A Quick Reference Guide for Internet and Computer Security

AlliedBarton® Security Services

Serving And Securing The People,
Homes And Businesses Of Our Communities

Securing Your PC and Web Browser

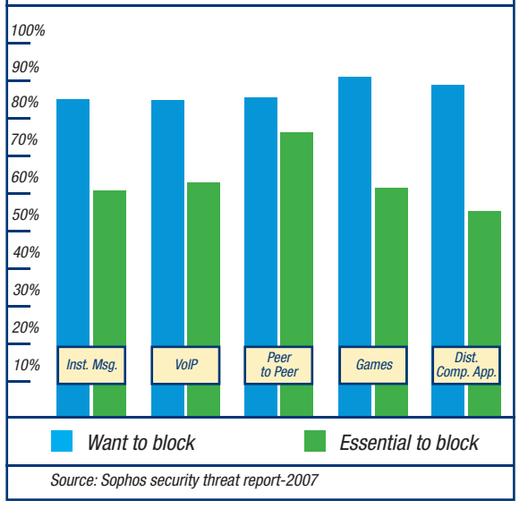
Eliminate Vulnerability of Information Systems

For businesses of all sizes, protecting computer networks from external disruptions is a necessity. At a time when computers are the lifeblood of many companies, technology is more susceptible than ever to intrusions that can inhibit productivity and erode competitive advantage.

With so much at stake, AlliedBarton has compiled this handbook for small and large businesses, as well as families and individuals.

Sincerely,
Your Friends at AlliedBarton Security Services

A recent survey of IT directors shows their main concerns regarding the types of nonessential applications they would most like to control.



Source: Sophos security threat report-2007

Triumph Over Malicious Web Scripts and Spyware

Malicious Web scripts are computer programs written to obtain proprietary information without permission.

Preventing malicious Web scripts from attaching themselves to browsers has become increasingly difficult because:

- Many browsers are configured to provide increased functionality at the expense of security.
- A growing number of Web sites require users to enable certain features or install more software.
- Many users do not know how to configure Web browsers securely.
- Many users are unaware of how to determine if their computers have been compromised.
- A growing amount of proprietary information is finding its way into unauthorized hands.

Spyware is a general term describing software that performs a number of unwanted functions. It often infiltrates computers during software installation and can:

- Change a computer's settings.
- Cause a system to slow down or crash.
- Switch a Web browser's home page.
- Add browser components that a user does not want or need.
- Cause large numbers of pop-up advertisements to appear.

What can you do to avoid these threats?

- Download software exclusively from reputable companies.
- Only visit legitimate Web sites.
- Rely on true experts, including IT professionals, to configure and maintain your network systems.

Following these steps can go a long way toward preventing malicious Web scripts and spyware from affecting the performance of a computer or network.

training TOP 125

Internet Safety In Your Home

Internet Safety Tips for Teens

Many teenagers use the Internet to keep in touch with friends, find homework support and read the latest news. In addition to the millions of sites to visit and things to do, the Internet also gives teens many ways to get in trouble, or to be taken advantage of financially or physically. **Teenagers should protect themselves online by:**

- Never giving out key information such as full name, home address, phone number, Social Security number, passwords, names of family members or credit card numbers.
- Using a nickname in chat rooms that is different from their real name.
- Telling a parent, or another adult, if a chat room conversation becomes uncomfortable.

Internet Safety Tips for Younger Children

For elementary school-age children, the Internet offers a wide range of learning opportunities, but it can also put their safety at risk. **Youngsters can protect themselves online by getting parents' permission before:**

- Giving out personal information, such as address, phone number and parents' work numbers.
- Sending a picture or other items.
- Installing software, or downloading programs or files from the internet

Parents should learn how to monitor their children's online activity, including checking the history files to see which Web sites have been visited. They may also choose to install software that filters out inappropriate Web sites, monitors activity, blocks access to various kinds of sites, or blocks Internet access during specific times.

