

*Webcentric Computer Services has provided this free downloadable document as a public service. We highly recommend the advice given below. We hope that the effort everyone contributes, from the individual to the corporation, toward securing their systems against cybercrime and cyberterrorism, will make the Internet a safer place for all.*

# The National Strategy to Secure Cyberspace

From the President's Critical Infrastructure Protection Board Draft Document. \*

## LEVEL 1: THE HOME USER AND SMALL BUSINESS

The strategic goal is to empower the home user and small business person to protect their cyberspace and prevent it from being used to attack others. This goal can be achieved through the following:

- raising cybersecurity awareness of the home user and small business, including children and students;
- making it easier for home users and small businesses to keep current with anti-virus software, software patches, and firewalls, perhaps through activity by the Internet service providers;
- encouraging and helping facilitate the installation and use of firewalls on all broadband Internet connections, such as cable modems, DSL, satellite and wireless; and,
- bringing cybersecurity resources closer to the users through local organizations and educational courses. Issues and Challenges

### ***Too Small to Matter?***

Many Americans think that those who would seek to damage us in cyberspace would certainly direct their attacks at major government departments and large corporations. They think cybersecurity is someone else's problem, not the concern of the home Internet user or the small business owner. Unfortunately, such beliefs are inaccurate. Even the home user and small business can be damaged severely and, in some cases, can be used to severely damage others. See table to the right for some examples of what can, and does, happen.

### ***Will It Happen to Me?***

Unfortunately, Americans live in an environment in which cyber attacks of the types described in this Strategy are common. As more and more tools become available to auto-mate these attacks, reaching each and every user becomes easier to do. For example, the "Honeynet Project" uses "dummy" systems attached to the Internet to measure actual computer attacks. According to the project's most recent results, a random computer on the Internet is scanned, meaning it is checked for its presence, setup or weaknesses, dozens of times a day. A common home user setup the project created was hacked five times in four days. Home users or businesses with larger systems are also a target. Systems are subjected to certain scans across the Internet an average of 17 times a day. In some cases, insecure servers have been hacked 15 minutes after plugging into the Internet.

### ***Secure Internet Use***

Using the Internet in a secure manner does not just happen. Rather it is the purposeful result of both awareness and the availability of services and tools which facilitate secure Internet use. It is often difficult for home users and small businesses to access secure Internet services. For example, many home users and small businesses do not use firewalls to protect their computers from unauthorized intrusions. "Always-on-connections" to the Internet, such as broadband, digital service line (DSL), wireless and satellite services, are increasing in popularity. Such connections offer tremendous speed and efficiency. However, they also present unique challenges, because many users are not aware of the security

implications of an “always-on-connection.” For example, these connections generally mean that larger amounts of data can be sent at any time and the data can be sent continuously. These two factors can be exploited and used to attack other systems, possibly even resulting in nationally significant damage. Facilitating and promoting more secure use of the Internet by home users and small business can be greatly advanced by the entire product chain that prepares the consumer for the Internet. The Internet service providers, hardware manufacturers, software vendors, retailers, and providers of security services can all facilitate this effort by making products and services available and easy to use.

### **What can happen What it means**

*Hard Drive Crashing* - A common problem caused by computer viruses on home and small business computers has been extensive damage to files, software, and operating systems that can leave the user with a blank screen and costly repair bills. Often, more importantly, the small business owner or home user may lose irreplaceable data, such as customer records or personal correspondence.

*Identity Theft* - Information stored on a home computer may provide a hacker with enough personal data that the thief could apply for a credit card or identification in the user’s name.

*Credit Theft* - Rather than applying for a new credit card, a thief might just use credit card data on the hard drive of a home user or small business to buy products online and have them shipped to a drop site, such as a commercial “mail box” store.

*Tunneling* - When employees work at home and then transfer files to a computer at the office, there is a potential that someone could remotely gain access to the home PC and place a secret file in a document that ends up on the company system.

*Extortion* - For the small businesses, someone may access the customer’s names and credit card numbers and threaten to post that information on a Web site, unless the business owner pays up.

*Zombies* - Automatic programs search for systems that are connected to the Internet, but are unprotected, take them over without the owner’s knowledge, and use them for malicious purposes.

*Compromise of Private Information* - Some viruses send private or confidential files from a user’s hard drive to people in the user’s email address book.

### **Five Steps to Safety**

There are many places a homeowner, parent, or small business person can turn for help in avoiding security problems on the Internet. Before reviewing the helpful web sites cited below, consider these five simple steps:

*1. Use a Tough Password:* Hackers use software that is commonly available on the Internet to guess passwords and gain access to personal accounts and computers. It is important to use a strong password and change it on a regular basis. Strong passwords usually include:

- at least eight digits;
- a mix of upper and lower case letters;
- a random mix of letters and numbers (not just numbers at the end); and,
- keyboard symbols (#,\$,&, \*).

