Safety Net

www.aoema.org

Not feeling safe in the online world?

Use this guide to create your own "Safety Net".

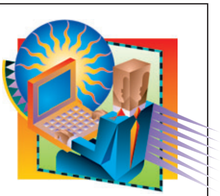
INSIDE! Take The 2-Min "Safety Net" Test and avoid online trouble before it happens.

FEATURING vital info on dot.com scams, web bugs, trojans and other internet traps...

Safety Net

Contents

The Internet has become an important communication tool for the 21st Century. With more than 300 million people worldwide taking advantage of this exciting phenomenon, the Internet is nothing short of a revolution. It has changed how we relate to each other and the world around us. We now have access to people, places and information never before available. Businesses and governments are streamlining operations, grandparents are staying in touch with grandchildren living half a world away, school children are communicating with astronauts in outer space – all over the Internet. The Internet has become ubiquitous, permeating all aspects of life. The Internet is literally changing our way of life.



You may, however, have some concerns about venturing into the online frontier. We hear about viruses, Trojans, invasion of privacy, lack of consumer protection, "dot.com scams" and even something called "web bugs" – all reasons to be concerned. However, this is the way of the future and it will become increasingly difficult to ignore the online world. Your best defense against these potential problems is to learn how to **prevent** them from occurring in the first place.

This booklet is a practical guide for beginners as well as experienced Internet users for creating your own "safety net" to safeguard against fraud in the online world. There is risk associated with everything we do and nothing can be 100%. We can, however, greatly minimize the risks associated with online transactions if we take a little time to learn what the "bad guys" know and beat them at their own game by taking preventive measures. The Internet can be an enjoyable experience and if you follow the simple advice in this booklet, you can **avoid trouble before it happens**.

Introduction

ESSENTIALLY THERE ARE 4 QUESTIONS WE NEED TO ASK:

How do I secure my computer?

How do I protect my personal data?

How can I trust online transactions?

How do I avoid Internet trouble, traps and scams?

This booklet aims to answer these important questions in a simple, straightforward manner, without getting too technical or bogged down in so much detail that you end up more confused. There are 24 topics, covering a range of security concerns and organized according to which question they relate to. For each topic there is a definition of the potential problem, recommended steps for avoiding trouble before it occurs, and references to websites that can provide further assistance or more in-depth coverage of the topic.

For more information and updates on all subjects, including specific references for individual APEC economies, refer to **www.aoema.org/safetynet**.

	YES	NO	
Do you have anti-virus software installed on your system?	□	□	**See p.32**
Do you know if you have the most recent version of anti-virus software?	□	□	**See p.32**
Have you selected the "automatic update" option for continuous updating of virus definitions?	□	□	**See p.32**
Have you downloaded new virus definitions in the past 7 days?	□	□	**See p.32**
Do you have a personal firewall installed on your system?	□	□	**See p.12**
Do you have the most recent version of your firewall software program?	□	□	**See p.12**

TAKE THE 2-MINUTE ”SAFETY NET“ TEST AND AVOID ONLINE TROUBLE BEFORE IT HAPPENS.

You don't have any questions at this time? You have everything under control? Very possibly, but we would like to recommend that if you do nothing else, at least take this 2-Minute Safety Net Test to determine if you have accounted for all critical security measures.

The 2-Min "Safety Net" Test

Do you "disconnect" from your Internet connection when not in use?	□	□	**See p.12**
Do your passwords include a combination of numbers, uppercase and lowercase letters?	□	□	**See p.23**
Have you changed your passwords within the last 30 days?	□	□	**See p.23**
Do you remember your passwords without having to write them down?	□	□	**See p.23**
Are you using the latest version of operating system software, browser, email and all application programs?	□	□	**See p.27**
Have you selected "automatic update" for all programs that offer that option?	□	□	**See p.27**
Do you know what the "cookies" setting is on your browser?	□	□	**See p.10**

If you answered "NO" to any of these questions, it is highly recommended that you refer to the pages noted and become more familiar with those topics.

