

Protect Your Vital Data with Today's Technology

Author: Ray La Foy

Safeguard Your Most Valuable Data

A quality security device protects your personal information as well as your computer. Identity theft and viruses don't have to pose a threat. The expert advice, tips and resources at <http://www.securitydeviceonline.com> will help safeguard your most valuable data whenever you're online.

Protect Your Vital Data with Today's Technology

Table of Contents

An Open Door To Your Home Wireless Internet Network Security?	3
Basic Steps To Optimize Your Internet Security	5
Internet Banking Security and Safety	7
Internet Monitoring, Safety And Security	8
Internet network security policies need a radical rethink!	9
Internet Security Basics 101	12
Internet Security Threats: Who Can Read Your Email?	17
Internet Security to Protect Small to Medium Businesses	20
Internet Security: Backups	22
Online Security – Your Responsibilities as a Consumer	24

Protect Your Vital Data with Today's Technology

An Open Door To Your Home Wireless Internet Network Security?

This is not some new fangled techno-speak, it is a real tool to be used for the protection of your wireless internet network and LAN. African American SMBs have to realize that if your Internet connection is on 24/7 then your network, and it is a network that your computer is connected to, is at risk. Any business that uses the Internet to share or exchange information, news, or ideas with clients, vendors, partners, or other locations look in the reflection of your monitor and realize that your business is an unintentional (or intentional) target.

You should already be aware of all the thousands of bugs, viruses, denial of service attacks and other unfriendly items that lurk on the internet and virtually try attacking every second. It's like having a screen door on your most valuable assets. Let's not repeat what you know about, let's look at a larger picture that should concern everyone - the unknown. There are attacks that go unreported for various reasons, these are the ones that the major software and hardware vendors have no clue about and can only warn you after an attack is reported.

If your files, email, identity, client or product information is important to your African American business and you cannot afford a network being down for 24 hours. Then a firewall is what should be between the internet and everything else. You need to expect an intrusion if you have a small amount or no network protection. Hackers have tools that search the Internet 24/7 looking for a vulnerable point to destroy. Overzealous marketers use similar tools to harvest information to use for spamming and unfortunately no one currently calls that a crime that we know as identity theft.

You have a deadbolt and a door lock on your front door and some even have a home security system in place. Why have a screen door latch on your home computer network, when you know there are people trying that door 24/7?

If you want to put a digital rottweiler between your home wireless network and hackers, marketers and other cyber-vandals then evaluate a strong firewall for your African American business.

Don't have the time or resources to get your home wireless network protected and need an African American Wireless Solution Provider partner to be there for you? We can help give you your freedom back...and a whole lot more. Copyright © 2005 Daviyd Peterson About Daviyd: Daviyd Peterson: 10-year consultant, instructor, trainer Helps African-American homeschools bridge the digital divide by becoming computer homeschools. Free article on "Computer Homeschooling" and other related articles <http://www.homeschoolwireless.com/homeschoolwireless.htm> MDTG <309.403.4983 phone/fax>

[Maximum Security System](#)

Protect data, safeguard personal information online with affordable, reliable security devices.

[Learn How I Make \\$12K On eBay® Part Time.](#)

The guide to successfully selling on eBay®

[SystemSuite 6 Professional](#)

Premium collection of essential PC utilities designed to maintain and protect your PC! Earn 40% for

Protect Your Vital Data with Today's Technology

a payout of \$21.78 per sale!

[Write and Sell Ebooks](#)

Two books about writing and selling ebooks Affiliates Make 24.00 per sale

Protect Your Vital Data with Today's Technology

Basic Steps To Optimize Your Internet Security

After seeing many people complain about their weak Internet security I decided to write down some things that will help you for your Internet security.

First, here are some tips to make windows safer : For basic security and update patches install Service Pack 2 for Windows XP or Service Pack 4 for Windows 2000. Once a month use Windows Update so you can get the latest patches. When you download software from the Internet make sure you download it from the original website. Always run anti Trojan and anti virus software. Even if you don't use it you have to make your Internet Explorer as safe as possible. When you access the Internet you are browsing the web using a browser such as Internet Explorer. The Internet Explorer contains several security vulnerabilities. You should make it as safe as possible or switch your default browser to an alternative. You will have to set some options from the Manage Add-Ons in the Internet Options. You will see a list of add-ons that can be activated or deactivated. If you see any unusual entries just deactivate them so you can be sure you don't have a trojan/worm. Under Internet Options -> Security -> Internet -> you will see the Edit Level. You should set it to high in order to disable most of the security threats. Your Web Browser should be ok now. Let's see what we have to do from our email point of view. Because it's built-in in their Windows system lots of users like to use Outlook Express for emailing. But it's a fact that it contains many security vulnerabilities so I advise you to use alternatives. If you use a web based Email (you can browse your email with your web browser) you can delete viruses even if you don't download them to your PC. Make sure you have installed an Anti Virus for 100% virus protection. One that I've found to be very good and never disappointed me is the AVG Anti virus. If you take the time to regularly update it you will be safe enough with it. Lots of people install Firewalls because they believe their Internet security will be higher. I personally disagree. If you do not know how to best configure it, and you have to know much about the tech behind it to do so, it will just make your PC slow and software not working. You can just use the Windows XP SP2 firewall for basic security. All this tips should make your PC safer. I browse the Internet every single day for some time now and they worked great for me. I haven't met a virus/worm for some time now.

