is for simply making the Internet connection work to all your computers. The second is SPI (stateful packet inspection). Most modern routers have SPI, which keeps extra track of data in network packets and makes sure it’s proper (i.e., you requested it), protecting both the router and your computers by filtering out the bad. Note that these are not a replacement for software firewalls on your PC—every computer should have one running. Other security you get from a router: limiting a network to just computers you trust with MAC address filtering, secure wireless transmission, parental controls, and web site filters.
- It gives you wireless freedom. Why be tied to one place with your computer or phone? Modern Wi-Fi is the brand name for a technology called 802.11, which comes in many flavors, all with different speeds and ranges. Buy 802.11n products, especially if they’re dual-band, and you’ll be covered. They’re slightly more expensive, but you get what you pay for. In this case, you’ll have speed almost as good as a wired network, with extended range. The performance is improved even in spots where signals used to get hung up. You can move around and stay connected, even in your own home or office.

The router, which may include a wireless access point for wireless networking, should be wired between your ISP-provided modem and your computers. *You must configure your router properly to protect your network.* Follow

the directions provided by the router manufacturer to configure the router so it provides maximum security for your networked computers:

- Check the manufacturer's website to ensure your router is using the latest firmware version. Your owner manual will have directions for determining the version and updating it.
- All routers have a default password for administrative access. Change the default password immediately to prevent hackers from taking control of your router and your network. Use a strong password according to standards defined elsewhere in this document.
- All routers have a default network name, called the SSID (Service Set Identifier). This identifies your brand of router to casual hackers who may know of security flaws in the router (especially if you didn't change its default password). Change the default SSID immediately.
- If you are not going to use wireless networking, disable the wireless networking in the router's configuration menu.
- If you are going to use the wireless networking capabilities built into your router, follow the directions in your owner manual to:
  - Encrypt your network traffic using Wi-Fi Protected Access (WPA or the improved WPA2), which provides authentication and encryption for wireless networks. Do not use Wired Equivalent Privacy (WEP), which is outdated and easily cracked.
  - Use an Access Control List (ACL) based on the Media Access Control (MAC) address of each network card in each of the computers you want to connect to your network.
  - Disable broadcasting of the SSID of your home network.

# Secure Your Data

## Data Ownership and Responsibility

You are responsible for the data stored in your head, on your computer, and on your paper—including any consequences arising from its misuse.

Computers can store vast amounts of information, which is good and bad. For instance, you could create a computerized inventory of all your personal property—model numbers, serial numbers, dates of purchase, and prices. This information would be useful to your insurance agent if your house burned down and your insurance would replace your possessions. That's convenient. That's good.

Now for the downside...Your home computer that stores all that information can crash and lose all your data. If you backed up your data, you have the computer reloaded and copy the backed-up data to the newly-loaded computer. If you didn't backup the data, it's gone—you have to recreate the entire list from scratch. That's inconvenient. That's bad.

But it can get worse...Remember when your computer crashed? It didn't just crash—it got hacked, *then* it crashed. Somebody you've never met took control of your computer and got access to all of your files, including your inventory list. Remember the other stuff you entered in your computerized inventory—bank accounts, credit card numbers, Social Security number, driver license number, date of birth, car VIN number? Somebody else now has your personal information—and they can sell it on the Internet so someone can steal your identity. This scenario occurs thousands of times every day and is an important source of income for international organized crime.

## Data Storage Guidelines

- Backup your data daily, then store your backed-up data securely.
- Deleted data can be recovered...maybe. The process is complex, expensive, and rarely recovers all deleted data. ITCS does not provide or fund data recovery services, although we can advise you about hiring a data recovery service to recover your data at your expense. There is no substitute for regularly scheduled data backup.
- Storage of Social Security Numbers is forbidden unless you have obtained permission from the Registrar. Contact the University Help Desk for information.
- Never copy or download sensitive data from the University's administrative systems. These systems have strong security controls to protect the sensitive data—much stronger than a normal computer.
- If your job requires that you download data from administrative systems, keep in mind that you are personally responsible for that data. You are also required to get written permission to store the data—call the University Help Desk for information. When storing sensitive data, you should implement additional security controls such as:
  - Remove the confidential part of the information if it is not needed (e.g., Social Security number, date of birth).
  - Store the data on a secured server, not on a workstation or laptop.
  - Store the data on Piratedrive rather than your workstation or laptop.
  - Encrypt the data. Refer to the following section named "Data Encryption" for more information about encryption.
  - Physically secure any data storage device that can be easily moved.

- Dedicated web servers or any computer running web server software (e.g., “personal” web servers) must never be considered secure and should never be used to store sensitive data.
- Do not create databases or applications that use Social Security numbers. Create a unique identifier that does not use the SSN or any part of it.
- Email is not secure, so you should not send sensitive data via email. If you must email sensitive data, it should be encrypted.
- Protect sensitive data that is printed.
  - Store it in a locked desk, drawer, or cabinet.
  - Do not leave sensitive data unattended on a copier, fax machine, or printer.
  - Shred all paper containing data you wish to delete. Do not use a shredder that produces long strips of shredded documents—they can be reassembled into their original format. Use a “cross-cut” shredder that renders documents into small pieces resembling confetti.
- Secure your workstation by following the suggestions in the section of this document titled “Secure Your Computer.”
- Ensure that all data is wiped (not just deleted) from your computer before it is transferred to someone else or surplused, as required by the University Disk Sanitizing Policy. Hackers can recover your deleted data, even from a freshly formatted hard drive. If you need to have a computer sanitized, contact the Help Desk at 328-9866 and open a Service Request.