Safety Net

Topics and Recommended Actions

HOW DO I SECURE MY COMPUTER?	Page Reference:
How can I stop hackers from entering my computer system?	FIREWALLS Page 12
How can I protect my young children from pornographic material and hate sites?	MONITORING Page 19
What is wrong with using my dog's name for a password? It's easy to remember.	PASSWORDS Page 23
Why should I update to the latest version of my software when I don't need the new functionality?	SOFTWARE Page 27
Is it true that programs can be put in my system that either disrupt my computer or cause trouble for others?	TROJANS Page 31
What can I do to prevent viruses from entering my computer?	VIRUSES Page 32

Where To Find The Answers To Your

HOW DO I PROTECT MY PERSONAL DATA?	Page Reference:
How do I prevent websites from capturing the personal information contained in my computer?	COOKIES Page 10
Are chat rooms a safe place to meet people and exchange information?	CHAT ROOMS Page 14
How do I prevent businesses from using my personal information without my consent?	PRIVACY Page 24
How can I protect myself when accessing the Internet from a public location like a library or Internet café?	PUBLIC ACCESS Page 25
I am so sick of junk emails, but do they actually pose any type of security risk?	SPAM Page 28
Are there really "spy" programs that can get into my computer?	SPYWARE Page 30

Page Reference:

Page 8 CONSUMER PROTECTION

Page 11 DIGITAL SIGNATURES

Page 18 LEGAL

Page 21 DISPUTE

Page 26 SECURE WEB PAGES

HOW CAN I TRUST ONLINE TRANSACTIONS?

How can I protect myself from con artists operating in the "dot.com" world?

How is it possible to sign legal documents and business contracts in the online environment?

How can I find out what is legally permissible and what isn't in the online world?

How can I resolve a dispute over a purchase if the merchant is halfway around the world?

How can I tell which sites are secure before I shop on them?

Questions

Page Reference:

Page 13 IDENTITY THEFT

Page 15 IPR

Page 16 DUMPING

Page 17 SCAMS

Page 20 DEFAMATION

Page 22 STALKING

Page 29 SPOOFING

HOW DO I AVOID INTERNET TROUBLE, TRAPS AND SCAMS?

How can I make sure someone isn't using my personal data and pretending to be me?

Am I free to use any information I find on the Internet?

I understand some users are finding mysterious charges on their phone bills. How do I prevent that?

How do I know if a business opportunity discussed on the Internet is actually legitimate?

What if someone publishes defamatory statements about me personally or about my business?

Someone is continuously harassing me with emails and while in chat rooms. How do I stop this?

How is it possible that a friend of mine received an email from me, but I never sent it?

Consumer Protection

ABOUT CONSUMER PROTECTION

Con artists have been around forever and consequently, consumers have always had to be careful about who they do business with. The old Latin phrase "caveat emptor" or "let the buyer beware" should be heeded whether shopping in person or over the Internet. Considering most people have yet to make an online purchase, there is a certain amount of fear associated with the unknown. Consumers should use reasonable caution and common sense, just as you would in the physical world.

Let the following list of Recommended Actions serve as a guide for what to do BEFORE you actually make a purchase over the Internet.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.econsumer.gov

