Name: James Blankenship
Certification: GIAC Security Essentials (GSEC)
Assignment: Version 1.4, option 1 (April 2002)

Cyber Preparedness for the Home User in an Age of Internet Warfare

Abstract

As the Internet community continues to grow so do the dangers. Unsuspecting and unprotected home users, classified as "casual," face an increased risk of attack and, moreover can present a greater threat to others. Despite an increased emphasis by the government and commercial organizations stressing home computer security and Internet dangers, evidence indicates that the casual user continues to struggle with two key security issues: risk awareness and the necessity to secure home systems.

To combat these problems it is necessary to first establish a foundation of awareness; this guide introduces fundamental security concepts, common threats, vulnerabilities, and risk impacts to the user and Internet community. Then by building a framework using a confidentiality, integrity, and availability triad coupled with a multiple layer approach, the casual user is provided countermeasures that blend online awareness with best practice techniques and technologies. This guide offers the casual user a structured framework that includes online resources, techniques, and technologies to secure information and assets that demand protection. Individuals that diligently apply the approach of awareness and layered protection will be well informed and tightly guarded against risks threatening their confidentiality, integrity, and availability. Disciplined users will also contribute to the protection of our nation's critical systems and networks.

Introduction

Gadgets abound. Consumers around the world welcome new technology, whether for reasons of productivity or style, at astounding rates. Internet connectivity for the home has been no different. In the spring of this year, the United States home population showed the greatest increase. "The worldwide Internet population reached 323.7 million users in April 2002, according to a new report by comScore" ("Global Net Pop. Incr.").

Contributing to this worldwide expansion is the availability of broadband. Broadband differs from common dial-up connections by providing users with high-speed, "always-connected" access to the Internet. This type of Internet access translates into faster downloads of web pages, software, music, and video. High-speed connections use the cable service from a local cable TV provider or a Digital Subscriber Line (DSL) provisioned by a local telephone company. The U.S. Government has aggressively promoted the deployment of broadband infrastructure for some time now. In fact, Senator Tom Dachle has a vision to make broadband service “as universal tomorrow as telephone access is today” (Gilmore). This initiative, coupled with the availability and affordability of the service, will only contribute to the number of home users connected worldwide.

The casual user has become an increasingly exploited group within the Internet community due to the growing user base. Home users are experiencing first-hand the impacts produced from the rapid expansion of the Internet population. Therefore, the casual user must know as much as possible about the dangers they face, the threat they might be to others and the countermeasures available to reduce their risk.

Fundamental Security Concepts

The issue of risk awareness and securing home computer systems is fast becoming a heightened concern. Whether securing government, corporation, small business or home computers, there are three common areas that demand protection: confidentiality, integrity, and availability. Confidentiality is the intended level of privacy for information or assets deemed private. A tax return stored on a personal computer is intended to be confidential. Integrity is the quality or soundness of an application, information, or resource held personal or private. The accuracy of the data and application used for filing tax forms online is an example of integrity. Availability is ensuring the uninterrupted use of or access to the personal asset or information. Tax records stored in a safe location ensure future access to the information. Before examining the significance of protecting these three key elements, risk awareness is discussed.

Dangers for the Home User

Today computers are so prevalent that they can be found in almost every home. A home user’s growing dependence upon the personal computer and Internet increases their exposure to the dangers plaguing users today. As a result, risk awareness is essential for combating current threats and vulnerabilities. There are all types of dangers a casual home user should recognize. For instance, fire, water damage, burglary, mechanical, and user error are all examples of environmental threats. Although obvious environmental threats are serious and should not be overlooked, the most common threats confronting the home user are technological, social, and some not so obvious environmental dangers.

