WEBROOT® SOFTWARE

A HANDBOOK TO SAFE ONLINE HOLIDAY SHOPPING

webroot SOFTWARE

Companion Guide to
State of Internet Security:
Protecting Consumers Online
Full report available at www.webroot.com

Table of Contents

About the Study

In October 2007, Webroot® Software conducted its Holiday Shopping Survey in the U.S., Canada and the UK. All 1,810 respondents use a Windows PC and plan to purchase holiday gifts (on or off line) this year, and all have bought at least one item online in the past year. Respondents were divided evenly between the three countries with an equal number of males and females.

Did You Know?

- Seventy-four percent of online shoppers in the U.S., UK and Canada say they have concerns about shopping online.
- Forty-eight percent of online shoppers are concerned about stolen credit card or bank account numbers, 49 percent about identity theft, and 42 percent about spyware or virus infections.
- Seventy percent of U.S. online shoppers are comfortable entering their credit card online.
- However, in the last year, 48 percent of online shoppers in the U.S. have experienced spyware or virus infections, which can lead to identity theft. Almost ten percent experienced online fraud, and 7.5 percent had their credit card numbers stolen.

The Benefits of Online Shopping

The U.S. National Retail Federation recently released a forecast that Internet-related sales (excluding travel) will jump 19.1 percent to $174.5 billion in 2007. According to the Webroot Holiday Shopping Survey, 87.7 percent of respondents plan to buy some of their holiday purchases online this year. In contrast, only 79.5 percent of the same group did some of their holiday shopping online last year.

In addition, the percentage of total holiday shopping that individuals plan to do online is increasing. Last year, 21.9 percent of the respondents did more than half of their holiday shopping online, whereas 32.1 percent indicate they plan to do more than half of their holiday shopping online this year, an increase of over 10 percent.

These trends are not surprising given the large number of respondents that identified numerous benefits of online shopping.

Benefits of Online Shopping	
Benefit	**Percentage**
Can shop anytime	95.8%
Avoid long lines at checkout counters	93.4%
Easier to comparison shop	88.7%
Greater selection (more items to choose from)	76.6%
Lower prices	74.9%
Online stores provide gift wrapping and shipping	50.6%

Figure 1 – Source: Webroot Holiday Shopping Survey, October 2007 (N=1,181)

Almost 30 percent of respondents find the benefits of online shopping so significant that they prefer to shop online for their holiday gifts instead of going to stores or ordering via phone.

However, while online shopping can offer greater convenience and selection, there are also some risks associated with Internet use. Just like in the physical world, consumers need to be smart shoppers when they venture to the cyber mall.

The Risks of Online Shopping

Given the increasing number of online shoppers, and the increasing percentage of online holiday purchases, it is essential that individuals take steps to ensure their personal information is safe and their transactions are secure.

Among the most significant risks online shoppers face is the theft of sensitive personal information, such as credit card, bank account and identification numbers, which can lead to identity theft. Spyware infections are a serious concern since they put this type of personal information at risk.

Risks of Online Shopping

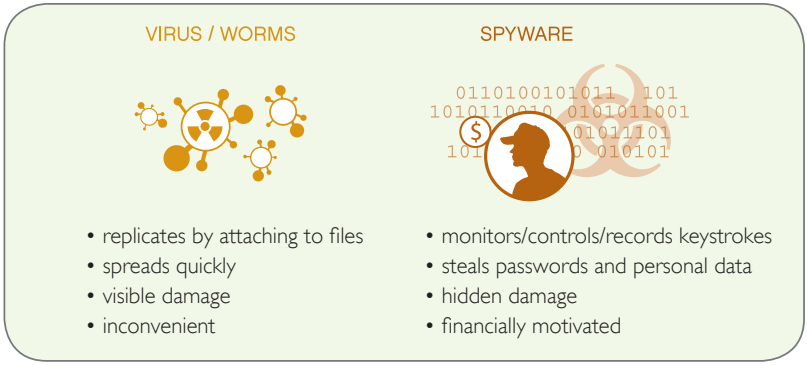
Risks	Extremely concerned	Very concerned	Somewhat concerned	Slightly concerned	Not at all concerned
Stolen credit card or bank account numbers	25.8%	21.7%	23.0%	20.3%	9.3%
Identity theft	24.6%	23.2%	22.9%	20.8%	8.5%
Stolen identification number (such as Social Security)	21.8%	18.5%	19.5%	20.2%	20.0%
Spyware or virus infections	19.1%	22.6%	25.6%	20.8%	12.0%
Loss of privacy	18.0%	20.4%	25.5%	22.7%	13.5%

Figure 2 – Source: Webroot Holiday Shopping Survey, October 2007 (N=1,181)

Online criminals use sophisticated tools to find unprotected and vulnerable networks and computers. Today's spyware programs are more complex and dangerous than ever before. They infect machines with more spyware more deeply, to make removal extremely difficult. Further complicating removal efforts, many pieces of spyware monitor each other so that when removal is attempted, the malicious code will be repopulated or downloaded from the Internet.