www.bbbonline.org

RECOMMENDED ACTION

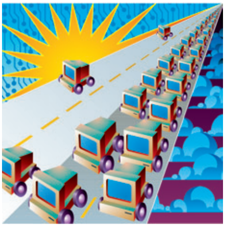
- Look for and read policy statements on websites. This includes statements on the privacy of personal information, customer satisfaction and product return procedures, and the security of financial transactions made on the website.
- Make sure that online forms are secure.
- Reject unnecessary cookies.
- Use a secure browser and make sure it is the latest version available from the manufacturer.
- Make sure you clearly understand the merchant's shipping and refund policies.
- If there is an "FAQ" (Frequently Asked Questions) section, it is a good idea to read through the list of questions to find out more about how a particular merchant deals with its customers.
- Don't disclose more personal information than is necessary to complete a transaction. Don't provide any personal information to a website unless you feel comfortable with the stated policies and procedures, and you can be sure that your personal details will be transmitted over a secure link.
- Never divulge your password to anyone online or over the telephone.
- Be sure to keep records of your online transactions. You may need to refer back to this information should you question a charge on your credit card statement.
- Review monthly credit card and bank statements for errors or unauthorized purchases. It is important to notify the appropriate financial institution immediately.
- Be cautious of any company that makes claims you find hard to believe. Chances are it is not a reputable business.
- Get to know the business you are dealing with. Honest merchants tend to be "up front" about their business practices, providing clear instructions on how they intend to do business with you and will typically respond to email queries if you have a question that isn't covered by a policy statement or included in the FAQ section.
- Make sure the terms and conditions of the sale are clearly stated, including product availability, method of shipping, price, additional costs that might be incurred by the customer, return and refund policies, warranties and guarantees.
- Use a credit card rather than a bank debit card. With a debit card, the funds are immediately debited to your bank account and it is generally more difficult to deal with disputed charges.
- Be wary of consumer rating sites, as many of them are not being honest with consumers.
- Most importantly, learn what rights you have as a consumer by finding out what consumer protection laws are in effect in your local area. Consumer protection laws vary dramatically.

IF A PROBLEM OCCURS, DO THE FOLLOWING:

- Contact the merchant to discuss the problem.
- If an agreement cannot be reached contact your local consumer group.
- If the merchant participates in a recognized program like BBBOnline, contact program administrators.
- Contact your credit card company for advice.

10 Cookies

ABOUT COOKIES



The main purpose of cookies is to identify users for purposes of customizing web pages to better meet the specific needs of consumers. Some websites will ask you specific questions and then package your responses into a "cookie" to be stored by your Web browser for later use. Others will simply track how you interact with their website and create a cookie that reflects your browsing or shopping habits. Then, the next time you visit that same Web site, it will look at the cookie on your machine and the information will be used to create personalized Web pages for you. For example, a welcome page might have your name on it or you might be presented with special offers for products you are likely to be interested in based on your buying history. Cookies generally enhance your online experience and with reputable businesses there is little to worry about. However, there are some businesses that use something called "third-party cookies" and this is what you have to be wary of.

A "third-party cookie" comes from a website different from the one you are actually visiting and typically originates from an advertiser wishing to learn more about your interests and preferences in order to determine which ads are most appropriate for you. These advertising companies are also interested in displaying new ads each time you visit a particular site and cookies help them keep track of your viewing history. This type of cookie is imposed on your browser without your permission, often resulting in a lot of pop-up screen ads you didn't ask for nor are interested in. While "third-party cookies" are not likely to cause damage to your system, they can be intrusive and certainly a nuisance.

RECOMMENDED ACTION

It is now possible to control cookies. Free, downloadable, programs are available to help you manage this annoying problem. Refer to the websites noted below.

The easiest way to find out if a business is using cookies and if they are, how they are using the information they collect from cookies, is to look for a policy statement on their website. Reputable online businesses today are very honest with consumers about exactly how they use cookies and explain their intentions in the form of a policy statement. If a website does not include this type of disclosure, you may want to think twice about dealing with that business entity.

Check the cookie setting in your browser. For example, in Microsoft Internet Explorer, go to "Tools" then "Internet Options" then "Privacy" and select the setting that best meets your needs.

Regularly delete temporary Internet files (refer to "help" menu on your browser).

WHERE TO GO FOR HELP AND MORE INFORMATION

www.cookiecentral.com

www.lavasoft.de

Digital Signatures

ABOUT DIGITAL SIGNATURES

In the paper world we use handwritten signatures as a way to signify our agreement with, acceptance of or commitment to a paper document. Many people are concerned the electronic world may not provide that facility. Digital signatures do in fact provide it and much more.

