

# Learn How to Protect Yourself in the Cyber World

Tips from: © 2000 - 2005 Business Software Alliance

All computer users should have a basic understanding of how to protect themselves from the possible risks that may spoil their online experience. The Internet permits anonymity among users and online anonymity can be used to disguise illegal behavior. Our Cyber Safety Glossary provides useful information to educate you about illegal, fraudulent schemes and how to avoid them. Computer users are by no means defenseless. In addition to the wide array of anti-virus, anti-spyware, firewall and other security programs and technologies available, a user's most important protection is his or her own awareness.

We hope that this valuable resource will help be your guide to a safe and legal online experience.

## 419 Fraud

### Also Known As:

The Nigerian Scam, Advance Fee Fraud, Four-One-Nine (after the relevant section of the Criminal Code of Nigeria), and The Nigerian Connection.

### Description:

419 Fraud involves an unsolicited email message, purportedly from Nigeria or another African nation, in which the sender dangles the promise of a huge sum of money to the email recipient. To earn this money, the recipient is asked to pay an advance fee or provide identity, credit card or bank account information. There are uncounted variations on these tales from crude oil and other commodity deals to unclaimed bequests.

### How to Recognize This Threat:

Unsolicited email messages from a stranger who promises great wealth - a "get-rich" scheme.

### What Should I Do:

Do not respond. Never send a check or reveal identity, credit card, or bank account numbers. If you are so inclined, forward the message to the United States Secret Service 419.fcd@usss.treas.gov. U.S. citizens and residents who have responded to this scam and have consequently suffered a financial loss are instructed to telephone the nearest Field Office of the United States Secret Service (USSS).

### » Nigerian scam example 1

From: nelson donell [mailto:nelsondonell@universia.net.co]  
Sent: Wednesday, July 13, 2005 5:25 AM  
Subject: URGENT REPLY NEEDED

Dear Friend,

I am Barrister Nelson Donell , the Personal Attorney to a Foreign Contractor, who worked with a Multinational Oil Firm in Nigeria. On the 11th of September 2001, my client, a Mexican National, late Engineer Carlos Montoya, an oil Merchant Contractor with the Federal Government of Nigeria, until his death some years ago in a ghastly terrorist attack to American Airlines Flight 11, from Boston, Massachusetts, to Los Angeles, California, crashed into the North Tower of the World Trade Centre with 86 people on board. All occupants of the Aeroplane unfortunately lost their lives. Since then I have made several inquiries to Several Embassies to locate any of my clients extended relatives, this has also proved unsuccessful.

After these several unsuccessful attempts, I decided to trace his relatives over the Internet, to locate any member of his family but of no avail, I have contacted you to assist me in repatriating the money left behind by my client before they get confiscated or declared unserviceable by the Bank where this huge deposits were lodged. Particularly, the Bank where the deceased had an account valued at about US\$9.Million has issued me a notice to provide the next of kin or have the account confiscated within the next twenty official working days.

Since I have been unsuccessful in locating the relatives for some years now I seek your consent to present you as the next of kin to the deceased so that the proceeds of this account valued at US\$9.Million can be paid to you and then you and I can share this money. 70% to me and 25% to you, while 5% should be for expenses or tax as your Government may require. All I require is your honest and co-operation to enable us see this deal through. I guarantee that this will be executed under a legitimate arrangement that will protect you from any branch of the law. Please get in touch with me via email as soon as you get this mail to enable us discuss on the modalities and process for success of this transaction.

I will equally want you to send the following information to enable me move ahead for the transfer in your name.

- 1, Your Full Name
- 2, Your contact address
3. Your private fax and telephone number.
- 4, The name and address of bank you wish we will use to receive the fund successfully. 5, The account information for urgent transfer.

Do reply to my private email: {nelson\_donell@yahoo.fr } I await your kind response, Good day and God bless.

Regards,  
Barrister Nelson Donell.