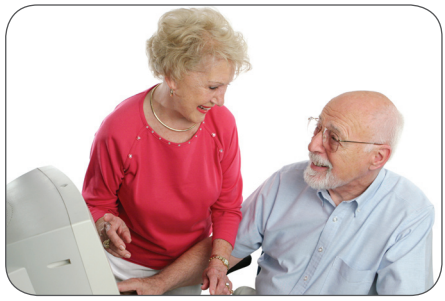
Spyware vs. Viruses

In contrast to viruses that typically make their presence known by spreading across many systems simultaneously and seriously impacting machine functionality, the success of spyware programs depends on their stealthy nature. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware program writers are adept at covertly infiltrating a system and installing programs deep within a computer or network.



Even things that may seem more innocuous or just mildly annoying, like spam or pop-up ads, are increasingly dangerous as they can be used to carry more serious threats, such as spyware, viruses and worms. There is almost zero cost associated with mass junk mailings. This makes spam an easy and cheap delivery mechanism for malicious attacks that can have significant impact on both businesses and individual consumers.

Tips for Safer Online Shopping



1. **Install Security Software:** A layered approach to security is best. Your PC should have three types of security software installed and up-to-date; antispyware, antivirus, and a firewall. Be sure to purchase anything you might be missing.

2. **Know the Retailer:** It is always a good idea to do business with companies you already know and trust. If you are unfamiliar with the retailer you want to purchase from, it's best to look for more information about the company. Contact the Better Business Bureau or the Office of the State Attorney General in the state where the retailer is located, which can be accessed through the National Association of Attorneys General.

3. **Monitor Your Credit:** Many victims don't realize they are a victim until they have lost a lot of money. In fact, according to the FTC, it takes the average online identity theft victim about five months to remediate the problem. Agencies like Equifax, Experian and TransUnion are excellent sources to monitor your credit and provide alerts.

4. **Use a Credit Card not a Debit Card:** When shopping online, use a credit card not a debit card. If you are a victim of fraud or cybercrime, federal laws limit your liability for unauthorized charges to $50.

5. **Ask About a "Single Use" Credit Card:** Many credit card companies are using a new technology that allows them to issue single use credit card numbers for online purchases – you can avoid using your real credit card number online.

6. **Read the Privacy Policy:** Read the merchant's privacy policy carefully to find out what information they are gathering from you and more importantly, how the information will be used. If a site does not have a privacy policy posted, you may not want to do business with it. If it does have a privacy policy, there will probably be a link to it from the seller's home page, or it could be included with the Legal Terms.

7. **Purchase from a Secure Website:** When providing payment or personal information, make sure you are on a secure web page. Typically, this is indicated by an "https" at the beginning of the web address. (See the "How to Identify a Secure Website" section.) Also, do not shop on an unencrypted or open wireless network. Using a secure online payment service such as PayPal is also a good practice.

8. **Avoid Purchases on Public Computers:** Using a public computers to make online purchases, like in a library, hotel lobby or computer lab, is a bad idea. A hacker or someone with malicious intentions can easily put a keylogger on a computer before you use it; this would allow them to know everything you've typed – including credit card numbers and passwords.

9. **Beware Phishing Attempts:** If after making a purchase you receive an email that asks for personal information – or at any time – be very suspicious. Many times, hackers will attempt to trick folks into thinking they are getting an email from a company they do business with, but they are actually just "phishing" for private information. Legitimate businesses do not send emails claiming problems with an order or an account to lure the "buyer" into revealing financial information. Pick up the phone and call the contact number on the Web site where you made the purchase to ask if there was a problem with your transaction.

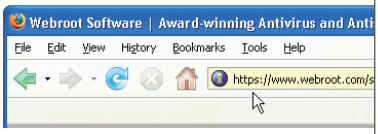
10. **Avoid Saving Your Credit Card Number Online:** Many Web sites provide you the option of saving your credit card information in an attempt to make future transactions easier. Your credit card would then be stored in a database that you have no control over. If the company's Web ssite is hacked, your personal information would potentially be exposed.