Helpful Links and Resources

www.cert.org/tech_tips/securing_browser/index.html
www.kidshealth.org
www.microsoft.com/athome/security/spyware/spywarewhat.mspx
www.protectkids.org
www.safekids.com

Viruses, Worms and Abusive Email Practices

training TOP 125

Preparation Saves Time and Money

A computer virus is a software program designed to replicate itself and spread to other computers. Viruses can spread through diskettes, CD-ROMs, email attachments and the Internet.

Signs that a computer is infected with a virus include:

- Slower-than-normal operation.
- Crashing and re-starting every few minutes.
- Malfunctioning of applications.
- Inability to print correctly.
- Distorted menus and dialog boxes.

Actions to prevent viruses include:

- Open attachments from known parties only.
- Install only commercial operating software from CD-ROMs or DVDs purchased from legitimate software vendors.
- Download software from reputable Web sites only.
- Install good anti-virus software.

If a computer becomes infected with a virus, taking these steps can remove it:

- Install and update anti-virus software.
- Perform a thorough computer scan.
- Download, install and run a "malicious software removal" program. (NOTE: Virus removal software only eliminates existing viruses and does not prevent other viruses from infecting a system.)

Anatomy of a Worm

A worm is a software program that replicates itself over network computers. Unlike a virus, which may be programmed only to infect multiple files on one computer, worms are spread through email, instant messaging, file-sharing and the Internet to infect multiple computers. Worms come in "good" and "bad" varieties.

"Good" worms may be used to download software patches to fix vulnerabilities in a system. "Good" worms, however, can increase network traffic considerably, slowing down a computer's operation.

The best protection against harmful computer worms is:

- Using software produced only by reputable companies.
- Updating anti-virus and anti-spyware software regularly.
- Opening email messages from known parties only.

Spoofed and Forged Email

Spoofing consists of falsifying an identity or data to gain unauthorized access to a computer. Spoofing is easy because Simple Mail Transfer Protocol (SMTP), which enables the transfer of email from one server to another, lacks authentication. Tactics that spoofers and forgers use include:

- Sending email from a "system administrator" asking users to change their passwords and threatening to suspend their accounts if they do not comply.
- Posing as a person of authority and asking users to send them a copy of a password file or other sensitive information.

To prevent spoofing or forging, users should:

- Allow email to enter at a single point only.
- Configure mail delivery systems to prevent direct connection to SMTP ports.
- Use cryptographic signatures to exchange authenticated email messages.

Prevent RAT Infestation

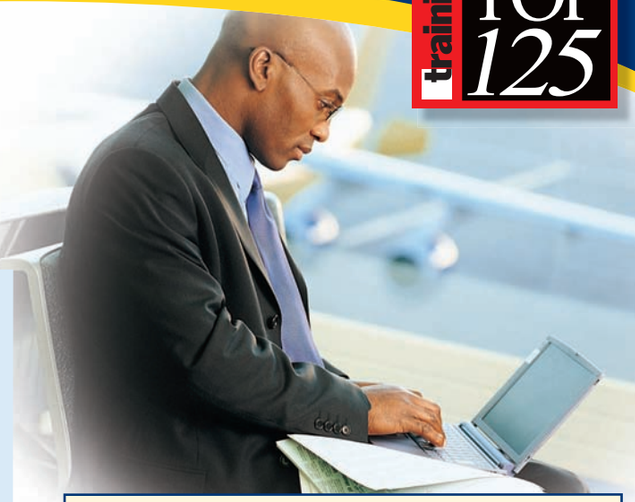
Remote Access Trojans (RATs) are malicious software programs that control a computer through an Internet connection. A RAT can expose a user to scams and can enable a criminal to view and change a computer's files without the user's knowledge.

RATs are often hidden in files that are downloaded from the Internet. They also appear in email or Instant Messages disguised as attachments.