### **Data Encryption**

Encryption is a method of scrambling data so that only someone who possesses the appropriate password or “key” can access the information. Encryption can be a confusing subject because there are so many different types of encryption that can be used to protect data. Currently, the most desirable type of encryption is called AES (Advanced Encryption Standard). AES encryption is available in different strengths, expressed in “bits”—the more bits, the stronger the encryption. The current US government standard for data encryption is 256-bit AES encryption.

- WinZip is an application familiar to many people for its ability to compress the size of data files. The licensed version, named WinZip Pro, can encrypt files using 256-bit AES encryption. Although ECU does not have a site license for WinZip Pro, the application is recommended and supported by ITCS. WinZip Pro 12 can be purchased and downloaded from the WinZip website at <http://www.winzip.com> in single-user or multi-user licensing formats.
- If you have sensitive data stored on a workstation or (especially) a laptop computer, you should encrypt the sensitive data to protect it from unauthorized access or theft.
- Flash drives, also known as thumb drives, are popular for transporting data between computers. Sensitive data stored on flash drives should be encrypted using 256-bit AES encryption. Some flash drive manufacturers like SanDisk include an encryption program with some of their flash drives. The encryption program can be used to divide the storage on the flash drive into two areas of variable sizes—one area for encrypted data and one for unencrypted data.
- Email is not considered a secure method of communication. However, if you must send sensitive information via email:
  - Encrypt the data.
  - Include the data in an email as an attachment
  - Send the password required to decrypt (open) the encrypted data to the recipient under separate cover (e.g., a separate email, telephone call).
  - The recipient will also require a licensed copy of WinZip Pro to decrypt the encrypted data.

# Updating Microsoft Software

Older versions of Microsoft Windows (e.g., 3.x, 95, 98, Windows NT 4, Windows 2000) are no longer supported by Microsoft and cannot be secured against modern security threats. If your computer runs any of these operating systems, you need to upgrade to Windows XP or Windows 7 immediately. The following guidelines apply to computers running Windows XP (with Service Pack 3) and Windows 7, although they may also apply to other operating systems.

*You must use the following resources to ensure the security of your Windows computer:*

- Microsoft Update (in Windows XP) or Windows Update (in Windows 7)
- Microsoft Baseline Security Analyzer (download from Microsoft website)

## **Microsoft Update (Windows XP) or Windows Update (Windows 7)**

To access the Microsoft Update website:

- Exit all applications except your antimalware program (don't just minimize them to the Task Bar).
- Select on the Start button on the Task Bar in the Windows desktop.
- Select "Microsoft Update" or "Windows Update" from the Start Menu. This will connect you to the Microsoft website if your computer has Internet access.
- When the Microsoft website opens, you may be required to install software required to access the site. Select "Yes" to install it.
- If you have never updated your computer before, you may need to visit the Microsoft website, install patches, and reboot several times to download all available patches. Keep updating and rebooting until you have no more updates available for your computer.
- In Windows XP, after all Express updates are installed, select the "Custom" button and install the latest versions of Internet Explorer and Media Player. You may find other updates listed under Custom, which may be required to improve your computer's functionality. You may need to visit the Microsoft Update site several times to update the updates you have just installed.

## **Automating Microsoft Update/Windows Update**

If you do not set Update to run automatically, you must check the Update website daily for critical updates.

- If you use Windows XP, set your computer to update automatically as follows:
  - Right-click on My Computer on the Windows desktop.
  - Select "Properties" from the menu.
  - Select the "Automatic Updates" tab in the System Properties window.
  - Select "Automatic" and specify a time of day when you know your computer will be turned on.
  - Select "OK" to save your choices.
- If you use Windows 7, set your computer to update automatically as follows:
  - Open the Start Menu, then select "Control Panel"
  - In Control Panel, select "Windows Update, then select "Change Settings""
  - Choose "Install updates automatically" and select a time the updates should be installed. Note the computer must be turned on at this time or the updates will not be installed.
  - Select the checkboxes for "Recommended updates," "Who can install updates," "Microsoft Update," and "Software Notification." Click the "OK" button.

### **Microsoft Baseline Security Analyzer (MBSA)**

- Free utility from Microsoft that scans the following software in addition to the operating system:
  - Microsoft Office applications
  - Microsoft Internet Explorer browser
  - Microsoft Internet Information Server (web server)
  - Microsoft SQL server
- Microsoft changes the download location for this utility without notice, so use an Internet search engine (e.g., Google) to find its current location for downloading.
- MBSA reports missing hotfixes.
- MBSA makes suggestions for securing the computer in addition to hotfixes.

# Applying Patches to a New Computer

If you are installing a new computer or reloading an old one, you must finish ALL steps in this section before the computer can be left connected to the ECU network. *If you cannot finish ALL these steps at one time, DO NOT LEAVE THE UNPATCHED COMPUTER CONNECTED TO THE CAMPUS NETWORK FOR ANY REASON! Turn off the computer or disconnect the network cable immediately until all the following steps have been completed.* Failure to do so will result in the computer getting compromised—sometimes within minutes. Then you'll have to reformat the computer and start all over again.