The term "digital signature" should not be confused with the terms "electronic signature" or "digitized signature". An "electronic signature" covers a broader range of possibilities and in its simplest form can be a name typed at the end of an email. A "digitized signature" is actually an electronic picture of your handwritten signature. Sign your name on a piece of paper and scan it into your computer. While it might look like your signature, it may not be a legally binding signature for an electronic document.

Complex mathematical formulas are used to create digital signatures. At the heart of the process is something called a "key pair". One part of the "key pair" is private and used to digitally sign your name. This key should never be revealed to anyone. The other part of the "key pair" is public and is used to verify that a signature belongs to a particular person or entity. The public key is either available from an online repository or is sent with an email message to the intended party.

But, I hear you ask, how do I know that the private key actually belongs to the person who is using it?

The key is verified by a trusted third party and this entity signs the key to signify that they are satisfied that the key belongs to a particular person. This is called certification and a certificate is attached to the public key. A group of trusted third parties working together to verify identities is called a Public Key Infrastructure or PKI.

An example in the paper world that makes this process easy to relate to is your passport. When you apply for a passport, you must provide a photo of yourself and more than one document to verify your identity. Your government then verifies that you and your photo are the same person and are valid. You are then issued a passport (certificate) that attests to your identity. Other governments trust that your government has done its job and they accept your identification. Just as there are false passports, it is possible to falsely obtain a certificate. It is, however, highly unlikely that you will ever have to deal with this problem as the incidence rate is extremely low.

To send a private message to someone you must first encrypt it using the recipient's public key. It is the private key paired with the public key that allows the recipient to decrypt your message and read it. By employing the "paired key" methodology, no one can read an encrypted message unless they have access to the private key. Therefore, it is extremely important to protect your private key.

The subject of digital signatures is actually very complex and this is only a basic introduction to the topic. To learn more about this subject and related technologies, refer to the websites noted below.

NEVER GIVE OUT YOUR PRIVATE KEY TO ANYONE.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.apectelwg.org/apecdata/telwg/eaTG/crypto.html

http://searchsecurity.techtarget.com

Firewalls

ABOUT FIREWALLS

Through the use of a "personal firewall" you can protect your computer from hackers and prevent unwanted programs from entering your system in the first place.

You might think that you have nothing on your computer worth looking at or stealing and therefore see little or no reason to concern yourself with a personal firewall. There are, however, many reasons why hackers may want to break into your computer, such as for purposes of:

VANDALISM – to gain access to your critical files and potentially cripple your system;

THEFT – obtain account details and passwords, or deploy "spyware" to take on your identity;

MANIPULATION – use your computer to attack or spam other computers.

It is not necessary for the hacker to know anything about your system or your passwords. Software is available to randomly scan the Internet, looking for open "ports" or doorways into computers. If, for one reason or another, your system has an open port, a hacker could gain access to the data on your computer, or send spam to other computers from your computer, which may result in your Internet address being blocked. Firewalls can help to protect you from these threats and ensure that your system will run smoothly and without problems while connected to the Internet. Firewalls can also help to protect you from unwanted cookies, pop up ads and prevent programs from being planted in your computer without your knowledge.

There are two types of firewalls. One is a hardware-based firewall and is most appropriate for internal networks (computers networked for home or business use). The other type of firewall is created by installing a software program on an individual computer and monitors all traffic to and from the Internet.

It is best to "disconnect" your Internet connection when not in use (extremely important for broadband users).

RECOMMENDED ACTION

All computers accessing the Internet today should use a firewall. This should not be optional or based on your level of Internet activity. The occasional user is just as vulnerable as the full-time user in terms of random scanning by hackers. There is no excuse for not installing a firewall since several excellent programs can be downloaded from the Internet at no cost. Refer to the websites below for examples of this type of firewall software and for additional information on firewall technology.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.zonelabs.com

www.symantec.com

www.sygate.com

ABOUT IDENTITY THEFT

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. While this type of crime occurs in both the physical as well as the online environment, there are concerns that we may become even more vulnerable to this type of crime as more and more personal data is collected, maintained and accessed via the Internet.