#### » Nigerian scam example 2

From: tnjoku@mailbg.com  
Sent: Monday, July 18, 2005 5:51 PM  
To: tnjoku@mailbg.com  
Subject: REPLY AS SOON AS POSSIBL

GOOD DAY,  
I AM DR.TONY NJOKU A DIRECTOR OF THE CONTRACT AWARD/REVIEWDEPARTMENT WITH THE NIGERIA NATIONAL PETROLEUM CORPORATION(NNPC).I AMCONTACTING YOU ON THIS BUSSINESS OF TRANSFERING THE SUM OF US\$30 MILLION(STATE DOLLARS ONLY).

INTO A SAFE FOREIGN ACCOUNT AND THE NEED IS VERY URGENT .I GOT YOURCONTACT FROM A RELIABLE SOURCE AND IT IS WITH BUSSINESS TRUST THAT MADE ME TO CONTACT YOU ON THIS MATTER.I WRITE TO SOLICIT FOR THE TRANFER OF THIS FUND INTO YOUR ACCOUNT.THIS MONEY WAS GENERATED FROM AN OVER INVOICED CONTRACT FUND IN MY CORPORATION(NNPC). I AM CONTACTING YOU FOR YOUR HELP AND PARTNERSHIP FOR THE FOLLOWING TWO REASONS AND ALSO ON BEHALF OF MY TWO OTHER COLLEAGUES.

1.AS A CIVIL SERVANT I AM NOT PERMITTED TO OWN FOREIGN ACCOUNT DUE TO CIVIL SERVICE CODE OF CONDUCT.

2.MY PRESENT FINANCIAL RESOURCES AS A CIVIL SERVANT IS NOT SUFFICIENT FOR ME TO HANDLE THE TRANFER ALONE SUCESSFULLY WITHOUT FINANCIAL ASSISTANTFROM A RELIABLE FOREIGN PARTNER ABOARD.25% OF THIS SUM WILL BE FOR YOU ASCOMPENSATION FOR USING YOUR BANK ACCOUNT IN TRANSFERING THIS MONEY.5% WOULD BE USE TORE-IMBURSE EXPENSES MADE BY BOTH PARTIES DURING THE PROCESSING OF THE TRANFER WHICH INCLUDED TELEPHONE BILLS,TRAVELLING EXPENSES AND FEES .

WHILE 70% IS FOR ME AND MY COLLEAGUES.PLEASE NOTE THAT I WILL ARRANGE TO MEET WITH YOU IMMEDIATELY AFTER THE SUCCESSFUL CONCLUSION OF THE TRANSFER.THE 70%SHARES OF OURS WILL BE USED FOR INVESTMENT OVERSEAS.YOUR ASSISTANCE AND COOPERATION IS HIGHLY NEEDED.I ASSURE YOU THAT THIS TRANSACTION IS 100% RISK FREE.

IF YOU ARE INTERESTED I WILL REQUIRE YOUR BANKING INFORMATION AS MENTIONED BELOW.

1.NAME TO BE USE AS BENEFICIARY AND ADDRESS.

2.YOUR PRIVATE AND CONFIDENTIAL TELEPHONE/FAX NUMBER(S)

3.YOUR BANK NAME AND ADDRESS,YOUR BANK TELEPHONE AND FAX NUMBER(S)

4.OR IF YOU ARE NOT COMFORTABLE WITH PROVIDING YOUR EXISTING ACCOUNT,YOU CAN WITHIN THE SHORTEST POSSIBLE ME,CONFIDENTIALLY

OPEN AN ENTIRE NEW(VIRGIN)ACCONT FOR THE TRANSACTION.I WOULD PREFER THIS ARRANGEMENT. I HOPE TO CONCLUDE THIS BUSINESS WITHIN THE NEXT FOURTEEN (14)WORKING DAYS. LOOKING FORWARD TO YOUR ANTICIPATED AND URGENT POSITIVE RESPONSE.

BEST REGARDS,

DR.TONY NJOKU.

## **Adware**

### **Also Known As:**

Advertising-supported software.