Home users should change their password at least once every six months, perhaps when the clocks change to daylight saving time and back to standard time.

*2. Maintain an Updated Virus Protection Program:* New viruses appear weekly and the new ones are the most frequent source of damage. The virus protection programs that come installed on the computer are quickly out of date, but they can be kept current by enrolling with the antivirus company for an update program. Many update programs now offer automatic notification of new data, so that the user does not need to remember to go to the antivirus site every week.

*3. Update Patches:*

Many commonly used soft-ware programs (operating systems, web browsers, e-mail readers, and others) are regularly discovered to have security holes or flaws. The software companies issue the equivalent of "recall notices," but unlike a similar notice from a car company, it may not appear in the mail. Typically, a user has to go to the software company's web page to discover the problem and the solution. The solution is usually a small amount of additional software that can be downloaded over the Internet. These fixes, called "patches," are recommended for most home users and small businesses running uncomplicated systems. (In larger systems, the patch must be analyzed first to see if it will create conflicts with other programs.)

*4. Filtering:* Parents may want to consider managing their children's Internet use with software that allows them access to age-appropriate sites and materials. Many ISPs offer such software or filters, or they can be obtained from private vendors. In addition to filtering inappropriate sites, a parent may wish to limit the people from whom their child can receive e-mail. Most ISPs allow users to filter by listing the addresses from which they are willing to receive e-mail on all e-mail accounts they maintain, or just on their children's.

*5. Firewalls:* If you Have a Cable Modem, Digital Subscriber Line (DSL), Satellite or Other High Speed Connection, you should install a firewall. A high-speed connection that is always connected to the Internet (or more often than with dial up modems) makes the home user or small business an attractive target for the "bots" that search the Internet automatically for insecure connections. Even with updated virus software and current patches, smart "bots" can find a way to get into a system without the user knowing it. To prevent such covert entries, those with broadband connections (e.g., DSL, cable, satellite or wire-less) should have additional software, known as a "firewall." Firewalls can be easily configured to close the many doors to the Internet that all computers have, leaving open only the few that people typically use (e.g., for e-mail and web browsing). A user can specify what Internet programs are trusted to enter, and require all others to knock and be granted permission. (*Even dial-up should have a firewall if you are connected for long periods of time - Webcentric Computer Services*).

### ***Where to go for General Cybersecurity Advice***

An alliance of government agencies, corporations, and nongovernmental organizations, have joined to form the "National Cyber Security Alliance" to help home users, parents, and small businesses. Their web site is filled with helpful information and links to other sites with additional data. Go to: [www.StaySafeOnLine.info](http://www.StaySafeOnLine.info).

### ***For Small Businesses***

Small business persons may want to seek cybersecurity ideas from local programs at nearby community colleges or chambers of commerce. On the national level, the Federal government's Small Business Administration ([www.sba.gov](http://www.sba.gov)) and the not-for-profit National Federation of Small Businesses ([www.nfib.com](http://www.nfib.com)) can also provide assistance. In many larger cities, the National Infrastructure Protection Center part-ners with local businesses, the FBI, and academic experts in chapters of "Infragard", a grass roots public-private partnership for cybersecurity and against cybercrime, [www.infragard.net](http://www.infragard.net). In some metropolitan areas, the U.S. Secret Service sponsors a public-private partnership for cybersecurity related to financial institutions, credit cards, and cell phone theft. These groups are called the "Electronic Crimes Task Forces," [www.uss.gov/ectf.htm](http://www.uss.gov/ectf.htm). In addition, the Computer Security Division of the National Institute of Standards and Technology maintains a computer security resources web page which provides

helpful links to other centers of expertise where users can locate more alerts, software updates, and lists of the most common security threats, [www.csrc.nist.gov](http://www.csrc.nist.gov) .

### ***For Parents and Teachers***

In addition to the web sites already noted above that provide filters and teaching ideas, there are additional resources online that can help plan curricula, provide children with good advice, and help parents to decide what is safe:

The “CyberSmart School Program” is designed for teachers and provides lesson plans and professional development material. See [www.cybersmart.org](http://www.cybersmart.org) .

“NetSmartz” is designed to teach children directly about what to watch out for when surfing the net. See [www.netsmartz.org](http://www.netsmartz.org) .

“Get NetWise” is a resource for families trying to decide what they should consider about their children’s web access. See [www.getnet-wise.org](http://www.getnet-wise.org) .

The Information Technology Association Foundation sponsors “Cybercitizen Awareness,” which teaches teenagers about ethics online and the risks of cybercrime. Its site also provides material for teachers, parents, and smaller children. See [www.cybercitizenship.org](http://www.cybercitizenship.org).

### **Specific actions that government and nongovernment entities can take to promote cybersecurity.\***

R1-1 Because automated hacking programs scan the Internet for unprotected broadband connections to exploit, those home users and small businesses planning to install a DSL or cable modem should consider installing firewall software first. (Some Internet service providers (ISPs), offer firewall software with DSL or cable modem set up.) Once firewall software is installed, it is important to regularly update it by going to the vendor’s web site.