Identity theft can have dire consequences for the victim and therefore should be taken seriously. If someone takes on your identity, they can ruin your credit history, create massive debt due to unauthorized use of your credit cards, or worse yet, cause you to be charged with crimes you had nothing to do with. Not only is your good name ruined by identity theft but it can cost you a lot of time and money to repair the damage that has been done. Considering the rather severe consequences of this type of problem, it is far better to take preventive measures than to wait for it to happen and then deal with it.

Identity Theft

RECOMMENDED ACTION

Since this is a crime that can occur in either the physical or online environment, the following preventive measures should be heeded at all times:

1 Some personal data is more critical than others from a security standpoint. For example, in the United States a Social Security Number (SSN) is used extensively to identify a person and often becomes the primary question asked when trying to enter a secure website or on the telephone when you want to get account details from your bank or other financial institution. Other critical data is mother's maiden name, driver's license number and any other form of identification that is considered to be the most personal and therefore the most secure.

2 Be very careful with bank account details and monthly bank statements in both the online and physical environments.

3 Do everything you can to protect your credit card accounts. Keep an eye on your card when you hand it over to someone for processing. If you anticipate using your credit card for an online purchase, first check to make sure the website uses adequate security for processing financial transactions. It is also a good idea to cancel any account you haven't used in the past 6 months as open, but inactive, accounts are often a target.

4 Be ever vigilant when using ATM cards to prevent your pin number from being seen by people standing near you.

5 Make sure you have strong passwords for all your accounts and change them frequently.

6 Regularly monitor your bank and credit card statements for any unusual activity.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.idtheftcenter.org
www.privacyrights.org/identity.htm
www.consumer.gov/idtheft/

Instant Messaging, etc

ABOUT INSTANT MESSAGING, CHAT ROOMS, FILE SHARING

There are many different ways to communicate or "chat" in real time over the Internet. Web-based chat is the simplest method, and only requires a browser. Instant Relay Chat (IRC) requires that you either purchase or download a specific software package that allows you to participate in established "chat channels" or discussion groups. Instant messaging (IM) lets you to set up a list of friends or co-workers and keep track of who's online. If someone in your group is online at the same time you are, a message can be sent and they will receive it instantly.

Businesses are increasingly utilizing IM for internal, as well as external, communications. Conferences involving two or more employees can now be done online. Companies are also using IM to effectively communicate with suppliers and customers. While IM has become a useful communications tool for large and small businesses, Chat Rooms seem to be the domain of teenagers. Both forms of real-time communications over the Internet pose potential security risks if preventive steps aren't taken to protect both your computer and your personal information. Follow the recommendations in this section and review the suggestions included in Online Stalking, Monitoring, Firewalls and Viruses.

Another popular application on the Internet today is known as file sharing. Different approaches to file sharing pose different security risks, but they all have the potential to unintentionally open up some or all of your computer's files to hackers on the Internet. Ignoring the security risks could compromise your personal or financial information, or result in your computer being vandalized. "Peer-to-Peer File Sharing" is particularly popular today and programs like Kazaa, Morpheus and LimeWire allow people to share files by taking them directly from the owner's computer. The risks associated with this type of application include:

- improper configuration of file sharing software making your computer accessible to anyone on the Internet;
- violating copyright laws. Permission must be sought from copyright owner to avoid infringement of copyright.

RECOMMENDED ACTION

- Maintain up-to-date virus protection and be sure to install a firewall.
- Be very careful when installing file sharing software, and only allow access to those files that you want to share, not all your files.
- It is extremely important that you do not reveal personal details while in Chat Rooms.
- Be aware of copyright implications of sharing files.
- Be aware that this area of the Internet is not private and often subject to scrutiny.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.icq.com/support/security/

www.cert.org

Intellectual Property Rights

ABOUT INTELLECTUAL PROPERTY RIGHTS (IPR)

Human creativity and innovation is everywhere. From the plates we serve our meals on to the paintings we enjoy on the wall, hand-made carpets we walk on, the refrigerator, the telephone, the music we listen to and the books we read, these are all creations of the human mind and considered to be intellectual property (IP).