### **Description:**

Adware is any computer program or software in which advertisements are displayed while the program is running. Adware is sometimes used to help recover programming development costs or reduce the price of the software application. See Spyware in the BSA CyberSafety Encyclopedia.

### **How to Recognize This Threat:**

An abundance of pop-up and banner ads and/or system slowdown.

### **What Should I Do:**

To prevent malicious Adware, install anti-Spyware software and a firewall.

## **Cookies**

### **Also Known As:**

Session Cookie, Persistent Cookie.

### **Description:**

Cookies are files stored on a user's computer that identify a PC to a Web server. A Web page that welcomes a visitor by name does so through the use of cookies. Cookies typically authenticate or identify a registered visitor of a Web site or are part of a login process. Other uses are maintaining a shopping basket of products selected for purchase during a session at a site and personalization of a site. Cookies can contain personal information that was freely given to a site as part of the user's site registration. Users rely on the organization behind the Web site to keep this information from being compromised.

### **How to Recognize This Threat:**

Personalized Web pages indicate the cookie function is turned on.

### **What Should I Do:**

Many people like the convenience of cookies and leave the function enabled. Others feel

uncomfortable storing cookie information permanently. Internet browsers allow users to disable or set cookie preferences.

## Malware

### **Also Known As:**

Malicious Software, Virus, Worm, Trojan Horse, Spyware.

### **Description:**

Any software programs developed for the purpose of doing harm to a computer system or create mischief. The most common are Viruses, Worms, and Spyware.

### **How to Recognize This Threat:**

Any unsolicited correspondence from an unknown source is a potential carrier and should be considered suspect. Be wary of executable (.exe) file extensions, even if sent by an acquaintance. Software download and file sharing sites that are not trusted may harbor Malware.

### **What Should I Do:**

It is recommended for every computer user to have anti-virus software loaded on their computer. Furthermore, the anti-virus software should have the capability of being automatically updated, to ensure it protects against the latest threats. It should also automatically scan incoming and outgoing email. On a regular basis - at least weekly - the anti-virus software should automatically scan every file on the computer. You should also have anti-Spyware software installed on the computer and have firewall protection. Avoid opening suspicious .exe files that arrives via email.

## Pharming

### **Also Known As:**

Spoofing, DNS Cache Poisoning.

### **Description:**

Pharming (pronounced "farming") is a technically sophisticated scam designed to trick individuals into disclosing sensitive information such as bank account, credit card, and Social Security numbers. It is similar to Phishing (see Phishing), but Pharming poses risks even if you do not click a link within the email. Pharming uses malware or spyware to re-direct users from real web sites to fraudulent sites (typically through Domain Name System hijacking), even if the user enters a legitimate web address.

### **How to Recognize This Threat:**

Pharming relies on scare tactics. If a message implies that immediate action is needed to update sensitive financial and identity information, it must be considered suspect.

### **What Should I Do:**

The malware-based method of Pharming is stopped by maintaining up-to-date anti-virus and anti-Spyware programs on your computer as well as by having a firewall. These precautions will reduce the likelihood that a virus will redirect you to a scammer's Web site. Look for the lock or key icon at the bottom of the browser when entering a site that purports to be secure. If the site has changed since your last visit, be cautious. If you are concerned, give the organization a call and explain the situation.

## Phishing

### **Also Known As:**

Brand spoofing, Carding.

### **Description:**

Phishing refers to the process of imitating legitimate companies in emails or creating fake Web sites designed to look like a legitimate Web site in order to entice users to share their passwords, credit card numbers, and other personal information. The perpetrator then uses the information to steal the target's identity or to sell that identity to others. Users need to be educated not to give away personal information in response to an unsolicited email.

One of the newest Phishing schemes is to send a fraudulent text message to a cell phone user. The concept is the same; someone is trying to obtain sensitive information.

### **How to Recognize This Threat:**

Official looking and sounding messages that urge immediate action to update sensitive financial and identity information.