ABOUT THE AUTHOR

DSW Distribution Ltd has all you need for your internet security: mcafee antivirus, norton antivirus 2005, microsoft office 2003 standard edition, panda antivirus, windows xp and many more ... Visit us at <http://www.dswtrade.com>

[Internet Security Secrets](#)

Learn how to secure your PC, safeguard your business and protect your family

[Your 10 Free Mind Power Lessons!](#)

You Are Just Moments Away From Discovering How To Instantly Develop Your Mind-Power And Endless Potential

[Power Station Financial Models](#)

Power Station Financial Models Membership Website - Project Finance Spreadsheet MS Excel Models

Protect Your Vital Data with Today's Technology

[Clickbank Profit Feeds Generator](#)

Add Hot, Fresh, Revenue Generating Content Across Your Entire Site Automatically Updated Every Hour 24/7/365

Protect Your Vital Data with Today's Technology

Internet Banking Security and Safety

Is Online Banking A Safe Choice

Many people hesitate to take advantage of Internet banking because they aren't confident it is a safe and secure method for conducting financial business. Fortunately Internet banking is extremely safe and becoming safer and more secure every day. Currently the Internet sends information from computer to computer using unsecured lines of communication. Normally that would allow anyone to access information transferred from one computer to another.

Most banks however provide secure financial service networks using Secure Sockets Layers or other technology that encrypts information you send over the Internet. That means the data you send from one computer to another is encrypted to prevent outsiders from peaking in and seeing your private information.

This technology, referred to as SSL technology is now accepted or compatible with most browsers including Internet Explorer and Netscape Navigator. Usually you'll see a little yellow padlock in the right lower hand corner of your screen, indicating that a page is being secured using this technology.

Other Security Measures

Most Internet banks offer other protective measures to ensure your information is kept safe and secure. Some examples of other security measures in place include:

Secure logins

You will create your own online access account number and code that you will need each time you log in.

Limited logins

Many banks limit the number of times you can attempt to log in per day and lock you out if you exceed this. That way someone can't attempt to break your login code easily.

Limited sessions

Most banks offer limited sessions that require you to re-login after you have been inactive for a period of time preventing anyone from viewing your information if you leave your computer for too long.

About the author:

Article by Frank Owen, visit his web site for more information on internet banking
<http://www.internetbankingfacts.com>

Protect Your Vital Data with Today's Technology

[Clean Surfer](#)

Security software

[Sample Business Letters Now](#)

Sample Business Letters Store

[Database Normalization eBook](#)

Comprehensive eBook on Normalization techniques for general Relational Databases such as Oracle, SQL Server and others

[Instant Home Writing Kit \(Revised Edition\)](#)

One-stop general home/business writing toolkit full of tips, tricks, pointers, and over 80 real-life downloadable writing templates.

Protect Your Vital Data with Today's Technology

Internet Monitoring, Safety And Security

Internet monitoring is a necessary part of having internet service. Whether you allow your children to surf the web or if you have the need to monitor employees, effective programs can be used to help you to do this simply. There are many aspects that can be monitored and the results can be delivered to you privately. No one needs to know that you are using internet monitoring technologies either.

There are many options when it comes to internet monitoring. No matter what your need is in these products, you can expect to use high tech gadgets and software. But, they are simplistic to use. Many software programs that monitor internet usage will tell you such things as how long the individual was online as well as what websites they visited, who they chatted with in instant messages, as well as anything that they input into the web. Emails can be tracked as well as a number of other things.

Why should you use internet monitoring? If you are not sure your employees are using their time on the job for job related tasks, this can help you know for sure. If you are unsure of who your spouse is chatting with at night, consider the use of these monitoring solutions. Do you know if someone is stalking your child as they play games on the web? If they use instant message software, find out who they are talking to and what they are saying. Internet monitoring is really a necessary part of keeping people safe and your business under control. Effective internet monitoring software products can be purchased and installed quickly and discreetly. Be in the know.