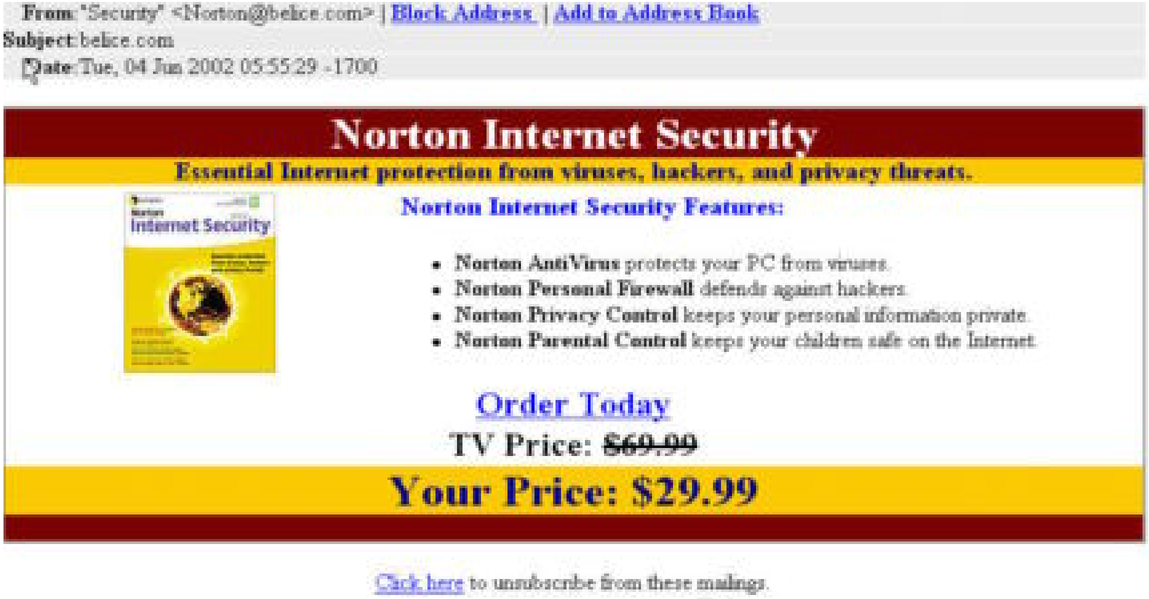
Technologically Engineered Threats

News headlines read of perpetual attacks upon the Internet community. As high-speed services and new technologies are introduced, evidence of constant hacking attempts, next generation viruses, and the propagation of advanced malicious code increases. The CERT coordination center posted advisory CA-2001-20 stating, “This year, we have seen a significant increase in activity resulting in compromises of home user machines” (Carpenter, Dougherty, Hernan). In addition to constant hacking attempts, increasingly sophisticated malicious code technology called “worms” and “hybrids,” preys on unsecured computers. Once introduced to the public network, the code requires no action on behalf of a user to spread from machine to machine. The code is automated to seek out systems and attack unprotected network shares and other known system vulnerabilities. This aggressive code is fast becoming the most significant online threat to vulnerable computers and networks. Recently, a next generation virus, W32.Perrun, introduced a new threat to text and picture files passed freely among home users. The virus raises new concerns for the user community by impacting file types historically found to be safe from infection. In its current form, Perrun is more like the first 1.0 version of DOS. A Symantec security response report described the virus as saying, "W32.Perrun is a virus that appends itself to .jpeg or .txt files. The malicious content of files that it alters will not spread to other computers" ("W32.Perrun").

Socially Engineered Threats
If technological threats are not enough, social attacks are occurring on a greater scale against the unsuspecting home user. By exploiting such services as e-mail, news groups, Instant Messenger, MSN Chat and Internet Relay Chat (IRC), socially engineered attacks attempt to fool unsuspecting users into installing malicious software or supplying confidential information. For instance, an unaware user opens an infected executable file attachment from an e-mail or news group and unknowingly installs a viruses or "Trojan horse" program. Sometimes these attachments are cleverly disguised using double file extensions; a malicious file called "advice.txt.exe" might be displayed on a system configured to hide file extensions as "advice.txt". In this example, the malicious program appears to the user as a simple text attachment. Systems configured to hide file extensions place users at an increased risk for installing malicious code. Once installed, an attacker's code has been known to forward personal information to remote servers or install backdoors permitting future access by an intruder to browse or control the computer remotely. An intruder's exploitation of Internet Relay Chat and Instant Messaging services is another tactic used to trick unsuspecting users into downloading and executing malicious programs. A recently published incident warning users to be aware because "tens of thousands of systems have recently been compromised in this manner" (Householder).

Environmental Threats
An evolving environmental threat to an individual's confidentiality is the use of SPAM mail and fraudulent web-sites intended for fraud or theft. SPAM mail is electronic junk mail that can be used to deceive or lure home users to fraudulent web sites requesting personal information. For instance, perpetrators fool unsuspecting users into supplying information: name, date of birth, social security number, or credit card number. Diagram 1 shows an example of SPAM mail designed to lure an unsuspecting user into using a credit card for payment or to capture a user's e-mail address for future SPAM mailings using the "Click here" link. This solicitation is designed with a professional look to appear as an actual offer from the software vendor, Symantec.

Diagram 1: Unsolicited SPAM Mail.



From: "Security" <Norton@belice.com> | Block Address | Add to Address Book
Subject: belice.com
Date: Tue, 04 Jun 2002 05:55:29 -1700

Norton Internet Security

Essential Internet protection from viruses, hackers, and privacy threats.

Norton Internet Security Features:

- **Norton AntiVirus** protects your PC from viruses.
- **Norton Personal Firewall** defends against hackers.
- **Norton Privacy Control** keeps your personal information private.
- **Norton Parental Control** keeps your children safe on the Internet.

Order Today

TV Price: ~~$69.99~~

Your Price: $29.99

Click here to unsubscribe from these mailings.

This technique often leads to another form of abuse such as Internet credit card fraud or identity theft. Electronic mail and web pages are the two most common techniques used to deceive adult online users into providing personal and credit card information. Today, home users aware of the current technological, social and environmental threats incorporate a layer of preparedness into defending his or her domain.

Vulnerabilities

The idea of being vulnerable to Internet attacks and intruders while their computers are secured inside their home is hard to imagine for many casual users. A casual user's ignorance regarding potential system, network, and Internet connection weaknesses widens the door for an attacker. There are several unsuspecting vulnerabilities that can affect a user such as new software releases, new operating systems, outdated operating systems, broadband connections, and a lack of security awareness. Conditions that contribute to vulnerabilities are factory delivered settings with no consideration for security, newly purchased computers with patch outdated operating systems, and the variety of operating systems supported. Software vulnerabilities are typically discovered after the product has been released to the public. When possible, vendors will issue a software fix commonly referred to as a "patch" or a "work-around" to correct the problem; however, the user is typically responsible for acknowledging and applying the countermeasure. As known security flaws are released, attackers will continue to count on the uninformed user to exploit those weaknesses for which a patch is available. The dependency upon each individual to research and apply timely patch updates from various vendors presents a huge vulnerability for the ill informed home user.