### **What Should I Do:**

Avoid clicking on a link within the text of a suspect email. Avoid responding to a cell phone text message that urges immediate action or requests you to update sensitive personal information. Delete the message immediately from the Inbox, the Trash box, and/or from your cell phone. If you are concerned that the message may be real, then open your Web browser and type in the URL of the site that you wish to visit. If you have up-to-date anti-virus software, which helps guard against Pharming (see Pharming), this procedure should take you to the legitimate site. You can also call the company customer service department, using a telephone number on a bill or other paper-based documentation from that company. There are also mutual authentication technologies available that allow you to verify that the sender is legitimate and trusted.

## National Credit Union Administration

[Share Insurance](#) | [Resources for Credit Unions](#) | [Resources for Consumers](#) | [News](#) | [Search](#)

	<p><b>Account Info Verification</b> Dear FCU holder account,</p> <p>As part of our security measures, we regularly screen activity in Federal Credit Unions (FCU) network.</p> <p>We recently noticed the following issue on your account: A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID Number: PP-065-617-349</p> <p>For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause. Please log in to your FCU account to restore your access as soon as possible.</p> <p>You must <b>click the link below</b> and fill in the form on the following page to complete the verification process.</p> <p><a href="#">Click here to update your account</a></p> <p>In accordance with NCUA User Agreement, your account access will remain limited until the issue has been resolved. Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure. We encourage you to log in to your FCU account as soon as possible to help avoid this. We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account.</p> <p>We apologize for any inconvenience.</p> <p>Sincerely, NCUA Account Review Department</p> <hr/> <p>Please do not reply to this e-mail. Mail sent to this address cannot be answered.</p>	<p><b>About NCUA</b></p> <p>The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions. NCUA, backed of the full faith and credit of the U.S. government, operates the National Credit Union Share Insurance Fund (NCUSIF) insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions. During the 1990s and into the 21st century, credit unions have been healthy and growing. Credit union failures remain low and the Share Insurance Fund maintains a healthy equity level. The National Credit Union Administration (NCUA) is comitted to maintain a safe environment for over 80 million account holders in all federal credit unions and many state-chartered credit unions. Protecting the security of holders account and of the Federal Credit Unions (FCU) network is our primary concern.</p>
--	--	---

» **Phishing scam example 2**

From: PayPal [security@paypal.com]  
Sent: Tuesday, September 27, 2005 7:17 PM  
Subject: New Security Measures



Dear PayPal customer,

We are currently performing regular maintenance of our security measures. Your account has been randomly selected for this maintenance, and you will now be taken through a series of identity verification pages.

Protecting the security of your PayPal account is our primary concern, and we apologize for any inconvenience this may cause.

You are receiving this message as a result of our regular accounts verification process. Because we had some problems with our data base, we now need to check identity of our all customers. This account verification process will increase security of our customers account.

In order to verify your identity, we ernestly ask you to visit the following link and to confirm your PayPal account information.

[Click here to confirm your account records](#)

Thank you for using PayPal Services.

Copyright © 1999-2005 PayPal. All rights reserved.

## **Software Piracy**

**Also Known As:**

Unlicensed software use, Pirated software, Ripped software, Counterfeit software, Warez.

**Description:**

The illegal use and/or distribution of software protected under intellectual property laws. Software piracy may take many forms:

- **End-user piracy** occurs when an individual or organization reproduces and/or uses unlicensed copies of software for its operations.
- **Client-server overuse** occurs when the number of users connected to or accessing one server exceed the total number defined in the license agreement.
- **Counterfeiting** is the illegal duplication of software with the intent of directly imitating the copyrighted product.

- **Hard-disk loading** occurs when a computer hardware reseller loads unauthorized copies of software onto the machines it sells.
- **Online software theft** occurs when individuals download unauthorized copies of software from the Internet.
- **License misuse** occurs when software is distributed in channels outside those allowed by the license, or used in ways restricted by the license.

**How to Recognize This Threat:**

Pirated software is often peddled through spam email messages, bogus Web sites, auction sites, and storefront operations. Spam messages that offer computer software at unbelievably low prices are suspect. Compilations of software titles from different manufacturers, or software labeled "backup" copies, are a clear indication that the software is not legitimate. When the pirated software does not run properly, causes compatibility issues, and has no technical support or update capabilities, purchasers find to their dismay they have thrown their money down the drain.