There are also many information portals now devoted to the subject and we recommend reading about it at one of these. Try googling for "internet monitoring" and you will be surprised by the abundance of information on the subject. Alternatively you may try looking on Yahoo, MSN or even a decent directory site, all are good sources of this information.

About the author:

for more information please see <http://www.internet-monitoring-help.co.uk>

[Privacy Software: X-Cleaner Anti Spyware](#)

Anti-spyware, inoculation and security tool for windows

[Sig File Profit System.](#)

Make Money With Adsense Now.

[Net Biz Tips](#)

Learn How to Promote any Product or Service Online

[Wholesale Directory](#)

We publish a wholesale directory as well as produce business

Protect Your Vital Data with Today's Technology

Internet network security policies need a radical rethink!

Data-recovery-reviews.com, the leading portal on data storage, data recovery and network security has suggested that internet network security policies that deal with organization wide internet security need a radical rethink. In a recent interview, Gary J, lead editor for data-recovery-reviews.com, suggested that 'Internet network security policies' are flawed in strategy and implementation. Gary suggests that the use of external consultants for the entire internet network security policy framework is not a great idea since the external consultants will find it difficult to grasp the intricacies and business drivers for the network security decisions.

Also, in terms of implementation, the internet network security policy should be disseminated to each and every employee of the company through seminars, handouts and quizzes rather than an innocuous email that no one reads.

Gary also suggested that the network security policy, should capture the latest trends in the network security industry rather than playing catch up. One of the network security aspects that Internet network security policy makers should be worried about now is access to corporate data through a Blackberry or a mobile phone.

Gary P is one of the editors of Data-recovery-reviews.com, is the leading portal on data storage, data recovery and network security. A recent article on [IS internet network security policy frameworks](#)

About the Author

Gary is a leading freelance data center disaster recovery consultant having consulting experience in Fortune 500 companies for over 13 years. He is one of the principal editors of [Data recovery reviews](#), the premier portal in the data center data storage, network security and data recovery space

[Hide files and folders](#)

Hide files and folders with this folder security software.

[Master Mind In A Box](#)

Automated Mastermind Group For Your Website

[Guide to Search Engine Optimization](#)

Guide to Obtaining a #1 Ranking in the Search Engines

[Online Wealth Training - Build Wealth!](#)

Get out of debt and create multiple streams of income with Abundant Wealth

Protect Your Vital Data with Today's Technology

Internet Security Basics 101

The explosive growth of the Internet has meant that thousands of people are today experiencing the joys of being online for the first time. With growth there always comes pain. Be it your growing pains as a child or the growth and development of this part of our culture called the Internet.

Firstly we need to quickly explain what the Internet is and where it came from. The Internet is the offspring of a military project called Arpanet. Arpanet was designed to provide reliable communication during global nuclear war. A vast network of interconnected computers was set up all over the world to allow the various branches of US and NATO forces to communicate with each other.

Nuclear war never came (thankfully) and the world was left with a massive network of computers all connected together with nothing to do. Colleges and universities started to use these computers for sharing research internationally. From there it grew and spread outside colleges to local homes and businesses. The World Wide Web was born and its father was a guy called Tim Berners Lee.

When you're connected to the Internet you're sharing a vast network with hundreds of millions of other users. This shared network provides resources that 15 years ago were never thought possible. Unfortunately when something is shared its open to abuse. On the Internet this abuse comes from hackers and virus creators. Their sole intent is to cause chaos and/or harm to your computer system and millions of other computer systems all over the world.

How do you combat this? You need an Internet security system. This might sound complicated but your Internet security system will be quite straightforward being comprised of just 2 - 3 Internet security products. We'll look at each of these products in more detail now:

AntiVirus Software

The first and most critical element of your Internet security system is antivirus software. If you don't have up-to-date antivirus software on your PC you're asking for trouble. 300 new viruses appear each month and if you're not constantly protecting your system against this threat your computer will become infected with at least one virus - it's only a matter of time.

Antivirus software scans your PC for signatures of a virus. A virus signature is the unique part of that virus. It can be a file name, how the virus behaves or the size of the virus file itself. Good antivirus software will find viruses that haven't yet infected your PC and eliminate the ones that have.

Antivirus software can only protect your computer from viruses trying to infect it via email, CD-Rom, floppy disk, Word documents or other types of computer files. Antivirus software alone will not keep your computer 100% safe. You also need to use firewall software.