How to Identify a Secure Website

Only make purchases from secure websites. The quickest and easiest way to tell if you're on a secure website is to look at the web address. Secured websites will start with "https:" instead of "http:" – see Figures 3 and 4.

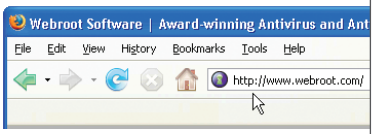
Note: You do not need to find websites that are secure on every page. Instead, you only need a page to be secure when private information like credit card numbers and addresses are requested. This typically would happen during the checkout process of an online purchase.

Figure 3



The "s" following the "http" indicates the Web page is secure.

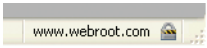
Figure 4



Web pages that appear with "http" and no "s" are not secure.

Another way to identify a secure web page is to look for a "lock" icon in one of the corners of your web browser – see Figure 5.

Figure 5



A padlock icon in the corner of your browser indicates the Web page is secure.

Many websites will indicate that they are protected with Secure Socket Layer (SSL) technology – see Figure 6.

Figure 6

GeoTrust is one of many companies that secure websites with SSL technology.

Other logos that indicate a trusted vendor include the TRUSTe logo and the Better Business Bureau OnLine Reliability logo:

Resources

American Bar Association, Section on Business Law
www.safeshopping.org

Bank Safe Online
www.banksafeonline.org.uk

Better Business Bureau (BBB)
www.bbb.org

Canada Safety Council
www.safety-council.org/info/child/webrules.html

Equifax
www.equifax.com

Experian
www.experian.com

Fraud Reduction
www.uk-fraud.info

Get Safe Online
www.getsafeonline.org

Insafe
www.saferinternet.org

Internet Crime Complaint Center
www.ic3.gov

iSAFE
www.isafe.org

ITSafe
www.itsafe.gov.uk

OnGuard Online
onguardonline.gov/index.html

National Association of Attorneys General
www.naag.org/find.htm

National Cyber Security Alliance
www.staysafeonline.com

National Retail Federation
www.nrf.com

TransUnion
www.transunion.com

TRUSTe Directory
www.truste.org/about/member_list.php

UK Office of Fair Trading
www.oft.gov.uk/oft_and_cd

U.S. Federal Trade Commission Identity Theft Site
www.ftc.gov/bcp/edu/microsites/idtheft/index.html

US President's Identity Theft Task Force
www.idtheft.gov

Visa Security Information
www.visa.com/security

Glossary

Adware
Adware is advertising-supported software that displays pop-up advertisements and is usually available via free downloads from the Internet Adware is often bundled with or embedded within freeware, utilitarian programs like filesharing applications, search utilities, information providing programs (such as clocks, messengers, alerts, weather, and so on), and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Although seemingly harmless, some adware programs may track your Web surfing habits. Deleting adware may result in the deletion of the bundled freeware application.

Antispyware software
Antispyware software protects a PC from spyware infection. Spyware protection software will find and remove spyware without system interruption.

Attachment
A file that has been added to an email. It could be something like a photograph or a clip of your favorite song. It could be something harmful to your computer, like a virus. Remind children to never open an attachment or email from someone they don't know.

Blog (short for Web log)
A web log is usually defined as a personal or non-commercial web site that uses a dated log format (usually with the most recent at the top of the page) and contains links to other web sites along with commentary about those sites. A web log is updated frequently and sometimes groups links by specific subjects, such as politics, news, pop culture, or computers.

Botnet
A botnet is a collection of computers running remote control software programs and under a common command and control infrastructure via a public or private network. Botnets can be used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Hijackers
Sometimes called Home Page Hijackers, browser hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, browser hijackers may redirect your searches to "pay-per-search" Web sites.

Chat room
An interactive forum where you can talk in real time. The chat room is the place or location online where the chat is taking place. Many chat rooms are established so that people can discuss a common interest like music or movies.

Cookie (or Adware Cookie)
Cookies are pieces of information that are generated by a Web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your Web experience. However, some Web sites now issue adware cookies, which allow multiple Web sites to store and access cookies that may contain personal information (surfing habits, usernames and passwords, areas of interest, etc.), and then simultaneously share the information with other Web sites. Adware cookies are installed and accessed without your knowledge or consent, and in some cases this sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms.

Dialer
Dialers have the ability to disconnect your computer from your local Internet provider and reconnect you to the Internet using an expensive pornographic, toll, or international phone number. They do not spy on you, but they have the ability to run in the background, hiding their presence. Dialers may rack up significant long distance phone charges.