To keep RATs from infiltrating a computer, users should:

- Share their primary email addresses only with people they know.
- Use trusted software from reputable companies.
- Use a firewall.
- Keep operating, anti-virus and anti-spyware software updated.

Internet Safety
On the Go...

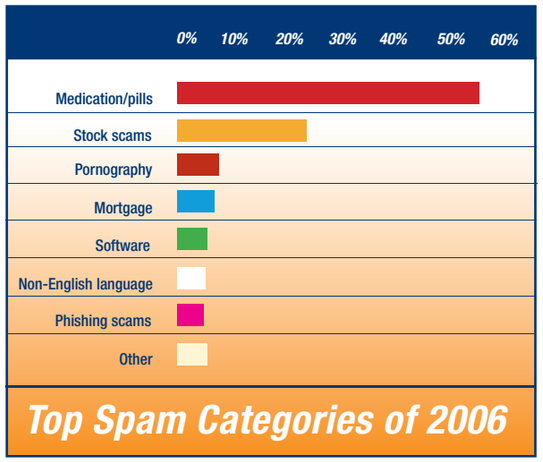


Stop Mobile Viruses

A mobile virus is a malicious computer program that targets mobile phones or wireless-enabled personal digital assistants (PDAs). As the number and complexity of wireless phone and PDA networks increase, it has become more difficult to secure networks against viruses.

To prevent mobile viruses, users should:

- Be careful when accepting Bluetooth files.
- Deactivate Bluetooth functions if a device becomes infected.
- Delete messages from unknown senders.
- Avoid installing programs of uncertain origin.
- Download ring tones and games from official Web sites only.
- Delete the infected application and reinstall it.



Top Spam Categories of 2006

Source: Sophos security threat report-2006 market research

Tips for Zombies and Botnets

A botnet (short for roBOT NETwork), also called a "zombie army," is a large number of computers that hackers set up maliciously on the Internet to forward transmissions, including spam or viruses, to other computers. Most computers compromised this way are home-based because they lack firewalls and other safeguards.

To prevent zombies and botnets from disabling computers, users should:

- Always use updated operating, anti-virus and Internet firewall software.
- Use licensed software products only.
- Open email messages, attachments and IMs from known parties only.

Helpful Links and Resources

www.rediff.com///money/2006/feb/08spec1.htm

http://www.mhc.ab.ca/services/educational-technology/resources/virus.htm

http://www.microsoft.com/athome/security/computer/viruses/protectyourcomputer_viruses.mspx

Practices for Protecting Confidential Information

Corporate Laptop Theft

Each day, thousands of computers containing confidential corporate information are stolen.

Many of these thefts are preventable through simple steps:

- Lock your notebook in your office during off-hours.
- Whenever possible, take your laptop home with you and keep it in a secure place.
- Review and understand the laptop insurance coverage included in your business and homeowner's policies to ensure that you have coverage for theft.
- Keep the least amount of proprietary information, that is practical, on your laptop.
- Do not load passwords on your laptop, particularly those allowing remote and email communication with clients or the office.
- Never leave your laptop unattended in a public place—even for a moment!
- Install a boot-up password, available on most portables, so only users with your password can access the hard drive.
- Back up your files and store them in a place other than the laptop carrying case.
- Consider engraving the company name or some other identification on the laptop.
- Pay attention to where you use the portable. Be aware that someone behind you, or next to you, can see your computer screen. This is especially true on an airplane.

When traveling you should:

- Carry your notebook in a strong, padded, nondescript bag. Do not use a carrying case that advertises there's a computer inside.
- Never leave a laptop in full view in your car, and never check the computer as luggage at airports.
- Be observant at airport checkpoints. Don't place the laptop on a conveyor belt until you are ready to walk through the checkpoint.

Portable Drives

Portable drives, also known as flash drives, have become popular due to their ease of portability and convenience. These lightweight devices can hold large amounts of your company's information and can be used on any computer with a USB port.