Firewall Software

Protect Your Vital Data with Today's Technology

The use of firewall software by home computer users is a relatively new occurrence. All Internet connections are a two way process. Data must be sent and received by your computer. This data is sent through something called ports. These are not physical things rather aspects of the way your computer communicates online.

Firewall software watches these ports to make sure that only safe communication is happening between your computer and other computers online. If it sees something dangerous happening it blocks that port on your computer to make sure your computer stays safe from the person who is trying to hack into your system.

An easier way to understand a firewall would be to picture your computer as an apartment complex. At the front door of this complex there is a security guard. Every person who enters the complex must pass this security guard. If the security guard recognizes the person entering as a resident he allows them to pass without saying anything. If, however, the person entering the complex is unknown to him then he will stop that person and ask for identification. If they have no business being at the apartment complex he escorts them from the building.

If you are not currently using firewall software your computer will get hacked into - that's a guarantee.

PopUp Blocker

You can get a good popup blocker at no cost. An easy way to do this is to install either the Google or Yahoo toolbar. Both of these come with popup blockers built in. Popups are not necessarily dangerous but are a nuisance and using either of these toolbars will make your life that bit easier.

A simple rule for practicing online security is: "If in doubt then don't". If you don't recognize the file, the email address, the website or if your gut feeling says "no" then don't click that button.

<http://www.affiliate-advocate.com> is run by Niall Roche. The site offers reviews of affiliate marketing ebooks and software as well as advice and tips for new and existing affiliate marketers.

[PCSecurityShield](#)

The Shield Pro 2007 - Antivirus and Firewall Protection

[PID control information from John Shaw](#)

Information for engineers in the industrial control field

[Sales Letter Creator](#)

Software that allows you to quickly and easily create sales letter style websites for maximum profit.

Protect Your Vital Data with Today's Technology

[Amazing Box Covers, eBook Cover Creator](#)

Ebook cover creator tutorial - create ebook covers better than ebook cover generators. 12 FREE ebook cover templates

Protect Your Vital Data with Today's Technology

Internet Security Threats: Who Can Read Your Email?

Before being able to choose a secure Internet communication system, you need to understand the threats to your security.

Since the beginning of the Internet there has been a naive assumption on the part of most email users that the only people who are reading their email are the people they are sending it to. After all, with billions of emails and gigabytes of data moving over the Internet every day, who would be able to find their single email in such a flood of data?

Wake-up and smell the coffee! Our entire economy is now information based, and the majority of that mission critical information is now flowing through the Internet in some form, from emails and email attachments, to corporate FTP transmissions and instant messages.

Human beings, especially those strange creatures with a criminal mind, look for every possible advantage in a dog eat dog world, even if that advantage includes prying into other peoples' mail or even assuming your identity. The privacy of your Internet communications has now become the front line in a struggle for the soul of the Internet.

The New Generation Packet Sniffers:

At the beginning of 2001, most computer security professionals began to become aware of an alarming new threat to Internet security, the proliferation of cheap, easy to use packet sniffer software. Anyone with this new software, a high school education, and network access can easily eavesdrop on email messages and FTP transmissions.

Software packages such as Caspa 3.0 or PassDetect - Ace Password Sniffer automate the task of eavesdropping to the point were if you send an email messages over the Internet with the phrase "Credit Card", it's almost a certainty that someone, somewhere will capture it, attachments and all.

(Caspa 3.0 - from ColaSoft Corporation, located in Chengdu, China <http://www.colasoft.com> ,PassDetect - a product whose advertised purpose is to sniff passwords sent in email, over HTTP, or over FTP from EffeTech Corporation, <http://www.ettetech.com>)

Protect Your Vital Data with Today's Technology

A good example of this new class of software is called MSN Sniffer, also from Effetech, and it highlights the "party line" openness of today's LAN and Internet environments. Just like old telephone party lines, MSN sniffer lets you listen-in on other people's conversations, just like picking up another phone on a party line.

On their web site, Effetech advertises MSN Sniffer as:

"a handy network utility to capture MSN chat on a network. It records MSN conversations automatically. All intercepted messages can be saved as HTML files for later processing and analyzing. It is very easy to make it to work. Just run the MSN Sniffer on any computer on your network, and start to capture. It will record any conversation from any PC on the network."

Just as the Internet has been flooded by a deluge of spam messages after the introduction of cheap, easy-to-use spam generation software, the same effect is now taking place with sniffer software. The major difference is that, unlike spam, Internet eavesdropping is totally invisible, and ten times as deadly. How much of the identity theft being reported today is a direct result of Internet eavesdropping? Its hard to tell, but with the every growing dependency by individuals and corporations on Internet communications, opportunities to "capture" your sensitive data abound.