High-speed connections are also becoming a huge vulnerability as more home users migrate from dial-up to broadband service. A common misconception is that a user is only connected to the Internet when the web browser is running. Since this type of access is “always-on,” users are often unaware that they are continuously connected to the Internet and accessible by others. Users unaware of this fact combined with non-existent or outdated virus or firewall protection are extremely vulnerable. Finally, a user’s lack of security awareness can be an incredible liability contributing to vulnerabilities already mentioned. The casual user unaware of the dangers and necessity to guard against threats and vulnerabilities is susceptible to a variety of attacks as well as a threat to others.

Risk Impacts to the User

Despite the number of individual threats and vulnerabilities, a user becomes exposed to the risk of attack once the two are paired. Using the previous tax record as an example, a user storing his or her confidential tax information on a computer without virus or firewall protection is not a risk by itself. The user becomes vulnerable to the threat of compromise once connected to the Internet. The personal risk impacts for home users are emphasized using three fundamental characteristics of computer security: confidentiality, integrity, and availability.

Breach in Confidentiality

A home user’s failure to protect confidentiality can be very costly and in some situations have a terrible financial impact. A breach in confidentiality typically involves the compromise of private information or resource: the theft of personal information such as social security, bank account, pin and credit card numbers. Identity theft in America is fast becoming a crisis situation affecting thousands of people across the country. Attackers intent on stealing private information can deploy a combination of social, environmental, and technological tactics to trick unsuspecting users. Once installed, viruses have been known to forward confidential information to remote servers on the Internet. Fraudulent web sites have been used to collect consumer credit card information and Trojan horse programs can offer easy access to compromised systems allowing intruders to collect financial records, tax information, and personal data.

A scenario exists where an intruder obtains access to an unprotected home system and extracts confidential palm pilot data. Small hand held computers called “Palm Pilots,” have the ability to store or “sync” large amounts of information to directories on home or laptop computers. In some cases, this confidential data can include user IDs, passwords, social security numbers, internal phone numbers and customer lists. Once private information has been compromised, a malicious user has the keys to an individual’s identity, private accounts and possibly corporate systems. A failure to protect or recognize the need to protect confidentiality can have a devastating financial and personal impact on a home user.

Breach in Integrity

Protecting system integrity is vital to ensure the soundness of hardware, software, and data. A compromise in system integrity can be frustrating for the average home user resulting in a time consuming and costly cleanup effort. Examples of violations in system integrity include deleted and or modified files and most commonly the installation of malicious code. Deleted personal or system files are the most catastrophic example of a violation of integrity. Most users today have experienced the agony resulting from a loss of important personal or system data. The time, effort, and money spent on recovering lost data can be a terrible lesson for any individual. One way attackers count on compromising systems is by exploiting unaware and unprotected users by way of viruses and Trojan horse programs. For instance, system integrity is often violated when an e-mail attachment containing malicious code marked with a .exe file extension is opened. A user opening such an attachment automates the installation of dangerous code, which can compromise the system by modifying or deleting files. Malicious code has also been known to install backdoors permitting future access by an intruder to browse or control the computer remotely. Viruses and Trojan horse programs count on unawareness by requiring action on behalf of the user for installation. On the other hand, aggressive code referred to as “hybrids” and “worms” requires no action on behalf of a user and violates a system multiple ways. Instead, the attack code spreads quickly taking advantage of unprotected network shares and other known vulnerabilities residing on unpatched systems. The impacts resulting from these virulent forms of code are frequently found in current news headlines with such names as “Code Red.” The casual home user should know that hackers and malicious code do not discriminate between unprotected government, corporate, or home systems.