*Before* connecting to the ECU campus network:

- Install the operating system or image from a CD-ROM.
- Install the latest operating system Service Pack from CD-ROM.
- Install the latest version of our site-licensed Symantec antimalware software from a CD-ROM.

*As soon as* you connect to the ECU campus network, complete the next steps immediately:

- Update your antimalware definitions before adding any other files to the computer (required by ECU Antivirus Policy)
- Go to Microsoft Update website and install all critical updates. This may require several reboots of your computer.
- Reboot and return to the Microsoft Update website until you have downloaded all critical updates.

Install the latest version of Microsoft Office, then:

- Go to the Microsoft Update/Windows Update website.
- Install all available updates.
- Reboot.

Install the Microsoft Baseline Security Analyzer (MBSA) and run it to see if any patches are missing. MBSA scans the Windows operating system, Microsoft Office applications, the Internet Explorer browser, Internet Information Server, and SQL Server. Apply all available patches, then check for new patches daily.

# When Your Antimalware Software Detects Malware

## Pay Attention

You must ensure that the latest version of your antimalware program is installed on your computer (not just the latest definitions, but the latest version of the entire program). Antimalware programs are normally updated as soon as security vulnerabilities are discovered. The newest version of the program is the most secure.

The antimalware program on your computer will communicate with you—pay attention to these messages. Ignoring this vital information can result in loss of all your data, an unplanned format of your hard drive, and subsequent reinstallation of your operating system and all applications.

## Appropriate Responses to Notices

Your appropriate response to malware notices from your antimalware program varies according to what your computer is doing when the notice appears:

- Retrieving email. If the notice states, “Quarantine successful,” relax. Your antimalware program has prevented the malware from reaching your computer.
  - Document the name of the malware.
  - Notify your coworkers that you received an infected email and ask them to update their virus signatures to ensure that they will be protected if they receive an email containing the same malware.
  - You do not need to take any further action. Do not send an email to the person on the “From” line of the infected email because the source of the email has probably been spoofed (forged).
- Installing new antimalware definitions. Your computer is infected by a new form of malware that your old definitions did not protect against.
  - The new definitions probably cannot fix the infection by themselves without the use of an additional specialized program created to remove this specific infection. Failure to run this additional program will result in the “removed” malware reloading every time you reboot your computer.
  - Immediately follow the directions in the following section named “When Your Computer is Infected.”
- Manually scanning files on your hard drive. Your computer was infected in the past by malware that arrived before updated virus definitions that could recognize it.
  - The new virus definitions may be able to fix the infection.
  - Immediately follow the directions in the following section named “When Your Computer is Infected.”

## When Your Computer is Infected

If your antimalware program identifies a malware infection already present on your computer, you must take action immediately. A malware infection will not go away by itself and it can spread from your computer to other computers on the campus network and the Internet.

- The antimalware software installed on your campus computer will attempt to repair the infected file. If the file is successfully repaired and nothing is placed in Quarantine, you do not need to take any further action other than notifying your coworkers so they can check their computers for infection.
- If the file cannot be repaired, the antimalware program will place it in Quarantine to protect your

computer. If this happens and your computer is connected to the ECU campus network:

- Leave the antimalware program's notification message displayed. Write down the exact name of the infection and the time it was detected. This information is critical to determine the steps required to fix your computer.
- Do not reboot or turn off your computer. This may result in your hard drive being formatted, which permanently erases all your data.
- Call IT Support Services at 328-9866 immediately for instructions. Support staff will need to know the exact contents of the message displayed on your computer.
- Tell the Support representative exactly what the virus notification message says, especially the name of the infection. Some infections will require a qualified technician to manually repair damage to your computer's operating system and applications. Simply deleting infected files may not fix your computer and may put other networked computers at risk. You may be required to disconnect your computer from the campus network to prevent the virus from spreading. According to University policy, an infected computer must be disconnected immediately from the campus network until it is repaired.
- Do not delete files placed in Quarantine until a qualified technician determines that deleting those files will not harm your campus computer.
- Never attempt to repair any malware infection without specific up-to-date information.
  - Check the Symantec Security Response website at [http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp) for complete descriptions and removal instructions for the malware on your computer.
  - You may need to run a removal tool (cleaning program) written to clean your specific infection. If you neglect to run it as directed, the malware will reload as soon as you reboot your computer.
  - Symantec displays the latest malware threats and also contains a searchable online virus encyclopedia containing details of all known malware.

# How to Avoid Malware Problems

The most important component of malware protection is *you*. Use safe computing practices to protect your computer and its contents.