Most FTP transmission are unencrypted!

As of November 2003, the majority of corporate FTP transmissions are still unencrypted (unencrypted is geek speak for "in the clear") and almost all email communications take place "in the clear". Many email and FTP transmissions travel over 30 or more "hops" to make its way from the sender and receiver. Each one of these hops is a separate network, often owned by a different Internet Service Provider (ISP).

Any Idiot in the Middle

Even a well run corporation must still primarily rely on trusting its employees, contractors and suppliers to respect the privacy of the data flowing over its networks. With the new sniffer technology, all it takes is one "idiot in the middle", and your security is compromised. It could be the admin assistant sitting in the cubical next to you, or a network assistant working for one of the many ISPs your data will travel over, but somewhere, someone is listening. Maybe all he is looking for is his next stock trading idea, or maybe he wants to take over your eBay account so he can sell a nonexistent laptop to some unsuspecting "sucker" using your good name. its all happening right now, at some of the most respected companies in the world.

Protect Your Vital Data with Today's Technology

Access to your network doesn't have to come from a malicious or curious employee-many Internet worms, Trojans and viruses are designed to open up security holes on a PC so that other software can be installed. Once a hacker has access to one computer in your network, or one computer on your ISP's network, he can then use a sniffer to analyze all the traffic on the network.

So I'll password-protect my files, right?

You're getting warmer, but this still isn't going to do the trick. It's a good way to stop packet sniffers from searching for key words in a file, but unfortunately it is not as secure as you might think. If you ever forget a Zip, Word or Excel password, don't worry, just download the password tool from Last Bit Software www.PasswordTools.com, it works very well. There are many other packages out on the Internet but Last Bit's tool is the most robust and easy to use, if a bit slower than some others.

So what can I do about it?

OK, so now that you understand the threat, what can you do about it?

Stop using the Internet? - More than a few professionals are returning to phone calls and faxes for all their important communications.

Complain to your IT department? - If you have an IT department in your company this is a good place to start. But did the spam mail stop when you complained about it to your LAN administrator? Unfortunately he is almost as helpless as you are.

Encrypt your communications with PKI, etc. - For email this is a bit drastic, and can be very expensive, especially since you will need to install a key on each PC and coordinate this with the receivers of your email messages, your IT organization, etc.

Use FileCourier - This is by far the easiest and most cost effective way to protect your email attachments, or replace FTP transmissions. It takes out the "idiot in the middle" with a very clever solution.

The FileCourier approach to Security

I believe that FileCourier is the easiest out-of-the box secure communication system available.

Protect Your Vital Data with Today's Technology

FileCourier approaches Internet data transfer security in a unique way. Until FileCourier was first released in December of 2002, all secure email and file transmission systems relied on encrypting the data during the tried and true method of "upload, store, and forward". When you send an email, it and any documents attached to it are first transmitted to one or more intermediate servers. These mail server store the documents and then attempt to forward it to the receivers email server. To secure the transmission of the email requires either the servers to use extra encryption software technology, or forces the individual sender and receivers to install encryption software and their associated keys, or both. Not only is this a costly and time consuming exercise but it also often fails to protect the data over the complete path of the transmission. What do you do if the receiver is in another company and doesn't have any encryption software installed? What if his company is using a difference encryption standard? Ignoring the complexity of existing secure email and FTP systems their biggest failings continue to be the "idiot in the middle". From a nosey email or FTP server administrator, to a hungry co-worker, to an incompetent who lets a hacker have free reign of their server, if your sensitive documents are stored on a server maintained by someone else then that person, or his company, can view your documents.

The FileCourier approach is creative, yet simple. FileCourier utilizes existing email and instant messaging systems in the same way you use an envelope to send a letter thru the US postal service, as a wrapper for the real content. We assume that EVERYONE can read what is in the email, so we don't send your documents in the email at all. In fact your documents never leave your PC, until the receiver of the email requests it.

How it works:

FileCourier lets you ticket the file you want to email, and then instead of sending the file in the email, sends a "FileTicket" instead. The file is only transmitted to the receiver of the email when he opens the FileTicket and is "authenticated". After the receiver is authenticated the file is transmitted through an SSL (secure socket layer) tunnel directly from the sender's PC to the receiver's PC through our secure relay servers. SSL is the same security used by banks and is impossible for packet sniffers to penetrate. With FileCourier each packet is encrypted using a 1024 bit key and is delivered to your receiver through his browser. FileCourier lets your communications go un-detected by any sniffer, and removes the "idiot in the middle" threat by never storing the data on an intermediate server. More over, FileCourier is the easiest way to secure your sensitive data transmission in both an Internet and corporate LAN environment.