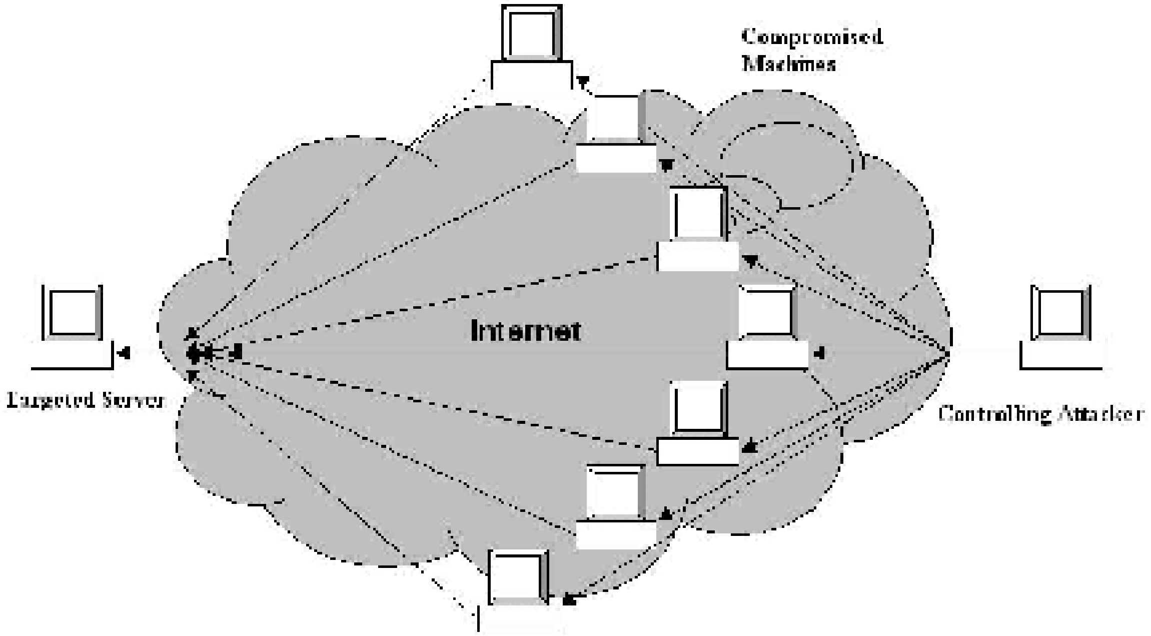
Breach in Availability

A continued consequence for allowing a compromise to take place is a loss of system availability. Interruptions in access to a system or information can be paralyzing to a home user. A down computer can result in a permanent loss of important data not to mention the cost, aggravation, and time to restore the system. Another example is the inability to perform a basic task such as opening a document or download data from the Internet without a severe drain on system resources. A casual user must be aware of the risks and how they are personally impacted when connecting to the Internet.

Risk Impact to Others Connected to the Internet

A lack of security in a home computer can severely impact an individual user, but a user’s neglect of their personal system combined with a high-speed connection often has further reaching consequences. Unknown to a user, a compromised system can be exploited to disrupt the availability to more important computers and networks. Perhaps the most realistic scenario using compromised machines, is an attack on our nation’s critical infrastructure. This issue is of so much concern to the U.S. Government that hearings are being held to help lawmakers understand the magnitude of the threats to critical systems as well as the countermeasures available. In a recent hearing, a Senior Director for Symantec Corporation voiced concerns that the threat to the U.S. government and others "will only grow more likely as home users move in greater numbers to broadband Internet connections through cable modems or Digital Subscriber Lines (DSL)" (Trilling). In addition, a collaborative effort between corporate and government organizations called the National Cyber Security Alliance has been created. The National Cyber Security Alliance attempts to raise Internet awareness with a strong emphasis on securing personal computers among the casual user community. Scenarios that demonstrate how compromised systems can be used to disrupt availability to others are Distributed Denial of Service attacks (DDoS) and the rapid propagation of hybrid malicious code. By violating the integrity of multiple vulnerable home or business computer systems, an intruder can use a DDoS technique to harness the distributed power from all compromised computers across the Internet and focus those resources in a concentrated manner to disrupt service at an organizational and national level. Diagram 2 illustrates the Distributed Denial of Service technique to disrupt service or crash the target machine by flooding it with packets of data from compromised systems.

Diagram 2: Distributed Denial of Service Attack.



Unsecured home computers can also be used to quickly spread infectious worms to other vulnerable computers disrupting the availability to many systems connected to the Internet. The Nimda worm was a well-known attack last year that quickly spread from one Microsoft machine to the next by way of system vulnerabilities and e-mail compromising system integrity and availability across the Internet. As ludicrous as these scenarios may sound to a casual user, they are in fact reality and a cause of serious concern for our nation's government as more home users connect to the Internet.

Layered Countermeasures

There is no one solution that protects a home user from the assortment of technological, social, and environmental threats that exists today. A common misconception among the home user community is that technology alone can protect a user from all potential threats. When in fact, a user's best defense is a multiple layered approach blending disciplined awareness, current technologies, and techniques.

Layer 1: Protecting Confidentiality

For most homes, technology is the only approach for securing one's confidentiality, though awareness combined with best practice techniques and technologies provide a solid layer of defense for securing a computer. There are an increasing number of resources devoted to the task of educating families and individual users. In addition, the application of disciplined techniques and technologies such as strong passwords and file encryption tools are also necessary.

Online Awareness

With social attacks proving to be the most difficult to defend and evidence of unsolicited environmental attacks increasing, the need for cyber awareness is more important than ever. Through awareness, individuals and families are more attuned to the dangers of the Internet confronting them each time they are connected. Some excellent sites educating the user on cyber issues and threats to home security are a combination of knowledge, instruction and best practice techniques. The first site, National Cyber Security Alliance, is an informative site created with the goal of educating individual users and families on Internet safety and security. This site is an excellent resource for learning the basics on safeguarding computers, educating family members, and accessing links to additional industry and government sites. An excellent web page devoted to Internet security testing for Windows users is Shields Up by Steve Gibson. This site tests the security of a single computer by probing the system's Internet connection and ports. This is an excellent tool to exercise the level of protection provided by the system's existing configuration. Another site published by the CIAC team and U.S. Department of Energy is the Internet Hoax and Chain Letter instructional page called Hoaxbusters. This public service site educates users on how to determine the legitimacy of rumored viruses and the negative impacts to mail servers caused by chain letters.

There are several sites and documents committed to guiding home users in the area of Internet threat prevention. The Internet Fraud Complaint Center, which publishes the "IFCC 2001 Internet Fraud Report," includes a best practice instruction educating home users about Internet fraud prevention. The Identity Theft Resource Center also offers practical online safety information for protecting an individual's confidentiality. The CERT Coordination Center publishes “Home Network Security” and other insightful articles and resources tailored for home users. The SANS Institute hosts the public Information Security Room. The site provides detailed research on a variety of home and small office computing topics. Finally, many vendors like Symantec frequently post informative articles about how to protect computers and families from online threats.