File Transfer Protocol (FTP) is the standard computer language that allows computers to exchange files quickly and easily, including the uploading and downloading of software programs. FTP sites can contain enormous quantities of program files, along with other information. When exploited by software pirates, FTP sites facilitate the distribution of large volumes of copyrighted software programs.

Peer-to-Peer (P2P) technology allows users to locate, share, and distribute information between workstations without connecting to a central server. Although P2P has many legitimate uses, it has been subject to abuse among pirates to become one of the more popular online methods used to share copyrighted materials illegally.

**What Should I Do:**

Purchase computer software from authorized dealers. If the online dealer seeking to sell you software isn't listed on that software manufacturer's Web site, then beware. Do your homework. Look for a feedback section on the site and look for comments on the seller based on previous transactions. Get the seller's address. That way, you can check the merchant's record with the Better Business Bureau (BBB) [www.bbb.org](http://www.bbb.org). If you can't find a physical address, then be suspicious. Look for a trust mark from a reputable organization like the BBB. Keep receipts. Print a copy of your order number and sales confirmation and keep them. If a computer software deal looks too good to be true, it usually is.

Never download copyrighted material. This is against international law. Anyone participating is liable and can be charged in criminal and civil proceedings.

» **Software Piracy and Fraud example 1**



» **Software Piracy and Fraud example 2**

Subject: I got XP and Office XP cheap.  
 Importance: High we got everything you need:

Bundle Special #1:  
 Windows XP

Professional Microsoft Office XP Professional = only \$80

Bundle Special #2:  
 Adobe - Photoshop 7, Premiere 7, Illustrator 10 = only \$120

Bundle Special #3: Macromedia  
 Dreamweaver MX 2004 + Flash MX 2004 = only \$100

Bundle Special #4:  
 Adobe Photoshop  
 CS + Adobe Illustrator CS + Adobe InDesign  
 Windows XP Professional With SP2 Full Version  
 Office XP Professional Office 2003 Professional (1 CD Edition) Office 2000 Premium Edition (2CD) Office 97 SR2

Windows 2003 Server  
Windows 2000 Workstation  
Windows 2000 Server  
Windows 2000 Advanced Server  
Windows 2000 Datacenter  
Windows NT 4.0  
Windows Millenium  
Windows 98 Second Edition  
Windows 95  
Office XP Professional  
Office 2000  
Office 97  
MS Plus  
MS SQL Server 2000 Enterprise Edition  
MS Visual Studio .NET Architect Edition  
MS Encarta Encyclopedia Delux 2004  
MS Project 2003 Professional  
MS Money 2004  
MS Streets and Trips 2004  
MS Works 7  
MS Picture It Premium 9  
MS Exchange 2003 Enterprise Server  
Adobe Photoshop  
Adobe PageMaker  
Adobe Illustrator  
Adobe Acrobat 6 Professional  
Adobe Premiere  
Macromedia Dreamwaver MX 2004  
Macromedia Flash MX 2004  
Macromedia Fireworks MX 2004  
Macromedia Freehand MX 11  
Corel Draw Graphics Suite 12  
Corel Draw Graphics Suite 11  
Corel Photo Painter 8  
Corel Word Perfect Office 2002  
Norton System Works 2003  
Borland Delphi 7 Enterprise Edition  
Quark Xpress 6 Passport Multilanguage

You need to save some money somewhere. Let it be here!  
Stop mailing now.

## Spam

### **Also Known As:**

Junk email, Unsolicited email.

### **Description:**

Spam is unsolicited email, advertising products or services. Spam is equivalent to junk mail and spammers have developed many ways of obtaining email addresses. Addresses are sold to spammers by unscrupulous Web sites. Spammers also use automated programs to troll the Web and collect valid email addresses. The term "Spam" is widely believed to be borrowed from the Monty Python Spam song, because like the phrases in the song, computer spam just keeps coming - "spam spam spam egg and spam; spam spam spam spam spam spam baked beans spam spam spam..."