Take Action Now!

Internet communications security is one of the most important privacy issues we face today. It might feel a bit paranoid for a law-abiding citizen to encrypt his email communications and computer document transmissions, but would you send a customers contract thru normal mail without an envelope? How would you feel if your employer sent your next pay stub to you on the back of a

Protect Your Vital Data with Today's Technology

postcard? Use FileCourier, just like you would use an envelope for regular mail. Download the no obligation free trial today at www.filecourier.com and send 50MB of data securely for free!

Mark Brooks is a software architect, internet entrepreneur and founder of CanDo Networks Corporation. CanDo Networks Corporation makes easy-to-use software for communicating large amounts of data securely and privately over the Internet. Its flagship product, FileCourier (www.filecourier.com), is used by thousands of legal, medical, and computer professionals to securely deliver files over the internet, to anyone, anywhere

mark@candonet.com

[Autoresponder Profits](#)

The Complete Guide To Setting Up And Running A Profitable Ezine

[1001 Killer eBay Marketing Tactics](#)

Make money on ebay. 1001 Killer eBay Tactics explains exactly how to make money on ebay and other inte

[Cash From Scratch Videos](#)

You read the book. Now watch the videos. The perfect upsell or backend product!

Protect Your Vital Data with Today's Technology

Internet Security to Protect Small to Medium Businesses

Internet Security to Protect Small to Medium Businesses

Internet security threats come in different shapes and sizes. There are viruses, spywares and hackers ready to attack your computer. Most often than not, small and medium businesses do not usually think that they are vulnerable to security attacks. They always assume that bigger companies are the likelier ones to become victims. But they are hugely mistaken.

Every business is vulnerable to these threats and attacks. But since most of these small and medium companies wrongly assume that they are safe, it is usually the case that they do not have any basic measures to protect their networks and computers.

Because of such risky confidence, their systems are not sufficiently protected from worms, viruses, trojans, hackers, data theft and other threats. Moreover, entrepreneurs in these types of businesses have so much in mind and are often busy such that security is last in their priorities.

In order for these businesses to wake up and smell reality, the following are some reasons why Internet security is important: 1. At present, viruses, spyware and other malicious programs are much more complex and sophisticated. They spread fast in the Internet and are more difficult to remove. Businesses need to install their systems with up to date patches for their virus protection, and other security programs to avoid becoming vulnerable to such malicious attacks. 2. Hackers have tools to browse the Internet that could look for unsecured systems and computers they can hack and attack. With just a single computer connected in a network, a hacker can access and control a business network. 3. Digital attackers have more difficulties penetrating the bolstered and highly secured systems of bigger companies and enterprises. Because of this, they focus their attention more in targeting smaller businesses. 4. Intentional or unintentional security threats usually come from people working within the business. Simple downloads such as music; videos can have spyware or viruses attached to them. To be able to control these, installed firewalls, spyware software and anti-virus software should be installed. 5. Attacks on businesses can be overwhelming in terms of loss of sales or income. This can also affect companies' reputations should their websites and systems become unreliable due to these Internet assaults. It is a good thing, however, that there are ways for businesses to protect their computers and networks from security risks. These are the following:

- The first step is for businesses to change their way of thinking. They should consider Internet security as their partner and an essential way for them to survive while conducting business in the World Wide Web.
- Businesses should determine what they need to bulk their security. To be able to do this, an inventory of what they have is in order.
- The basic protection business computers should have are the following: anti-spyware, anti-virus software and firewalls. These three can safeguard businesses against spamming, identity theft, phishing and other scams.
- If businesses have difficulties protecting themselves, then they can let others handle the job by either outsourcing or enrolling under service providers who could design, provide and maintain internet security in their business computers and network.
- Since, new viruses, worms, trojans and spywares are developed everyday, it is vital that security software installed in the business computers are updated regularly.

Protect Your Vital Data with Today's Technology

It is fortunate, however, that most security measures can be automatically updated. - In order for employees to comply and to avoid confusion, businesses should document all the Internet security plans and include in this the policies and regulations that should govern the actions of employees regarding this matter. - Wireless networks are more susceptible to security attacks because of the open transmission medium which makes data transmissions more vulnerable. This is the reason why more stringent protection measures should be employed. - Computers and systems are more difficult to use if there are so many security checks and scans that occur every time. It is therefore vital that businesses consider the balance between usability and security.

Installing security measures in business computers and systems and maintaining them might be tedious at first. But, the rewards of Internet security assure the survival of a business and its ability to thrive and grow in the World Wide Web.