Dangers from the use of flash drives include:

- Viruses from infected documents and programs when the drives are used at multiple computers.
- Malicious software including shareware, software pranks and inappropriate files that affect productivity and violate corporate policies.
- Data loss: flash drives have little to no security features and can hold a large amount of information, thereby opening the door for the potential for information to fall into the wrong hands.

Protect yourself and your company:

- Look for flash drives with built-in security features or those that require passwords.
- Educate users on the risks that flash drives can present and establish policies for the use and removal of the drives.
- Configure anti-virus software to scan portable drives and removable media. Scan files before opening them.
- Always include return information for drives that are lost or misplaced. Consider only providing an address and not the company name.

Internet Safety
In Your Office

Avoid the Lure of Phishing and Fraudulent Email

Phishing is online deception to obtain individuals' personal data or other valuable information. Con artists send millions of fraudulent email messages that appear to come from trustworthy Web sites, such as those of banks and credit card companies, and ask consumers to provide confidential information. As scam artists become more sophisticated, it is increasingly difficult to discern legitimate Web sites from fake ones.

Telltale signs of phishing scams are:

- Requests, via email, for passwords, login names, Social Security numbers and other personal information.
- Threats to close an account, or take other action, quickly.
- Generic salutations; email messages rarely contain a person's first or last name, and are addressed "Dear Valued Customer," "Dear Sir" or "Dear Madam."
- URLs that resemble the names of well-known companies but are altered slightly by adding, omitting or transposing letters (e.g., www.microsoft.com could appear as www.micosoft.com).

To avoid being victimized by fraudulent email and phishing scams, users should install and update:

- Phishing filters, anti-virus software and anti-spyware software.

Individuals who believe they have been victimized by phishing scams should:

- Report the incident to their credit card companies and to the Federal Trade Commission.
- Change the passwords on all of their online accounts.
- Review credit card and bank statements carefully for unexplained charges or inquiries initiated by a third party.

Corporate IT Best Practices

Organizations that want to minimize disruptions that computer security breaches cause should treat IT as a business unit that sets and meets specific, quantifiable objectives, much like operating divisions, product development and marketing units do.

Successful IT departments:

- Use portfolio management, project management or related methods to set priorities.
- Employ IT-dedicated financial officers.
- Make CIOs members of corporate boards or executive committees.
- Conduct regular strategic planning meetings to ensure alignment with the organization's strategic business objectives.
- Conduct internal customer satisfaction surveys.
- Perform financial audits on the IT function.
- Develop future leaders to ensure continuity.
- Win and showcase IT awards.