### **How to Recognize This Threat:**

Unsolicited product or service advertisements that are sent via email.

### **What Should I Do:**

Be judicious in giving out your email address. Many people have two email addresses, one for family and friends and the other for general use. Never request to be removed from a Spammer's list. This

simply tells the Spammer that your email address is valid and therefore worth selling to other Spammers. Never click on anything in a spam email. Delete the entire message. Most Internet service and email services offer Spam filters. Make sure to enable the filters. There are a host of Spam software programs available both for purchase and free download.

## Spim

### Also Known As:

Instant spam, IM marketing, spIM.

### Description:

Spim is the same thing as Spam - unsolicited advertisements - only Spim appears through instant messaging programs instead of email. Spim messages are simulations that appear to be from someone online. They are automated messages that urge the person receiving the message to visit a Web site. These systems use special software programs to troll the Internet looking for instant messaging screen names, which are then added to the "spimmer's" contact list.

### How to Recognize This Threat:

Unsolicited product or service advertisements that appear as instant messages.

### What Should I Do:

Blocking incoming messages from unknown senders is one way to prevent Spim. There are also a growing number of software programs available that help to filter out Spim messages.

## Spoofing

### Also Known As:

Pharming, Phishing.

### Description:

Spoofing is when a person pretends to be a business or organization in order to gain access to a computer user's sensitive information such as bank account, credit card, and Social Security numbers. Spoofing scams generally arrive via email, appear to be authentic and urge immediate action to update personal information.

### How to Recognize This Threat:

Official looking and sounding messages that urge immediate action to update sensitive financial and identity information.

### What Should I Do:

Maintain up-to-date anti-virus and anti-Spyware programs on your computer as well as having a firewall. Look for the lock or key icon at the bottom of the browser when entering a site that purports to be secure. **Never click on a link within the text of a suspect email.** There are also mutual authentication technologies available that allow you to verify that the sender is legitimate and trusted.

## Spyware

### Also Known As:

Malware, Pestware.

**Description:**

Spyware gathers information without the knowledge or permission of the computer user. While Spyware often gathers information for advertising purposes, these hidden programs can do much more. They can obtain credit card numbers, passwords, and email addresses. These programs can also monitor a user's Web activity, scan files, create pop-up ads, log keystrokes, or change the default page on the Web browser. Spyware finds its way onto computers as programs covertly bundled with downloaded software, through Peer-to-Peer (P2P) file sharing, or as a result of Internet browsing.

**How to Recognize This Threat:**

Computer system slowdowns and crashes can be signs of Spyware. Differences in your Web browser such as extra toolbars or different homepage settings as well as changes to your security settings or favorites list are indications of Spyware infection. Pop-up ads unrelated to the particular Web site you are visiting are another symptom.

**What Should I Do:**

Install anti-Spyware software and a firewall.

## Trojan Horses

**Also Known As:**

Malware, Virus.

**Description:**

A Trojan Horse appears to be a useful, legitimate file or software program, but once installed, it can cause havoc with a computer by damaging or deleting files. Just as the Trojan people were deceived into accepting the Greeks' gift of a monumental horse, users are often tricked into accepting the Trojan Horse software. One Trojan Horse scam claims that its program will rid the computer of viruses; another might claim to have pornographic images. The unsuspecting user opens the file or downloads the software and the damage is done. Unlike Viruses and Worms, a Trojan Horse is not designed to replicate itself. Some Trojan Horse programs open a backdoor into the computer, allowing unscrupulous individuals to steal sensitive financial and identity information.

**How to Recognize This Threat:**

If a file or an offer to download a software program looks "too good to be true," it just might be a Trojan Horse. Unsolicited messages with an executable (.exe) file or zipped (.zip) attachment can also include a Trojan Horse.