Distributed Denial-of-Service (DDoS) Attack
A means of burdening or effectively shutting down a system by bombarding it with an overwhelming amount of traffic. DDoS attacks are often launched using botnets. A vulnerability in one computer system can be exploited to make it the DDoS master.

Domain Name
A name given to the numerical or Internet Protocol (IP) address of a web site. For example, webroot.com is the domain name for Webroot Software, Inc.

Drive-by download
When programs are downloaded without the user's knowledge or consent. Most often accomplished when the user clicks to close or eliminate a random advertisement or other dialogue box.

Encryption
Encryption is the scrambling of data so it becomes difficult to unscramble and interpret.

Encryption
Encryption is the scrambling of data so it becomes difficult to unscramble and interpret.

Exploit/Security Exploit
A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system.

File-Sharing Programs
Programs that allow many different users to access the same file at the same time. These programs are usually used to illegally download music and software.

Filter
Software designed to restrict content viewed via a web browser.

Firewall
A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules. Firewalls provide effective protection against worm infection, but not against spyware like Trojans, which hide in legitimate applications, then install secretly on a user's PC when the application is launched.

Hijackers (Home Page Hijacker or Browser Hijacker)
Hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, home page hijackers may redirect your searches to "pay-per-search" Web sites.

Host File
The host file stores the Internet Protocol address of a device connected to a computer network. Some spyware can change a host file in order to redirect users from a site that they want to visit to sites that the spyware company wants them to visit.

Hyperlink (also called link)
An image or a portion of text that, when clicked, allows electronic connections. These connections access other Internet materials such as images, sounds, animations, videos, or other web pages.

Information Privacy
The interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

Keylogger
A keylogger is a type of system monitor that has the ability to record all keystrokes on your computer. Therefore, a keylogger can record and log your email conversations, chat room conversations, instant messages, and any other typed material. They have the ability to run in the background, hiding their presence. In some cases, a third party may be able to obtain private information such as usernames, passwords, credit card numbers or Social Security numbers.

Malware
Short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a computer.

Network
A network is created when computers are connected, allowing people to share information. The Internet is an example of a large network.

Operating System
The operating system is usually the underlying software that enables you to interact with the computer. The operating system controls the computer storage, communications and task management functions. Examples of common operating stems include: MS-DOS, Macintosh, Linux, Windows. Also: OS, DOS.

Parental Controls
Software that allows a parent to monitor or limit what a child can see or do on a computer.

Personally Identifiable Information (PII)
Information such as name, address, phone number, credit card information, bank account information, or social security number.

Pharming
An online scam that attacks the browser's address bar. Users type in what they think is a valid web-site address and are unknowingly redirected to an illegitimate site that steals their personal information.

Phishing
An online scam that uses email to "fish" for users' private information by imitating legitimate companies. People are lured into sharing user names, passwords, account information or credit-card numbers.

Piracy
Illegally copying copyrighted software, music or movies.

Post
To leave a message on a newsgroup or bulletin board.

Privacy
A privacy policy outlines the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary.

Privacy Policy
A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules. Firewalls provide effective protection against worm infection, but not against spyware like Trojans, which hide in legitimate applications, then install secretly on a user's PC when the application is launched.

Registry
A computer registry is a database integrated into certain operating systems which stores information, including user preferences, settings and license information, about hardware and software installed on a user's computer. Spyware often changes registry values in order to take control of parts of the system. These changes can impair the regular function of the computer.

"Remove Me"
Remove me is an option often included in spam which is fake. That is, if you respond to request removal, you very well may be subjecting yourself to more spam, because by responding, the sender knows that your email account is active. A 2002 study performed by the FTC demonstrated that in 63% of the cases where a spam offered a "remove me" option, responding either did nothing or resulted in more email.

Rootkit
A rootkit is a program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit.

Search Engine
A program that searches information on the world wide web by looking for specific keywords and returns a list of information found on that topic. Google.com is an example of a search engine.

Server
A special software package that connects to a network and provides data. The computer that this software runs on is also often called the server.

Shareware
Software distributed for evaluation without cost, but that requires payment to the author for full rights is commonly called shareware. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is pirating.

Software
Programs that help your computer work. For example, a filter is a type of software that can keep unwanted Internet content off of your computer.