## Malware Types

- **Virus:** A self-replicating program, often written to cause damage or mischief, which inserts itself into a software application without leaving any obvious sign of its presence. Your computer can pick up a virus when you copy an apparently normal file from a diskette, CD, or memory stick, when you open an infected email attachment, or when you download an infected file from the Internet.
- **Worm:** Like a virus, a worm is a self-replicating program, often written to cause damage or mischief. Unlike a virus, a worm is self-contained and does not need to become part of another program to propagate itself. Instead a worm infects the operating system, acts like a program in its own right, and spreads via the network.
- **Trojan horse:** A malicious program that appears to be innocuous or even beneficial, but conceals other malware that can compromise the security, data, and proper functioning of your computer. Trojan horses spread via the network and are sometimes referred to as “network viruses.”
- **Spyware:** Programs that scan systems or monitor activity and relay information to other computers or locations in cyberspace. The information that may be actively or passively gathered and disseminated by spyware may include passwords, log-in details, account numbers, personal information, individual files, or other personal documents. Spyware may also gather and distribute information related to your computer, applications running on your computer, Internet browser usage, or other computing habits. Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. Spyware can be downloaded from web sites (typically in shareware or freeware), email messages, and instant messengers. Additionally, a user may unknowingly receive and/or trigger spyware by accepting an End User License Agreement (EULA) from a software program linked to the spyware or by visiting a web site that downloads the spyware with or without a EULA.
- **Adware** enables delivery of advertising content to you through its own or another program’s interface. Adware may gather information from your computer, including information related to Internet browser usage or other computing habits, and relay this information back to a remote computer or other locations in cyberspace. Adware can be downloaded from web sites (often in shareware or freeware), email messages, and instant messenger programs. You may unknowingly receive and/or trigger adware by accepting a EULA from a software program linked to the adware or by visiting a web site that downloads the adware with or without a EULA.
- **Backdoor:** Software that bypasses normal authentication methods, such as a username and a password, and allows unauthorized people to access and control your computer without your knowledge. A backdoor may take the form of an installed program or an illegitimate modification to a legitimate program. Trojan horses are a common kind of backdoor threat.
- **Blended threat:** An attack on your computer from the network specially crafted to maximize the severity of damage and speed of infection by combining several kinds of malware. This could be a combination of a virus and a worm that also takes advantage of vulnerabilities in your computer and the network to which it is connected, or virus sent to you as an email attachment along with a Trojan horse embedded in a HTML file that is part of the email message.
- **Keylogger:** Spyware that records your keystrokes and sends the information to someone else without your knowledge. Keyloggers spread most commonly by email attachments or in a drive-by download when you

visit a specially crafted website. Keyloggers are often used to gather email and online banking usernames and passwords as a prelude to identity theft.

- Rootkit: Hides files or processes running on a computer, rendering them difficult to detect and remove. They can be installed by other forms of malware, like worms, which gain entry to your computer without your knowledge or permission. Rootkits are popular with hackers, who want to hide their nefarious activities on your computer.

### Avoiding Malware

- Keep all software up to date, especially your operating system, browsers, and antimalware applications. Check for updates to your operating system and all applications daily.
- Turn off your computer if you are not using it. If your computer is turned off:
  - It can't get infected by malware or hacked.
  - It can't be damaged by electrical voltage fluctuations or outages.
  - It will contribute to saving ECU thousands of dollars every month in electric bills.
- Backup your data *every day*. Data that is not backed up should be considered expendable. If your computer gets damaged by malware or just breaks and you lose your personal data, you have nobody to blame except yourself.
- Use the latest version of antimalware software with the latest version of the virus definitions. Update your definitions daily, before retrieving any e-mail.
- Never open any e-mail attachment, regardless of its source. Save the file to your computer's hard drive and scan it for viruses.
- Scan all files downloaded from the Internet for malware before you use them.
- Malware hoaxes
  - Don't believe every malware warning you receive—some are hoaxes. Malware warnings at ECU are distributed solely by the IT Security team. Virus warnings from any other source should be regarded with suspicion and reported to the Help Desk.
  - In a practice called *phishing*, you may receive unsolicited e-mail purporting to be from Microsoft or Symantec. It's a hoax, and may even be infected with a virus. Neither company sends unsolicited e-mail to users.
  - You can check the validity of a malware warning by accessing the Symantec Security Response web page at [http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)
- Don't use peer-to-peer (P2P) file sharing software (e.g., Kazaa, gnutella, BearShare, Grokster, Morpheus, Napster, LimeWire, BitTorrent, Skype, etc.). This software is inherently insecure and can share the entire contents of your hard drive with the Internet! Many new types of malware target P2P users exclusively.
- Don't click on anything inside a pop-up window to close it. Click on the "X" in the upper-right-hand corner to close the pop-up window.
- Adjust your browser to block pop-up windows.
- Don't click on links within pop-up windows—they may install spyware on your computer.
- Close pop-up windows by clicking on the "X" in the window's title bar. Don't use any buttons (e.g., Yes, No, or Close) within the pop-up window—you have no way of knowing what those buttons might do.
- Beware of "free" downloads that may install software on your computer without your knowledge or permission.
- Don't use add-on menu bars in your Internet browser.
- Don't use third-party search engines for your hard drive.
- Don't use shopping programs (e.g., Claria, formerly named Gator).
- Don't use coupon programs.

- Don't use any program that offers to save your userids or passwords for you.

Modern antimalware software can detect spyware, adware, and rootkits. Free software can be used in addition to your main antimalware program to provide multiple layers of protection:

- Malwarebytes from Malwarebytes.org: <http://www.malwarebytes.org>

# System Maintenance for the PC

## Check Disk

Run Check Disk weekly to check your hard disk for damaged files that degrade performance. It must be run separately on each partition on your hard drive, as follows:

- Double-click the My Computer icon, then:
- Right click the appropriate Drive icon, select Properties, select the Tools tab.
- Click the Error Checking button.
- Click the Check Now button.
- In the Check Disk Options, select both options by clicking on the boxes preceding them. You should now have a check in each box.
- Click the Start button to begin checking the hard drive.
  - You may need to reboot your computer for the disk to be checked.
- Repeat for any other partitions on your hard drive.