Strong Passwords

Most users today do not realize the tools that are available to crack passwords within seconds. The most complex passwords can be cracked in just a few days. A password is a user’s first layer of protection against unauthorized electronic and physical system access. Passwords also protect applications and shared resources including Quicken, Microsoft Money, directory folders, disk drives or hardware. Most users use common dictionary or short passwords to protect against unauthorized entry. Unprotected resources and easy-to-guess passwords are vulnerable to hackers and infectious code and should be strengthened.

The understanding and application of best practice password policies help to strengthen that first layer of security protecting one’s confidentiality. Some common practices for creating a strong password are:

- Choose a password with at least eight characters.
- Take the first character from each word of an easy to remember phrase such as, “**W**hen **i**t **r**ains **o**n **S**aturday **I g**et **m**ad!”
- Transpose the phrase into a password using a combination of numbers, uppercase, lowercase, and special characters. To help remember uppercase characters, apply capitalization to words with an emphasis such as “when,” “Saturday,” and “mad”.
- In the following table, the example phrase is transposed to create a strong password.
- The letters “O” and “I” are changed to numbers.
- The entire word “mad” is transposed using additional special characters to increase password strength.

When	**I**t	**R**ains	**O**n	**S**aturday	**I**	**G**et	**M**ad!
W	**I**	**R**	**0**	**S**	**1**	**G**	**M@#!**

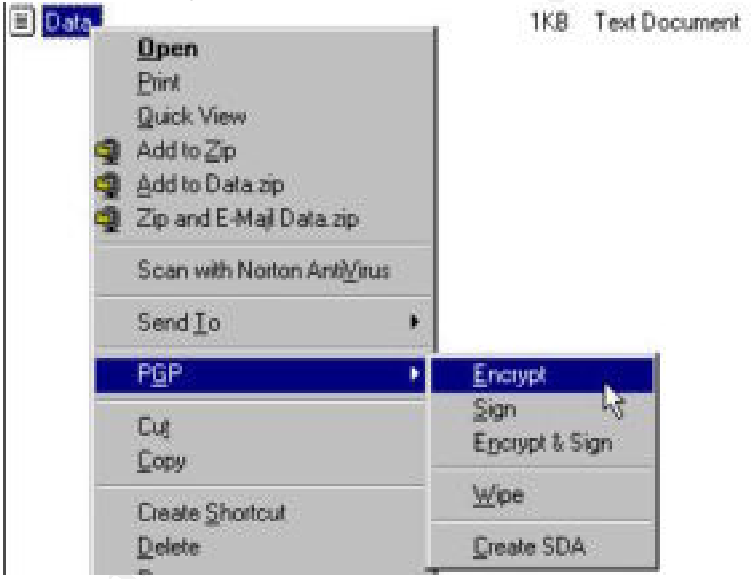
- Memorize the password and **do not** write it down on a piece of paper.
- Change the password on a regular basis.
- Do not use names of family members or pets.

Disciplined application of best practice password techniques should always be applied to protect from unauthorized entry or access to shared resources and applications. Implementing these common sense practices will assist in creating a tough layer of intruder prevention.

Encryption

Encryption is a process of converting ordinary language or text into code that is used to protect private information from becoming public. For the home user, quality encryption tools are available to help secure sensitive information. Unaware, many home users openly store tax records, bank account numbers, online banking passwords, and documents containing personal information like social security numbers. To restrict unwanted access, a home user storing or transmitting sensitive files via e-mail would be wise to implement encryption. PGP (Pretty Good Privacy) is a quality freeware package that is used for encrypting e-mail between recipients; however, PGP includes an individual file encryption tool as well. Diagram 3 demonstrates how selected files from within Windows Explorer can easily be encrypted and decrypted using PGP file encryption.

Diagram 3: PGP File Encryption.



PGP is available for Macintosh and Windows systems and is a handy tool for a home user to have. The PGP freeware version can be downloaded from MIT's site, **http://web.mit.edu/network/pgp.html**.

Layer 2: Protecting System Integrity

Securing the integrity of a home computer system and network is essential to ensuring the soundness of programs, data and the protection of others. Today's technology coupled with the diligence of a casual user can add a hard layer of defense against intruders. Some best practice recommendations include displaying file extensions, installing anti-virus and personal firewall software, performing critical software updates, and installing a network firewall for high-speed connections.

Anti-virus Protection

The dominant threat created by Trojan horse, virus, and worm code demands the application of anti-virus protection. Indeed, a home user has many choices when defending a system's integrity against malicious code. Two of the most effective products on the market are Norton Anti-Virus and McAfee Virus Scan. To ensure continued protection, timely virus signature updates are required. Virus signatures are in essence "patch" updates that enable anti-virus programs to recognize the latest malicious code. A user's disregard for the importance of regular virus signature updates leaves a system unprotected. Fortunately, top anti-virus software has automated this process making critical updates near transparent to the user. Along with regular virus signature updates, anti-virus tools are extremely effective in warding off malicious code.

Displaying File Extensions

Attackers are constantly inventing new ways to exploit common file types to compromise systems. Configuring a home system to recognize and display file extensions is a best practice technique that will help the casual user defend against social attacks. Some standard file types commonly downloaded or transmitted via e-mail are listed in the table below.