Spam
Spam is the common name for unsolicited commercial email. It is sent, usually in bulk, through "open-relays" to millions of persons. Spam is cost-shifted advertising. It takes a toll on Internet users' time, their resources, and the resources of Internet Service Providers (ISP). Most recently, spammers have begun to send advertisements via text message to cell phones.

Spyware
Spyware is any application that makes potentially unwanted changes to your computer while collecting information about your computer activities. This information may then be sent to a third party for malicious purposes, without your knowledge or consent. Spyware can be distributed by bundling with freeware or shareware, through email or instant messenger, as an ActiveX® installation, or by someone with access to your computer. Unlike traditional personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove without the use of an effective anti-spyware program.

Streaming (Media)
The exchange of video clips, sound, or other types of media over the Internet. It is a way for the user to quickly download these files.

System Monitor
System monitors have the ability to monitor all computer activity. They range in capabilities and may record some or all of the following: keystrokes, emails, chat room conversations, instant messages, Web sites visited, programs run, time spent, and even usernames and passwords. The information is gathered via remote access or sent by email, and may then be stored for later retrieval. In some cases, a third party may be able to gain access to private information such as usernames, passwords, credit card numbers or Social Security numbers.

TCP/IP (Transmission Control Protocol/ Internet Protocol)
The protocols or conventions that computers use to communicate over the Internet.

Trojan Horse (also known as Trojan or Backdoor Trojan)
A Trojan horse is a program that allows a hacker to make changes to a computer without the user's knowledge. Unlike a virus, a Trojan does not replicate itself. It is generally disguised as a harmless software program and distributed as an email attachment. Once you open the attachment, the Trojan may install itself on your computer without your knowledge or consent. It has the ability to manage computer files, including creating, deleting, renaming, viewing, or transferring files to or from the computer. It may utilize a program manager that allows a hacker to install, execute, open, or close software programs. The hacker may have the ability to open and close your CD-ROM drive, gain control of your cursor and keyboard, and may even send spam by sending mass emails from your infected computer. Trojans have the ability to run in the background, hiding their presence.

URL (Uniform Resource Locator)
The specific location or address of material on the Internet.

Virus
A program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, many also do damage.

Warez
Pirated or illegally distributed software.

Webmaster
The person responsible for administering a web site.

Whitelisting
A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate for children.

Worm
A program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. The name is an acronym for "write once, read many."

Zip File
Large files that have been compressed to make them easier to send over the Internet. The receiver must download the file with a program that will unzip it, breaking it up into the individual files that were compressed together in order to view the files.

Zombie
A zombie machine is one that has been taken over using remote control software. Zombies are often used to send spam or to attack remote servers with an overwhelming amount of traffic (a Distributed Denial of Service Attack). A collection of many zombies comprise a botnet.

About Webroot Software

Webroot Software, Inc. provides industry leading security software for consumers, enterprises and small and medium businesses worldwide. Globally recognized for its award-winning Spy Sweeper® line of antispyware and antivirus products, Webroot security software consistently receives top review ratings by respected third-party outlets and has been adopted by millions globally. Webroot AntiVirus with AntiSpyware & Firewall provides complete protection against viruses, spyware, data theft and hackers. Webroot Child Safe® offers powerful and easy to use protection to keep kids safe online. Webroot Window Washer® eliminates all traces of PC and Internet activity. Webroot products can be found online at www.webroot.com and on the shelves of leading retailers worldwide.

To find out more visit www.webroot.com or call 800.772.9383.

About the Research

Webroot has been compiling and issuing quarterly reports about trends and research related to Internet security since 2003. In October 2007, Webroot conducted a survey of Windows PC users that plan to purchase holiday gifts (on or offline) this year. All of the 1,811 survey respondents have purchased at least one item online in the past year. Survey Sampling International sent invitations to its online consumer panels in Canada, the United Kingdom and the United States. Respondents were a roughly equal number of men and women in each of the three countries. The margin of error is ±2.3 percentage points for the full sample and ±4.0 percentage points within each country's estimates.

© 2007 All rights reserved. Webroot Software, Inc. Webroot, Spy Sweeper, Child Safe, Window Washer, the Webroot icon and tagline are trademarks or registered trademarks of Webroot Software, Inc. in the United States and other countries. All other trademarks are properties of their respective owners.

NO WARRANTY. Information based on research conducted by Webroot Software, Inc. The information is provided AS-IS and Webroot makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at your own risk. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice.

Certain data is available upon request.

The Best Security
in an Unsecured World™

2560 55th Street • Boulder, CO 80301 • USA
Telephone: 800.772.9383 • Fax: 303.476.2222
www.webroot.com