**What Should I Do:**

Avoid opening an executable file (.exe) sent via email. It is recommended for every computer user to have anti-virus software loaded on their computer. Furthermore, the anti-virus software should have the capability of being automatically updated to ensure it protects against new Trojan Horses. It should also automatically scan incoming and outgoing email. On a regular basis - at least weekly - the anti-virus software should automatically scan every file on the computer. Users should also have firewall protection. Make sure the latest updates of the computer's operating system are installed.

## Viruses

**Also Known As:**

Malware, Worm, Trojan Horse.

**Description:**

Viruses are malicious programs or codes that are inserted into computer systems without the user's permission and operate without the user's knowledge. Viruses are executable files that, if opened, replicate themselves in host files and spread uncontrollably to other host files. Depending on their severity, viruses can extensively damage software on a computer or the computer itself.

**How to Recognize This Threat:**

Viruses are executable files. Any unsolicited correspondence from an unknown source is a potential carrier for a virus, and should be considered suspect. Any attachment (.doc, .xls, .ppt, .zip, .jpg, .gif, .txt, .tif, and .zip) is capable of hosting a virus executable file.

**What Should I Do:**

It is recommended for every computer user to have anti-virus software loaded on their computer. Furthermore, the anti-virus software should have the capability of being automatically updated, to ensure it protects against the latest virus programs. It should also automatically scan incoming and outgoing email. On a regular basis - at least weekly - the anti-virus software should automatically scan every file on the computer. Users should also have firewall protection. Never open an .exe file that arrives via email, even if it is from someone you know

## WareZ Sites

**Description:**

WareZ (pronounced "wares") is a term used on the Internet to refer to pirated software. The term began being used when free download Web sites were popular. Today, "warez" is used to describe any site which hosts pirated software; Web sites, FTP sites, etc. The organizations or people behind WareZ sites are software pirates who violate copyright laws and steal from the rightful owners of the material. WareZ site pirates often obtain current or pre-release copies of copyrighted works, then "crack" the security features and offer it for download to others on the Internet. WareZ pirates and those who download from them are actively prosecuted. On July 1, 2005, for example, law enforcement agents from 11 countries participated in one of the largest raids to date on suspected WareZ sites. More than 90 searches were conducted worldwide.

**How to Recognize This Threat:**

Any Web site that offers free download of games, movies, music, and software applications that are not designated freeware or shareware is a WareZ site.

**What Should I Do:**

Never download copyrighted material. This is against international law. Anyone participating is liable and can be charged in criminal and civil proceedings.

## Worms

**Also Known As:**

Malware, Virus.

**Description:**

Worms are malicious programs or codes that are inserted into computer systems without the user's permission and operate without the user's knowledge. Unlike viruses (see virus), which cannot spread without human intervention, Worms spread automatically from computer to computer. Worms can replicate themselves and send out hundreds or even thousands of copies from each infected computer, tapping into the user's email addresses to spread the infection. Worms can have a devastating impact on Internet traffic, Web sites, and the user's own computer, which could be co-opted by the Worm's creators. The infamous Blaster Worm in November 2003 brought to worldwide attention the devastating impact of this malicious software.

**What Should I Do:**

It is recommended for every computer user to have anti-virus software loaded on their computer. Furthermore, the anti-virus software should have the capability of being automatically updated, to protect against the latest worms. It should also automatically scan incoming and outgoing email. On a regular basis - at least weekly - the anti-virus software should automatically scan every file on the computer. Users should also have firewall protection. It is important to have the latest version of the computer's operating system installed. Additionally, you should make sure your operating system is set to automatically receive updates from the operating system software manufacturers.

**Security Products and Technologies: What They Are and What They Do**

**Anti-Spam Software:** Anti-spam software is now becoming a common feature in many email software packages and ISP offerings. Anti-spam software helps to block unsolicited commercial email by using email profiles and real-time information from users around the globe to automatically determine new sources of spam. Anti-spam software blocks spam at the ISP, server, or email client level - stopping it before it arrives at your in box.

**Anti-Spyware Software:** Anti-Spyware software can identify, prevent, and safely eliminate potentially unwanted programs such as Spyware, Adware, pop-ups, dialers, key loggers, and remote-control programs.