## Disk Defragmenter

Run Disk Defragmenter weekly to increase system speed. It must be run separately on each partition on your hard drive. In Windows 7, you can configure this utility to run automatically. To start the utility:

- Double-click the My Computer icon.
- Right click the appropriate Drive icon, select Properties, select the Tools tab.
- Click the Defragment Now button.
  - Select the partition you want to defragment.
  - Click on the “Defragment Now” button.
  - Repeat on each of your hard drive’s partitions.
- This utility will require several minutes to defragment each partition on your hard drive. The longer you wait to defragment your hard drive, the longer the defragmentation will take.

# How Hackers Work

## Technical Hacking

Computers lacking the latest service pack, security patches, and updates for the operating system and all applications *will* get hacked. Hackers use automated scripts to look for weaknesses (usually well-known vulnerabilities in operating systems or applications). When these vulnerabilities are discovered, the hacker uses them to compromise the security of the computer and gain elevated privileges without authorization. In this document, we'll consider a hacker to be somebody who takes complete administrative control of a computer without permission—the most common cause for hacking reports at ECU. If a computer has been hacked in this way:

- The hacker is now the administrator, and you are trying to break in to *his* computer!
- The hacker can add, delete, or modify any file or application on the computer—including your data.
- The hacker can setup a rogue file serving application on your computer. Then, the hacker and his cronies load illegal copies of copyrighted materials (music, video, or data) on your computer and use your computer to deliver these materials on demand to their subscribers. In this situation, the computer user is liable for the illegal materials (because it's your computer) and the University is liable (because the University's network is used for illegal distribution).
- The computer must be disconnected from the network immediately and must not be reconnected for any reason until it has been fixed by a qualified technician. Fixing a hacked computer is not a job for amateurs.
- The computer's hard drive must be formatted and/or re-imaged. Do not simply reload the OS and applications over the currently installed (and compromised) version.

Our experience with multiple hacked computers at ECU has shown that hackers don't install a single backdoor on a hacked computer—they install multiple backdoors. If an investigator finds a rogue software package and deletes it, the hacker will use another pre-installed backdoor to regain access—sometimes within a few minutes. If a computer has been hacked, the hard drive must be formatted, the OS and applications reloaded, and the data restored. There are no shortcuts.

## Social Engineering

Hackers don't always use mysterious high-tech methods to gain unauthorized access. Many of the most successful security breaches result from social engineering. Social engineers are nothing more than con artists who prey upon your social graces and good intentions—friendliness, politeness, and desire to help others. Like any other predator, a social engineer will attack the weakest perceived link first. With all of today's technology and protection, you can be the weakest link.

Hackers can attempt to deduce your network's infrastructure through the use of technology based tools, which are available on the Internet. However, this approach requires considerable time and experiences a high failure rate. Hackers realize this and often try the simplest approach to breaking into a system—they ask permission. They try to get unauthorized access by simply asking for it. They try to appear genuine when they apply their bag of tricks.

Social engineers move slowly when gathering intelligence about their target. A small piece of data may seem harmless by itself. However, when compiled, many small pieces of data can become a hacker's road map to an organization or a network. Some of their favorite exploits are:

- Telephones. Telephones aren't just appliances—they're taken for granted as part of our social and business structures. We tend to lower our guard when using the telephone—how else would telemarketers be so successful? Hackers know this, and they often try to take advantage.

- Masquerading. Social engineers use the phone or email to pretend to be someone they're not. Potential attackers will often appeal to someone's ego by challenging the person's question-answering skills. Or they may appeal for sympathy to gain information. They may pretend to be someone who is authoritative, demanding information by way of intimidation. They may fabricate an emergency. It's human nature for most of us to want to be helpful and trusting. However, in our efforts to do something helpful, we may be providing information to the bad guys. Don't be paranoid, just be aware and use common sense.
- Phishing. Criminals send out spam email with forged headers to draw gullible people to fake websites where they enter their sensitive information (e.g., account numbers, userids, and passwords). These data are then used for direct financial fraud or wider identity theft. Read more about phishing in the "Identity Theft" section of this document.
- Dumpster diving. Sifting through the trash isn't a glamorous approach to stealing information, but it's very effective. Imagine what a person could find in your trash at home. Would there be any receipts, bills, bank statements or personal notes?

Once social engineers have conducted a general reconnaissance, they progress to the next phase—getting more information by selecting an unsuspecting person or a key position in a company to attack. Favorite targets are:

- Help Desk/support areas. The single most important role that these areas play is to help people. Social engineering attacks focus on these groups because they typically have the ability to give out passwords and other sensitive information.
- Receptionist/administrative areas. These folks hold the keys to the organizational structure. They often have access to information on behalf of the executives for whom they work, so they often become targets for an attack.

The final phase is to execute the attack based on the information gathered and the target identified. This is when the phone calls begin, the phony mass mailings are initiated, and the game is afoot.

What should you do to prevent being exploited by social engineers?