Rebecca Hubbard

Hubbard Enterprises

www.eBooksProfit4u.com

www.ThePowerof10.ws

www.Christmas-In-A-Box.ws

www.Rags-To-Riches.ws

www.Profits4u.ws

www.HubbardEnterprises.ws

www.Profitsnmore.com

www.RU4Real.ws

www.GoogleCash4u.ws

www.eBooksMore.ws

About the author:

None

Protect Your Vital Data with Today's Technology

[Wholesale Ad Secrets! Instant Profits!](#)

Premium Classified Ad space for \$0.99 to rarely more than \$3.99. Big Savings on Thifty Nickel/Penny Saver. Magazines Too!

[Attorney Prepared Credit Report Repair](#)

Legal and Easy Ways to Repair Your Credit Report, Save Money, Avoid Scams, and More

[Cb Affiliate Reward.](#)

Motivate Your Affiliates With Extra Rewards.

Protect Your Vital Data with Today's Technology

Internet Security: Backups

A vital part of any security scheme is backup. No matter how tight your security is, you always have the chance that a virus or hacker or even your 5 year old kid is going to slip through your defenses and damage your system and your vital data files. If you don't back up your data regularly you will be out of luck. And anyone who has been there knows how horrible it is to realize that your computer is destroyed and there is no way to get the files back.

In order to back up your system, you will need a backup device. Some people use Zip or Jazz drives, others use tape drives, write able CD drives, or other removable cartridge systems. I know it sounds expensive, but compared with the cost of losing your valuable data forever, each of these is cheap.

I've found that the best all-around product for backup is Backup Exec. This product requires a tape drive, as do most other third-party backup solutions. Backup Exec is preferred because it can be made totally automatic and is one of the top-rated products industry-wide. If you want to back up to other media, though, you'll do best to stick with the backup software that comes with the media.

An important fact that I've noticed about backup is that you have to make it a part of your normal routine. Even if you have automated backups set up and working perfectly, you must check them constantly. If you don't you will find yourself without a backup when you need it most! My advice is to try restoring files from your backup occasionally when you don't need it so you are ready and are sure you have good backups when you do need them.

Be careful when choosing backup mediums for longer range storage. There is nothing more frustrating then to need a backup, go to it and find that the file that you need cannot be retrieved because the media is corrupt! For critical data I usually make sure I have backups on several different media (perhaps tape and zip disk), and for the really important stuff I tend to rotate through half a dozen different medias. I mean, think about it, is the data for your entire company worth a few dollars for some hardware and media? Don't risk all of your years of hard work trying to save a few dollars on media.

Backup Disaster - A True Story

Not having a good backup can be a disaster of epic proportions. In one instance I've seen the lack of a backup turn a situation which was uncomfortable into a complete disaster.

Protect Your Vital Data with Today's Technology

I knew a guy who was working on an older Macintosh computer. Our entire company switched to PCs except for him, because he didn't have the time. The Macintosh was old and unbeknownst to anyone it had been outfitted with an old RAID drive (mirrored) from a manufacturer that no longer existed.

This guy believed he was doing backups every day. Someone showed him how to do it and he followed those instructions to the letter, even to the point of ignoring the error that it produced each and every time it ran. That was actually in the instructions.

One day his hard disk started making strange sounds so he called us. We tried to boot it up but no go. We asked him if he was doing backups and he handed us his zip disks, which were blank! He had been faithfully doing backups for over two years, and not one of them worked.

We had to send the disk out to a disk repair shop, and they managed to recover about 20% of the data at a cost of over \$6,000! It took the poor guy almost six months with two temps to get all of the data hand-typed back into the computer!

ABOUT THE AUTHOR

Richard Lowe Jr. is the webmaster of Internet Tips And Secrets. This website includes over 1,000 free articles to improve your internet profits, enjoyment and knowledge.

Web Site Address: <http://www.internet-tips.net>

Weekly newsletter: <http://www.internet-tips.net/joinlist.htm>

Daily Tips: <mailto:internet-tips@GetResponse.com>

[Dating A Woman - How To Attract Women!](#)

Learn How To Date Beautiful Women!

[eBookForms](#)

Self-Incorporate, Financial Plan, Will & Trusts-All forms are Faxable, Printable & Interactive. Download Instantly!

[Adam Spencer's Maths Math Revision eBook](#)

Maths, math revision study e-Book from the young child prodigy Adam Spencer, A grade age 9! Affiliates Earn 50%

Protect Your Vital Data with Today's Technology

Online Security – Your Responsibilities as a Consumer

As a consumer, there are certain responsibilities that are inherent to online security. While some may find this hard to believe, there are actual steps you must take while shopping online to insure and protect your personal information.