File Type Description	File Extension
Windows Executable Program File	.exe
Windows Word Document File	.doc
Text File	.txt
Audio/Video MPEG Files	.mp3
Picture Files	.jpg, .gif

With the exception of program and document files, most file types are generally safe from virus infection. However, evidence of next generation virulent code impacting text and jpeg picture files signals the need for users to be cautiously aware of the various file types. Though data files are now showing the potential to host malicious code, the Windows executable file is still the most frequently abused file type. The Windows operating system is designed to recognize files with an exe extension as executable. Once a user "clicks" on the executable file, the program performs the built-in instructions. Configuring a system to display file extensions enables a guarded user to spot e-mail attachments containing executables such as "funny.exe" and "openMe.txt.exe." For example, a system configured to hide file extensions would misleadingly display the executable files as "funny" and "openMe.txt." To configure a Windows system to show files extensions, a user should consult Microsoft's help facility. Configuring a system to show file extensions helps to protect the user against installing unnecessary and malicious executable programs.

Critical Software Updates

For a home user, the application of critical software updates goes a long way in securing a system's integrity. This step protects a system by closing known operating system or application vulnerabilities. A user's failure to apply critical updates can allow attackers to exploit published security weaknesses. Updates are also another measure of protection against worms and hybrid code that seek out systems with known weaknesses. Many home users run a variety of hardware platforms and software applications. Microsoft and Apple are two sites that the casual home user should frequent depending on their computer operating system.

For Windows 9x and ME operating systems, the Microsoft Windows Update site provides users with the latest product and operating system updates. Microsoft offers a free tool called "CriticalUpdate" to automate the routine process of checking for critical updates based on currently installed software. The "CriticalUpdate" software is quick to download, and the program is easy to install with no configuration required to inform users of critical patches. For Microsoft's XP and 2000 based operating systems, the Microsoft Baseline Security Analyzer is the latest security tool to help prevent common security vulnerabilities. MBSA replaces previous versions of Microsoft's Personal Security Advisor combining the functionality of the Hot Fix Checker tool into one product.

For Macintosh computers, the AppleCare Support page offers the most current product and operating system updates. Users can also use the "Software Update" feature to get updates when connected to the Internet or schedule when to check for updates.

Personal Firewall

A personal firewall is software program that runs on the user's computer filtering unwanted incoming and outgoing Internet traffic. Personal firewalls are excellent for protecting a system's integrity from malicious attack. A personal firewall capable of filtering unexpected outbound traffic also protects confidentiality and availability. For example, an unexpected outgoing connection to a remote machine on the Internet can be the result of a rogue virus or Trojan horse program. Most people today associate the use of personal firewalls with high-speed connections. For this type of connectivity, a personal firewall is definitely recommended since the connection to the Internet is "always-on."

Personal firewalls are also excellent for protecting systems connected to the Internet by modem dial-up access. Dial-up modems also establish two-way connections allowing hackers to scan systems, receive transmission of confidential data, or connect to home systems running Trojan programs. Below are two examples of ZoneAlarm personal firewall software blocking unwanted Internet traffic to a computer connected via dial-up.

- *The firewall has blocked Internet access to your computer (NetBIOS Name) from x.x.x.x (UDP Port 1032).*
- *The firewall has blocked Internet access to your computer (UDP Port 1680) from x.x.x.x (UDP Port 1680).*

Whether using high-speed or dial-up access, this example demonstrates one case for the necessity of a personal firewall. For Windows XP users, Microsoft's new operating system offers a first attempt at a personal firewall to help protect users from the dangerous Internet traffic. However, Microsoft's personal firewall does not flag suspect outgoing Internet traffic. To obtain a better understanding of firewalls, a user should take the time to read Steve Gibson's page on "Personal Internet Firewall that Really Work!"

There is an overwhelming number of personal firewall products on the market today. The list below identifies a few choices for users to select from.

- ZoneAlarm
- BlackICE PC Protection
- Norton Personal Firewall
- McAfee Personal Firewall

An excellent resource providing up to date test results on personal firewall software is Gibson Research Corporation's LeakTest Firewall Evaluation page.

Network Firewall

For high-speed connections using cable or a Digital Subscriber Line (DSL), a network firewall restricting unwanted Internet traffic is a necessity. A system connected to the Internet without one is exposed. Similar in functionality to a personal firewall, a network firewall is a separate piece of hardware protecting one or more internal networks and computers from the public Internet network. The packet filtering firewall is the most common solution for home applications. A packet filter firewall drops unwanted incoming Internet traffic (ingress filtering), outgoing traffic (egress filtering), and conceals a network and computer's identity from other machines on the Internet using a tool known as NAT (Natural Address Translation). A network firewall cannot protect a user from all technological and socially engineered attacks. However, a firewall using NAT, ingress and egress traffic filtering provides the most cost efficient measure of protection for securing a network's perimeter. Unfortunately, the configuration of this device is not straightforward and can be complex for even an experienced person. Therefore, home users should be aware of the importance of a properly configured firewall and the issues with high-speed access. The SANS Institute's Information Security Room offers detailed research in the area of firewall and perimeter protection. Another resource to consult is "Internet Firewalls: Frequently Asked Questions" by Matt Curtin and Marcus J. Ranum. Individuals planning on configuring their own network firewall should become familiar with "The Twenty Most Critical Internet Security Vulnerabilities." Posted by the SANS Institute, this consensus document provides detailed technical recommendations on closing various vulnerabilities including commonly exploited firewall ports.