- Shred all documents before discarding them at work or at home. You may not consider a particular document important, but that doesn't mean an identity thief or social engineer can't use it against you or your employer.
  - Older shredders cut documents in only one direction and the shredded strips lay in neat piles. Using tape and patience, one can reassemble these documents. Use a *crosscut* shredder that cuts paper into small pieces resembling confetti.
  - Do you shred all your sensitive documents? Shredding only the sensitive documents calls attention to the information that the hacker really wants.
- Never reveal your password to anyone, *including your coworkers and superiors*. Your superiors do not have the authority to know your password. If any ECU employee pressures you to reveal your password, they are committing a serious violation of University policy. Notify ECU Human Resources immediately. Your anonymity will be protected.
- If it doesn't feel right, then trust your instincts and err on the side of caution. To be more specific, this doesn't mean that you should be rude and uncooperative, it means that you should raise your awareness of your surroundings and to whom you are speaking. Most people won't fault you for being cautious.
- Place a value on information. For example, your Social Security number is private and should never be given to a stranger or provided online unless you can prove that the receiver of it is authentic.
- Deepen your understanding of how one piece of information, such as an organization chart or floor plan, can help an attacker begin to know too much. Ask yourself why someone would need certain information.
- Don't assume that the individual with whom you are speaking is who he says he is. Ask for identification

from strangers in your work area. If you feel uncomfortable speaking with someone questioning you on the telephone, offer to call them back. Then tell somebody—your coworkers or supervisor—about your experience. You may all have been contacted by the same social engineer in a coordinated attack.

- Don't violate policy to "help" a friend or associate. Example: Don't allow "piggybacking" when entering a badge protected area. Piggybacking is allowing people to follow you into a secure area without them actually using their own badges or access credentials. Holding the door open to your secure office area for someone that you don't know is an example of piggybacking.
- Don't be a mark. We all have a personality signature. This could include anything from our daily drive to work, trip to the coffee shop or jog in the park. If you were to track your daily activities for one week, you would probably see a pattern. This pattern is part of your personality signature. Be aware of your personality signature, because this is the type of information that a hacker can leverage against you.
- Use common sense. Don't let your desire to be helpful and trusting overcome your basic instincts and responsibility to keep private information where it belongs.

Be careful. Be suspicious. Be the strongest link in the security chain.

# Is My Computer Compromised?

Your computer can be compromised by a hacker or by malware without human intervention. In either case, something malicious has been done to your computer without your knowledge or permission.

Indications that your computer may be compromised:

- The computer been particularly sluggish lately. It takes longer to start than it used to and applications open slower than they used to.
- The computer locks up or shuts down unexpectedly.
- Your Internet connection slows down.
- Pop-up windows appear, but you didn't open any application.
- The hard drive activity light continues to blink continually after the computer has been running for more than 60 seconds.
- The hard drive is full (especially if you had plenty of space yesterday).
- Your antimalware program stops working.
- You can't connect to antimalware sites on the Internet.

Running certain types of software greatly increases the probability your computer will get compromised.

- P2P (peer-to-peer) file sharing software (e.g., Kazaa, gnutella, BearShare, Grokster, Morpheus, Napster, LimeWire, BitTorrent, Skype, etc.).
  - P2P software can include RATs (Remote Access Trojans) in the original installation files.
  - Even if the original software installation didn't compromise the computer, many worms now target P2P software and as a means of propagating.
  - P2P software advertises your computer's contents on the Internet, thus helping hackers identify your computer as a target.
  - P2P software uses University network bandwidth, which ECU pays for according to usage (if the bandwidth goes up, so does the bill).
  - Installation of this software by ECU staff/faculty/students does not violate University policy. However, use of this software to share *any* copyrighted material (music, video, or data) violates University policy *and* federal law. It is considered grounds for termination.
  - P2P software represents an unpatchable security vulnerability, which must be eliminated if you want your computer to be secure. If you want your computer to be secure, delete all P2P software.
- Chat or Instant Messaging software
- Search assistant software
- Internet-based games
- Aftermarket screensavers.

# If Your Campus Computer is Compromised

(or if you suspect it might be compromised)

## React Quickly

- Remain calm, but act quickly. Once a computer has been compromised, the unscrupulous individual who controls it may use it as part of an organized attack on other computers, websites, companies, governments, or the entire Internet. *Evaluating and fixing a compromised computer is a job for a professional. Do not attempt to evaluate or fix the problem on a campus computer yourself. Immediately call the Help Desk at 328-9866 for directions.*
- According to University policy, compromised computers must be disconnected from the ECU network *immediately* by whatever means is necessary (turn off computer, disconnect network cable, deactivate network port). The computer must not be reconnected until it has been checked by a qualified professional—no exceptions.
- Does the compromised computer have any drives mapped to other workstations or servers? If so, the other computer(s) with the mapped drive(s) must be checked immediately to rule out a hack.
- Did anyone enter any passwords to any other systems while using the compromised computer? If so, *all* those passwords from *all* those users must be considered compromised and changed *immediately* using other computers known to be trustworthy.
- The compromised computer's hard drive should be formatted and all software reloaded—especially service packs, security patches, and antimalware software.
- When moving data to an alternate location before formatting/reloading a compromised computer, don't map a drive to another computer. The same creep who compromised that workstation may go after the server while you're transferring the files. Use a thumb drive or external hard drive to backup the user data offline.
- After the format/reload is finished and *before* the user logs on again, ensure that he/she has changed *all* personal passwords for all systems used (email, MVS, FRS, SIPS, etc.) from another (trusted) computer.
- If a server has been compromised:
  - It should be formatted and reloaded before being reconnected to the ECU network.
  - Ensure that all users connecting to that server immediately change all their passwords (email, MVS, etc.).
  - All passwords on all software apps installed on the server must be changed immediately. Passwords should never be re-used.