R1-2 Because new computer viruses are introduced every week, home users and small businesses should regularly ensure that they are running an up-to-date “antivirus system.” (Some antivirus vendors offer automatic updates online. Some Internet service providers scan all incoming e-mail for viruses before the e-mail gets to the user’s computer.)

R1-3 Because new viruses often come as e-mail, home users should use caution when opening e-mail from unknown senders, particularly those with attachments. To reduce the number of unknown senders, home users should consider using software that controls unsolicited advertisements, called “spam.” (Some ISPs offer programs to block spam. Some ISPs also offer to block all incoming e-mail except from those friends and associates that the user selects.)

R1-4 Home users should also regularly update their personal computer’s operating systems (such as Microsoft Windows, Linux) and major applications (software that browses the Internet or creates documents, charts, tables, etc.) for security enhancements by going to the vendors’ web sites. (Some software vendors offer automatic updates online.)

R1-5 Internet service providers, antivirus software companies, and operating system/application software developers should consider joint efforts to make it easier for the home user and small business to obtain security software and updates automatically and in a timely manner, including warning messages to home users about updates and new software patches.

### **PROGRAMS: *Existing efforts in cybersecurity.***

P1-1 Stay Safe Online web site: An alliance of government agencies, corporations, and non-government organizations have come together to form the National Cyber Security Alliance to help home users,

parents, and small businesses. Their web site is filled with helpful information and links to other sites with additional data. Go to [www.StaySafeOnline.info](http://www.StaySafeOnline.info) .

P1-2 FTC "Guide for E-Consumers," [www.ftc.gov/bcp/online/pubs/alerts/glblalrt.htm](http://www.ftc.gov/bcp/online/pubs/alerts/glblalrt.htm) .

P1-3 FTC "How to Be Web Ready," [www.ftc.gov/bcp/online/pubs/online/webready/index.htm](http://www.ftc.gov/bcp/online/pubs/online/webready/index.htm) .

P1-4 FTC "How to Protect Kids' Privacy Online," [www.ftc.gov/bcp/online/pubs/online/kidsprivacy.htm](http://www.ftc.gov/bcp/online/pubs/online/kidsprivacy.htm) .

P1-5 InfraGard: In many larger cities, the National Infrastructure Protection Center partners with local businesses, the FBI, and academic experts in chapters of InfraGard, a grass roots public-private partnership for cybersecurity and against cybercrime [www.Infragard.net](http://www.Infragard.net) .

P1-6 The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) <http://www1.ifccfbi.gov/index.asp> .

P1-7 American Library Association, "The Librarian's Guide to Cyberspace for Parents and Kids," [www.ala.org/parentspage/greatsites/guide.html](http://www.ala.org/parentspage/greatsites/guide.html) .

P1-8 The FTC, U.S. Secret Service, the FBI, and others have formed the "Consumer Sentinel" to help consumers get the facts on frauds from Internet cons, prize promotions, work-at-home schemes, and tele-marketing scams to identity theft and make it easy to file fraud complaints so they can be shared with law enforcement officials across the nation [www.consumer.gov/sentinel/](http://www.consumer.gov/sentinel/) .

P1-9 DOJs Computer Crime Web site: information regarding a wide variety of computer crime and computer security issues, including a children's Cyberethics page and a link to invite DOJ experts to speak [www.cybercrime.gov](http://www.cybercrime.gov) .

**DISCUSSIONS: Issues highlighted for continued analysis, debate, and discussion.**

D1-1 The biggest business in America is small business. Working through the SBA, many small businesses are able to obtain loans guaranteed by the Federal government. Increasingly, the cybersecurity of small business can impact its employees and the broader economy. Should SBA loans require an IT security check-list?

D1-2 How can parents and children create a useful dialogue about securing their families' cyber-space? Cybersecurity is an area where parents and children each bring their own experience and expertise. By sharing these experiences, families can improve the cybersecurity of their household and contribute to an overall increase in America's cybersecurity.

*\*Note: The feasibility and cost effectiveness of these recommendations will vary across entities. Individual entities should take into account their particular and changing circumstances in choosing whether to apply them.*

END DRAFT

*\*This document provided free of charge by Webcentric Computer Services. WCS is a consulting and Web design company specializing in small business solutions including custom Web site development, maintenance, Search Engine Positioning and e-commerce. We do consulting work for the small or home office including new systems, peripherals, networks, software, and computer virus/security issues. We also offer custom programming services including C, C++, C#, Java, VB, CGI/PERL, Java Script, VBScript, ASP, SQL, MySQL and XML.*

For more information about our services, see <http://www.web-centric.net>  
Email: [info@web-centric.net](mailto:info@web-centric.net) Phone: (209)296-4053 Fax: (707) 885-4679