**Anti-Virus Software:** An essential tool that every user should have installed on his or her computer. Anti-virus software scans for existing infections, removes them if they exist, and prevents future infections. Look for companies that offer periodic virus software updates, because updated virus software enables users to protect themselves against newly identified threats.

**Biometrics:** Biometric technologies are used to identify individuals using unique human traits such as fingerprints, retinal patterns, facial features, and voice patterns. Typically, electronic scanners record the trait and biometric software analyzes it. Biometric technologies verify that the person is who he says he is.

**Content Filtering Tools:** Content filtering tools are used by parents to block sites that are inappropriate for children. Most of the major Internet Service Providers offer filtering tools or child-safe services to customers. Check with your provider to see what they offer. When purchasing a filtering tool be aware that there are a number of different filtering strategies from key word and context sensitive software that analyzes language to services that limit access to specific categories and lists of Web sites. No single tool is 100 percent foolproof. It is important for parents to teach children safe Internet practices. There are a number of Web sites that are dedicated to this topic and parents should take the time to become familiar with sound safety practices.

**Device Authentication:** Device authenticators verify that only authorized PCs or other digital devices operate on a network. These devices can be used together with user authentication technologies to create cyber defense in depth and ensure that authorized users are operating computers they are cleared to use.

**Embedded Document-Level Security:** Embedded Document-Level Security enables a document's author to securely exchange information inside and outside a firewall. These technologies enable document authentication and maintain the integrity of its contents. Embedded Document-Level Security also enhances confidentiality.

**Encryption:** A mathematical means of protecting information. Encryption converts information into an indistinguishable format, which can then be reconstructed only with the proper algorithm and/or key. Encryption is used to protect data or to prevent unauthorized copying.

**Firewall:** A device or software that stands between the computer and the Internet and determines if a given IP packet should be passed through to the computer. A firewall helps to ensure that only suitable connections and traffic goes back and forth. Firewalls are used to prevent network-based attacks and probes through unused/unnecessary protocols, services, and ports. Every network or PC with an Internet connection should have a firewall.

**Intrusion Detection Systems:** These systems monitor failed login attempts, suspicious file activity, known attack patterns, and network probes to consolidate information across a network and automatically warn of a possible intrusion. Intrusion Detection Systems often use behavior monitoring to learn normal behavior patterns, and warn administrators when out-of-the-ordinary behavior is identified.

**Intrusion Protection Systems:** Intrusion Protection Systems can automatically detect attacks and stop them before they can do any damage. These tools watch for out-of-the-ordinary behavior such as buffer overflows or unusual port scans to automatically stop attacks.

**Logical Access Control:** A way of defining and limiting access to a system or site by user, role, or group affinity.

**User Authentication Technologies:** These technologies verify that the user is who he or she says they are using a password, electronic card, token, challenge-response grid card, or other unique identifier. Stronger authentication, often called two-factor or multi-factor authentication, uses a combination of identifiers to prevent unauthorized access to systems. Two-factor authentication, for example, involves using two separate pieces of information - usually a combination of something you know (a PIN or password) and something you have (a physical device).

**Virtual Private Network (VPN):** VPNs allow companies to use public networks for private data communication. VPNs use authentication methods to ensure secure data transfer across the Internet.

**Vulnerability Scanners:** Vulnerability Scanners are software tools that examine a computer or network configuration looking for poor security settings, configurations, or lack of up to date patches. These scanners often automatically carry out mock attacks against computers, firewalls, and servers to identify possible vulnerabilities.

The Business Software Alliance is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent the fastest growing industry in the world. BSA educates consumers on software management and copyright protection, cyber security, trade, e-commerce and other Internet-related issues. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cadence, Cisco Systems, CNC Software/Mastercam, Dell, Entrust, HP, IBM, Intel, Internet Security Systems, Macromedia, McAfee, Inc., Microsoft, PTC, RSA Security, SAP, SolidWorks, Sybase, Symantec, Synopsys, and UGS Corp.