## Can't Somebody Just "Clean" My Compromised Computer?

No! The *only* way to clean a compromised system is to format and reload it from scratch.

- You can't clean a compromised system by patching it. Patching only removes the vulnerability, not the attack results. Once an attacker gets into a computer, assume that he installed several other ways to get back in. Never assume that only one attacker got in.
- You can't clean a compromised system by removing the backdoors because you can't guarantee that you found all the backdoors the attacker installed. Just because you can't find any more may only mean you do not know where to look, or that the system is so compromised that what you are seeing is not actually what is there (e.g., root kit).
- You can't clean a compromised system by using a "vulnerability remover." Let's say your system was compromised by a worm that gave the attackers full remote control of your computer. Several trustworthy vendors will provide tools to remove the infection. Can you trust the "formerly

compromised” system after the tool is run? If the system was vulnerable, it was also vulnerable to more than one attack by more than one person. Can you guarantee that only one hacker using only one attack tool gained unauthorized access to the system?

- You can't clean a compromised system by using an antimalware scanner. A fully compromised system can't be trusted to tell you the truth. Even antimalware scanners must at some level rely on the system to not lie to them. If they ask whether a particular file is present, the attacker may simply have a tool in place that lies about it. If you can guarantee that: the only compromise in the system was a particular virus or worm, *and* you know that this virus has no backdoors associated with it, *and* the vulnerability used by the virus was not available remotely, then an antimalware scanner can be used to clean the system. For example, many e-mail worms rely on a user opening an attachment. In this particular case, it is possible that the only infection on the system is the one that came from the attachment containing the worm. However, if the vulnerability exploited by the worm was accessible remotely without user action and you cannot guarantee that the worm was the only thing that exploited that vulnerability, it is entirely possible that something else used the same vulnerability. In this case, you can't just patch the system.
- You can't clean a compromised system by reinstalling the operating system over the existing installation. Again, the attacker may very well have tools in place that can lie to the installer. If that happens, the installer may not actually remove the compromised files. In addition, the attacker may also have put backdoors in non-operating-system components.
- You can't trust any data copied from a compromised system. Once an attacker gets into a system, all the data on it may be modified. Copying data from a compromised system and putting it on a clean system will, in the best-case scenario, give you potentially untrustworthy data. In the worst case, you may actually have copied a backdoor hidden in the data that will re-compromise the rebuilt system. Or you may have copied a `Logic bomb` that deletes your data at some future time and then deletes itself.
- You can't trust the event logs on a compromised system. Once an attacker gets full access to a system, it's easy to delete the event logs on that system to cover his tracks. If you rely on the event logs to tell you what the attacker has done to your system, you may just be reading what they want you to read.
- You may not be able to trust your latest backup. How can you tell when the original attack took place? The event logs cannot be trusted to tell you. Without that knowledge, your latest backup is completely useless. It may be a backup that includes all the backdoors currently on the system.

It's a real pain to reload a computer from scratch—it's time consuming and inconvenient. That's another reason to keep your computer secure in the first place—so it doesn't need to be reloaded!

# Identity Theft

Guard your personal information as if it's your most important asset—*because it is*. We've all heard horror stories about fraud that's committed by stealing a name, address, Social Security number, credit card, etc. If someone steals your personal information, they can gain access to your assets within hours. They can buy cars or take out mortgages in your name—and *you* have to prove that you didn't do it. In the meantime, your credit rating and reputation are damaged.

## North Carolina Identity Theft Protection Act

The North Carolina Attorney General's Office maintains a website at <http://noscamnc.gov/yourself.html> that provides instructions showing you how to:

- Get a free copy of your credit report annually from all three credit reporting agencies. (If it contains any incorrect information, take action *immediately!*)
- Opt out of pre-approved credit offers.
- Prevent non-essential access to your credit information with a Security Freeze.

## Additional Identity Theft Protection

The first step in protecting your personal information is to avoid giving it away in the first place.

- Prevent telemarketers from contacting you by entering your telephone numbers on the National Do Not Call List at <https://www.donotcall.gov>.
- Use strong passwords. If someone guesses your weak password and breaks into your account (e.g., email, bank, credit card), you have nobody to blame except yourself. See "Secure Your Computer" section in this document for advice about creating strong passwords. If a computer you have used to enter passwords ever gets compromised, use another computer (one you know is not compromised) to change all your passwords immediately.
- When using a computer or accessing a website, never use an option to "remember my password the next time." This option will store your password in a standard location on the computer, which is the same as writing it down—and just as bad. If your password is stored, it can be found and used against you.
- Expect someone to read any document you discard.
  - Get a paper shredder, then use it. Old-fashioned shredders produce long strips of paper that can be reassembled into the original documents. Get a crosscut shredder that shreds paper into long strips, then chops the strips into tiny bits resembling confetti.
  - Shred all documents. If you only shred some documents, you're helping identity thieves identify your important documents. Be especially diligent in shredding unsolicited credit card applications and unused checking deposit slips.
- Beware of *shoulder surfers*—people who look over your shoulder at your computer monitor or keyboard. If they've got a camera or a camera-equipped cell phone, they can record the keystrokes of your ID and password and your personal information displayed on the monitor. They can also take pictures of your credit cards, including expiration dates.
- Guard your checking account.
  - The next time you order checks, have only your initials (instead of first name) and last name put on them. If someone takes your check book, they won't know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.
  - When writing checks to pay your credit card accounts, don't put the complete account number on

the “For” line—just write the last four numbers. Your credit card company knows the rest of the number, but anyone handling your check as it passes through all the check processing channels won’t have access to it.