Layer 3: Protecting Availability

For the casual home user, ensuring the availability of their computer is an ongoing process. At some time whether it is from user error, hardware failure, malicious code or burglary, a user will experience an interruption in service. Rather than ignore the inevitable, a user should implement preventative measures to protect against disruptions. Simple countermeasures that can be performed by the user are routine backups, implementation of backup and recovery tools, and a written plan to assist with recovery.

Routine Backup Approach

A determined backup approach implementing full and partial backups of important directories, data, and critical system files will help a user avoid disaster where the loss of critical information is at risk. Backing up important data and critical system files to removal media such as a floppy diskette, CD, or DVD is an easy and effective approach for most home users. In order to save data to a CD or DVD, a user must use a device called a CDRW (CD-ROM Read/Write) or CDRW/DVD. To help users ensure routine scheduled backups, most operating systems include a program to automate and schedule tasks. Commonly referred to as a "task scheduler", the program can be configured to start a scheduled backup at designated times.

Backup Tools

When it comes to ensuring system recovery, third-party backup tools are the best choice. A third party backup and recovery tool such as Symantec's Norton Ghost provides a disk-imaging feature that creates and stores an image of the hard drive on CD or DVD media. In the event of a disaster, this tool allows for the recovery of an entire system from the backup media. McAfee EasyRecovery offers a different approach by providing real-time recovery features to ensure a system's continuous availability. In the case where third party tools are not an option, a Windows user can utilize Microsoft's backup utility. Whether using third-party tools or a bundled backup application, a startup diskette created for emergency situations is a recommended practice. A startup diskette is a tool used to start a computer in MS-DOS mode for repair or recovery. Detailed help information on Microsoft's backup utility, startup diskette creation, and system registry database can be found using Microsoft's help utility. For Macintosh and Windows users, there are many excellent books on the market to suite different levels of expertise and provide specific guidance on full backup and recovery strategies.

Documentation

Tools and scheduled backups are a great first step, but a user without a recovery plan or procedure to follow during those high stress times lessens the probability of a successful recovery process. With the purpose to guide a user through the stressful recovery steps, a plan should be as detailed as necessary. A plan might highlight steps required to prime a recovery tool, list necessary user manuals, document hard drive partitions, or list the location of a startup diskette and backup media. To ensure a smooth restoration process, an up-to-date hard copy should be stored in an accessible location and contain the necessary information.

Layer 4: Protecting the Availability of Others

The final layer of protection is one that will contribute to the availability of other Internet systems and networks including this nation's critical infrastructure. Home users devoted to this commitment will apply a layer of responsible techniques and remain vigilant as new Internet services, technologies, and attack methods are introduced. Three areas where the casual home user can take responsibility: application of outgoing network firewall filters, subscription to security alerts, vendor updates, and familiarity with consumer response sites.

Application of Outgoing Filters

For broadband connections, the use of a network firewall coupled with outgoing filters, technically referred to as egress filters, protects the availability of others on the Internet. Recalling the Distributed Denial of Service example in Diagram 2, egress filters can prevent an attacker from using a compromised user's computer as a source of forged transmissions that flood targeted servers on the Internet. Egress filters should be applied allowing outbound transmissions to occur from only the home user's configured Internet address. A popular resource from the SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities," provides technical recommendations on the implementation of egress filtering.

Consumer Security Notification & Response

Most vendors and response centers offer a free e-mail subscription list publishing the latest security advisories, threat updates and security fixes. To recognize current dangers and apply the latest countermeasures, home users can subscribe to any of the following e-mail lists.

- Symantec Security Response
- The CERT Advisory Mailing List
- Microsoft TechNet Security
- McAfee
- Identity Theft Resource Center Consumer and Press Alerts

For users that have fallen victim to online theft or compromise, the National Infrastructure Reporting Center and Internet Fraud Complaint Center post online forms for consumers to report fraud, malicious attacks or activity.

Conclusion

As the Internet population grows stimulated by new services and the adoption of broadband technology, digital warfare against the user will continue unabated. New vulnerabilities and attack methods will threaten the home user's confidentiality, integrity, availability as well as the nation's critical systems. With no solution available to defend every attack, a user's most effective defense begins with a foundation of fundamental security knowledge and risk awareness. By applying layers of online awareness, techniques, and technologies to that foundation, the disciplined user establishes a structured framework that helps to secure the home perimeter from attacks against confidentiality, integrity, and availability. George Washington was once quoted on the subject of war stating, “Nothing can be more hurtful to the service, than the neglect of discipline; for that discipline, more than numbers, gives one army the superiority over another” (Washington p.320). The necessity for discipline in common warfare more than two hundred years ago is applicable today for defending home perimeters. During this age of Internet warfare, the casual home user that diligently applies awareness, layered techniques, and technologies will be well informed and tightly guarded against the dangers to self and country.

Works Cited

AppleCare Support. URL: http://www.info.apple.com/new/site5/ (29 May 2002).

"Beware of Identify Theft." Symantec.
URL: http://www.symantec.com/homecomputing/theft.html (20 May 2002).

BlackICE PC Protection. Internet Security Systems.
URL: http://www.iss.net/products_services/hsoffice_protection/buy.php (31 May 2002).

Carpenter, Jeff, Chad Dougherty, Shawn Hernan. "CERT Advisory CA-2001-20 Continuing Threats to Home Users." CERT Coordination Center. 20 July 2001.
URL: http://www.cert.org/advisories/CA-2001-20.html (20 May 2002).