Is the site secure? Most e-businesses offer secure areas for payment processing. However, there are still some holdouts out there who haven't implemented that feature on their website. If your browser doesn't display a locked padlock icon at the bottom of your screen, then the site isn't secure. You can set your browser to notify you before entering a secure area, to make sure that the information you are about to send is encrypted and secure.

Does the site's privacy policy protect your information? On the other hand, does the site even have a privacy policy? If you want to make sure that your information is not sold to the highest bidder, you need to read a website's privacy policy before making a purchase. You will need to make sure that it is clear and informs you of exactly what the site plans to do with your information. If you don't feel comfortable with their policy, find another store. Keep in mind that even reputable companies will share your information, unless they specifically state or ask you if you prefer to keep your information private.

Email is not for credit card numbers. One of the biggest mistakes consumers make is trusting that their email containing valuable credit card information is secure. Unless you are using an encryption key, and the person receiving your email is as well, anyone with the proper knowledge could hack into that email and steal your information. Only submit credit card information or passwords through a secure site.

Be on the lookout for copycats. A common problem right now is the copycatting of popular sites, such as Paypal, Earthlink, and other Internet providers. You might receive an official looking email asking you to update your password, or your billing information. Just because it looks official doesn't mean that it is. Check with the provider in question before changing anything. Emailed links can appear to be the real thing, but the actual web address that you are sent to will be anything but. Most providers clearly state that they will not ask you for your password or billing information via email. It is much better to be safe than sorry by falling for a carefully laid out copycat trick.

Is it really SPAM? Nearly everyone on the Internet has had at least one complaint about the amount of SPAM they receive. In fact, odds are that every day you grumble about it. Before you hit delete, or report an email as SPAM, double check to make sure that it is not an honest company, or a company you've done business with in the past. Many reputable retailers are being lumped in with the bad guys by overzealous SPAM haters. If you have visited the site or ordered from them before, and they previously mentioned sending emails to you in the past, think twice before reporting them as SPAM.

Ok, it is SPAM and I'm sick of it! If you zealously guard your email address and you are still getting abundant SPAM, there are steps you can take to prevent this in the future. Before giving personal information to a company, make sure they clearly state how they plan to use your information. If you belong to a message board, or similar service, your email address may be being "plucked" by a SPAM'ers software. If you do need to input an email address and you not 100% sure, it is a good idea to set up an email account with a free provider to make sure that your main email account isn't getting drowned with SPAM.

It is possible to have a safe time shopping on the Internet. You will just need to be aware of your

Protect Your Vital Data with Today's Technology

responsibilities and take an active role in guarding your information.

About The Author

Julie Martin is the publisher of "The Iscaweb eZine" a weekly eZine dedicated to increasing your online profits, no matter what you are selling. Julie also uses the "Plug-In-Profit" system to GREAT effect!

To subscribe to the eZine, or to learn more about the Plug-In-Profit system visit:

<http://www.iscaweb.com>

[PageRank Maximizer](#)

Boost Your PageRank Sky-High and Dramatically Increase Your Business!

[Mighty Coach](#)

High quality online video training

[Mega Website Traffic Guaranteed](#)

Unique formula will skyrocket your website's traffic as much as you want with just 1 click.

Protect Your Vital Data with Today's Technology

Protect Your Vital Data with Today's Technology

Stay Up to Date to Avoid Disaster

New viruses, spyware and adware are developed every day. Too often, we never even know we're vulnerable until it's too late. Keep your security device up to date to avoid disaster. Stay prepared with the resources available at <http://www.securitydeviceonline.com>, and you'll never be caught off guard.

Protect Your Vital Data with Today's Technology

Disclaimer

Disclaimer - Legal Notice:

While all attempts have been made to verify information provided in this publication, neither the Author nor the Publisher assumes any responsibility for errors, omissions, or contrary interpretation of the subject matter herein.

This publication is not intended for use as a source of legal or accounting advice. The Publisher wants to stress that the information contained herein may be subject to varying state and/or local laws or regulations. All users are advised to retain competent counsel to determine what state and/or local laws or regulations may apply to the user's particular business.

The Reader of this publication assumes responsibility for the use of these materials and information. Adherence to all applicable laws and regulations, federal, state, and local, governing professional licensing, business practices, advertising, and all other aspects of doing business in the United States or any other jurisdiction is the sole responsibility of the Reader. The Author and Publisher assume no responsibility or liability whatsoever on the behalf of any Reader of these materials.

Any perceived slights of specific people or organizations are unintentional.