- Put your work phone number on your checks instead of your home phone. If you have a P.O. Box, use that instead of your home address. If you do not have a P.O. Box, use your work address.
- Never have your Social Security number or driver license number printed on your checks. You can add them if required. But if you have them printed, anyone can get them.
- Copy the contents of your wallet on a photocopy machine—copy both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopies in a safe place. Also carry a photocopy of your passport when traveling in the U.S. or abroad.
- Don’t use public workstations for e-commerce, to check your email, or access your bank accounts. Many of these computers have been infected with keyboard loggers, programs that capture every keystroke and send the information to a remote location. When you type your name and password, they are recorded for exploitation.
- The Fight Identity Theft website contains useful information for avoiding and responding to identity theft: <http://www.fightidentitytheft.com> .

## Phishing

Beware of *phishing*—a form of social engineering in which criminals send out spam with forged headers to draw people to fake websites where they enter their sensitive information (e.g., account numbers, userids, and passwords). These data are then used for direct financial fraud or wider identity theft. Reading your email and browsing the Internet is fraught with dangers that passive protections such as firewalls can’t stop. You need to be suspicious.

- Does the company have your email address? Do they normally contact you via email? Does the salutation of the email contain your name or account number? A valid communication from a real company would contain information specific to you.
- If you receive an email containing a threat to close your account or terminate service, don’t be intimidated into divulging confidential information. Think about it—legitimate business entities normally notify you of problems via United States Postal Service, not email. If you’re worried by a threatening email, contact the business entity using contact information you already possess—don’t use the contact information in the suspect email.
- Phishing is an international curse. Formerly, many phishers didn’t speak English very well, so their email scams contained errors in spelling and/or grammar. Unfortunately, the con artists have polished their language and presentation skills. They may even include some of your stolen information in an effort to dupe you into revealing more.
- One of the most common phishing techniques provides an official-looking email message with a clickable URL that appears to link to the vendor site. In reality, the apparent URL is merely the text that disguises a link to a site that gathers personal information entered by unsuspecting visitors. You should develop the habit of checking the validity of a link before you click it. If your email client supports it, you can usually mouse-over the suspect link and display its actual URL in the status bar at the bottom of the screen (this also works in Internet Explorer if the status bar is enabled). Because messages with such embedded links are sent in HTML format, you can also typically right-click the message and select “View Source,” which displays the message’s HTML source code. With a little effort, you can usually sort out the suspect URL from the morass of HTML tag information.
- Confirm *all* unsolicited communications:
  - If you receive an unsolicited email allegedly from a company with which you conduct business,

assume it's a scam until proven otherwise. Confirm its authenticity by calling the company at a telephone number you already possess (e.g., on the back of your credit card). Don't use any phone number or link contained in the email.

- If you receive an unsolicited phone call allegedly from a company with which you conduct business, offer to record the contact person's name and call them back. Then call the company at a telephone number you already possess to confirm the original contact's identity and phone number. Better yet, tell the caller that you don't accept phone-based solicitations from anyone and insist they contact you via snail mail. Don't give them your mailing address. If the phone call is genuine, the caller will already have your address.
- If you are contacted by a collection agency about a debt you don't owe, record the collection agent's information, then immediately contact the alleged creditor yourself, using independently verified contact information. Don't trust the information from the alleged collection agent, who may be a phisher.
- To learn more about phishing: <http://www.antiphishing.org>
- To report phishing scams, go to the FBI Internet Crime Complaint website: <http://www.ic3.gov>

### **Take Action**

If your monthly credit card statement contains extra charges that aren't yours, contact the credit card company immediately to determine if the charges can be removed. You may need to cancel your current credit card and get a new one.

If your wallet or credit card gets stolen:

- Cancel your credit cards immediately. Have the toll-free numbers and credit card numbers handy so you know who to call. Keep those where you can find them quickly.
- File a police report immediately in the jurisdiction where it was stolen. Get a copy of the report and save it. This proves to credit providers you were diligent, and is a first step toward an investigation.
- This may be your most important task. Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. The alert means any company checking your credit knows your information was stolen and they have to contact you by phone to authorize new credit. The numbers are:
  - Equifax: 800-525-6285
  - Experian (formerly TRW): 888-397-3742
  - Trans Union: 800-680-7289
  - Social Security Administration fraud line: 800-269-0271
- The Federal Trade Commission provides information about identity theft and support for victims:
  - FTC ID Theft website: <http://www.ftc.gov/bcp/edu/microsites/idtheft>
  - FTC ID Theft Hotline: 877-438-4338