CERT Coordination Center. URL: http://www.cert.org/nav/index_main.html (29 May 2002).

Curtin, Matt, Marcus J. Ranum. "Internet Firewalls: Frequently Asked Questions." Internet FAQ Consortium. Rev. 10.0. 12 Dec. 2000.
URL: http://www.faqs.org/faqs/firewalls-faq/ (30 May 2002).

Danyliw, Roman, Chad Dougherty, Allen Householder, Robin Ruefle. "CERT Advisory CA-2001-26 Nimda Worm." CERT Coordination Center. 25 Sep. 2001.
URL: http://www.cert.org/advisories/CA-2001-26.html (20 May 2002).

"GartnerG2 Says Enterprises are Not Doing Enough to Prepare for Cyberattacks." GartnerG2. 1 May 2002.
URL: http://www.gartnerg2.com/press/pr2002-05-01.asp (15 May 2002).

"Global Net Population Increases." 14 May 2002.
URL: http://www.nua.com/surveys/ index.cgi?f=VS&art_id=905357952&rel=true (20 May 2002).

Gibson, Steve. "LeakTest." Shields UP. Vers. 1.1. 4 Nov 2001.
URL: http://grc.com/lt/leaktest.htm (6 June 2002).

Gibson, Steve. "Personal Internet Firewalls that Really Work!" Shields UP. 26 Feb 2002. URL: http://grc.com/su-firewalls.htm (6 June 2002).

Gibson, Steve. "Shields UP!!" URL: https://grc.com/x/ne.dll?bh0bkyd2 (6 June 2002).

Gilmore, Tom. "Broadband: Make the Players Carry Their Own Weight."

ITworld.com. 9 Jan. 2002. URL: http://www.itworld.com/nl /unix_sec/03282002/ (13 May 2002).

Hoaxbusters. CIAC team and U.S. Department of Energy.
URL: http://hoaxbusters.ciac.org/ (2 June 2002).

“Home Network Security.” CERT Coordination Center. 5 Dec. 2001.
URL: http://www.cert.org/tech_tips/home_networks.html (20 May 2002).

Householder, Allen D. “Incident Note IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging.” CERT Coordination Center. 19 Mar. 2002.
URL: http://www.cert.org/incident_notes/IN-2002-03.html (20 May 2002).

Identity Theft Resource Center. URL: http://www.idtheftcenter.org/ (30 May 2002).

“IFCC 2001 Internet Fraud Report January 1, 2001 – December, 31 2001.” National White Collar Crime Center and the Federal Bureau of Investigation.
URL: http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (21 May 2002).

“Internet Risk Impact Summary for December 22, 2001 through March 21, 2002.” Internet Security Systems.
URL: https://gtoc.iss.net/documents/summaryreport.pdf (16 May 2002).

Kelsey, Dick. “Online Fraud Loss 19 Times Offline's – Gartner.” Newsbytes. 4 Mar. 2002. URL: http://www.newsbytes.com/news/02/174918.html (20 May 2002).

Mcafee.com. URL: http://www.mcafee.com (31 May 2002).

Microsoft Baseline Security Analyzer. Microsoft. Ver. 1.0. 2 Apr. 2002.
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp (7 June 2002).

Microsoft TechNet Security. Microsoft.
URL: http://www.microsoft.com/technet/security (29 May 2002).

Microsoft Windows Update. Microsoft. URL: http://windowsupdate.microsoft.com/ (29 May 2002).

PGP Freeware. MIT Distribution Center.
URL: http://web.mit.edu/network/pgp.html (31 May 2002).

Mark, Roy. “Auctions Dominate Internet Fraud Complaints.” dc.internet.com. 9 Apr. 2002. URL:http://dc.internet.com/news/article/0,1934,2101_1006511,00.html (20 May 2002).

National Cyber Security Alliance. URL: http://www.staysafeonline.info/index.adp (21 May 2002).

National Infrastructure Reporting Center. URL: http://www.nipc.org (29 May 2002).

SANS Reading Room. SANS Institute. URL: http://rr.sans.org/index.php (20 May 2002).

Symantec Products. Symantec. URL: http://www.symantec.com/product (31 May 2002).

Symantec Security Response. Symantec.
URL: http://securityresponse.symantec.com/ (20 May 2002).

Trilling, Stephen, comp. “Testimony of Stephen Trilling Senior Director of Advanced Concepts Symantec Corporation Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.” Oversight Hearing on “What Can be Done to Reduce the Threats Posed by Computer Viruses and Worms to the Workings of Government?” 29 Aug. 2001.
URL: http://www.house.gov/reform/gefmir/hearings/2001hearings/0829_computer_security/0829_trilling.htm (13 May 2002).

“The Twenty Most Critical Internet Security Vulnerabilities (Updated): The Experts’ Consensus.” SANS Institute Resources. Ver. 2.504 2 May 2002.
URL: http://www.sans.org/top20.htm (2 June 2002).

“W32.Perrun.” Symantec Security Response. 20 June 2002.
URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.perrun.html (6 June 2002).

Washington, George. General Orders: Jul 6, 1777. Comp. Daniel B. Baker. PowerQuotes. Canton: Visible Ink Press, 1992. 320.

ZoneAlarm. URL: http://www.zonealarm.com (31 May 2002).