Helpful Links and Resources

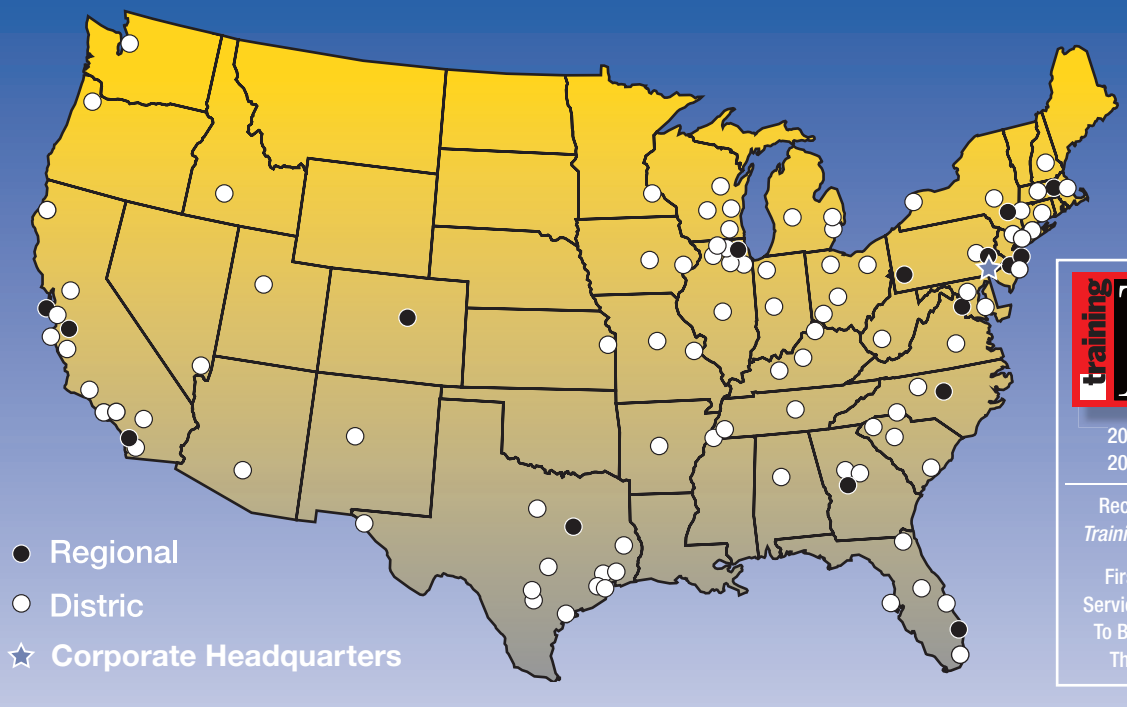
http://www.cert.org/tech_tips/email_spoofing.html

http://www.cio.com/archive/050104/best.html

http://www.microsoft.com/athome/security/email/attachments.mspx

http://www.windowsecurity.com/whitepaper/misc/How_to_protect_from SpoofedFordged_ email

AlliedBarton. Providing Quality Security Services Coast to Coast.



training TOP 125

2007 Winner
2006 Winner

Recognized By *Training* Magazine.

First Security Services Company To Be Named To The Top 125

AlliedBarton Fast Facts

Award-winning Quality Training – Leads the industry with innovative Web-based training through AlliedBarton Academy. A majority of our employees voluntarily participate in continuing education.

American-owned – The largest American-owned and managed contract security services firm.

National Presence – More than 100 offices nationwide serving customers coast to coast.

Fortune 500 Clients – Serves many Fortune 500 and Fortune 100 companies.

Professional Personnel – Offers employees competitive wages and one of the best benefits packages in the industry.

Leading-edge Technology – Utilizes a coast-to-coast Wide Area Network supported by thousands of computers providing real-time access to fully integrated business systems.

Focused Expertise – Our focus is security officer services: great officers who are well-trained and provide peace of mind for you.

Specialized Services – AlliedBarton brings a wealth of experience in several key markets with specialized services designed for the unique demands of each market.

Glossary of Terms

Adware – A component of software applications that displays ads while the program is running.

Bluetooth® – A protocol for short-range wireless communication between multiple kinds of devices, such as PDAs, computers and cell phones.

Browser – An application, such as Microsoft Internet Explorer, that locates and displays Web pages.

Firewall – A software program designed to control access between two networks.

Incident Response – A plan for reporting, analyzing, prioritizing, investigating, and responding to breaches in computer or network security.

Malware – Malicious software, such as a virus, designed specifically to damage or disrupt a system.

Security Alerts – Notices posted on a computer when virus protection software identifies a virus, worm or other potential threat to a network.

Spyware – Software that gathers information about a user's Web-surfing habits for marketing purposes, and without the user's permission.

URL – Uniform Resource Locator. The technical term for a Web address.

Vulnerability Scanning – Security measures an organization takes to protect its network and individual computers from viruses and other threats.

The information contained in this guide is provided strictly as a reference guide and useful resource. AlliedBarton Security Services assumes no responsibility for the accuracy or reliability of the information presented in this guide.

ALLIEDBARTON® SECURITY SERVICES

1-866-825-5433 • AlliedBarton.com

AMERICAN OWNED. AMERICAN MANAGED.

1969