To better understand the concept of IP, you only have to go as far as your refrigerator. Undoubtedly you will find a wide variety of branded food products, each displaying a familiar "trademark" or logo of the company that produced it. Thanks to marketing and advertising, company trademarks have become very familiar and tend to influence our buying habits.

Considering the marketing power of trademarks, companies will do everything possible to protect their brand and guard against trademark infringement. If we go back to the refrigerator and look at the many different containers and special packaging (such as canned, vacuum-packed, cartons, air-tight seals), we encounter registered designs for the shape of containers, patents covering the production of packaging and

trademarks for the brands and logos. The refrigerator itself may be subject to numerous patents covering refrigeration unit, shelving, and other components. Even the manual is covered by copyright, as it is original written text.

Since the Internet has become popular with mainstream society, there has been increased awareness and concern about the unauthorized distribution of IP, including films, art forms, music, photos, books and software over the Internet. As a user or provider of online content, it is your responsibility to become familiar with the issues, recognize all national IP laws that might apply, and generally be aware of international IP conventions.

When linking your web site to other web sites, permission should be sought to avoid infringing the other site's trade marks or copyright. Common problem areas are: meta tag abuse, banner advertisement, framing and unauthorized deep linking.

RECOMMENDED ACTION

Be aware that SEVERE penalties can be imposed when infringing on the Intellectual Property Rights (IPR) of another person or company. Copyright violations include using graphics without permission, plagiarizing someone else's work, and "peer-to-peer" file sharing of music, to name a few. Considering the importance of understanding what is at stake, it is crucial to refer to the websites noted below.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.wipo.int

www.apecipeg.org

Internet Dumping

ABOUT INTERNET DUMPING (OR MODEM HIJACKING)

What is it? Known by various names in different parts of the world, Internet dumping occurs when a program in your computer drops your connection to the Internet and dials another number (such as an international number or a "premium pay-for-service" number). In most cases you don't know that you have been "dumped" until you receive your phone bill and find mysterious charges.

How does it happen? Unscrupulous online businesses, many of which are "adult" sites, will trick users into agreeing to view their websites over alternate numbers that cost a premium. How this works is that a new user will be instructed to download a special program called a "viewer" for purposes of viewing the website, and the terms-and-conditions statement you must agree to prior to actually downloading the software includes a statement that you consent to use a different number to access the site. This terms-and-conditions statement is typically presented in such a manner that you are not fully aware of all the conditions, especially the use of an alternate number. Additionally, the so-called "viewer" is actually a program expressly designed to re-dial a premium number that results in outrageous charges on your phone bill.

Unfortunately, many people have unknowingly fallen for this scam and have been liable for the outrageous phone charges, as they explicitly agreed to the terms and conditions of the site when they downloaded the software. Claims to recover these costs are nearly always rejected, leaving the consumer with no choice but to pay.

RECOMMENDED ACTION

To protect yourself from this type of scam:

- Monitor the activities of your children or employees (anyone who might have access to your computer) to ensure that they are not agreeing to the terms and conditions on these types of websites.
- Ensure that the volume is turned up on your modem so that you can hear if it redials.
- Ensure that the "history" in your browser is kept for a long time so that you can trace back to the sites that might have caused the problem.
- You may want to speak to your telecommunications provider about barring international or "premium" numbers like "1-900" on your data line.
- If you intend to access "adult" sites, be extremely careful to read and understand all agreements before you actually click on "OK" or "YES".

WHERE TO GO FOR HELP AND MORE INFORMATION

www.tio.com.au/FAQ/int_dumping.htm

Internet Scams

ABOUT INTERNET SCAMS

Unfortunately there are many scams on the Internet today. Working from actual complaints lodged by consumers in the United States, the Federal Trade Commission (FTC) has identified the following as the 12 most common scams to be on the lookout for:

1 Business Opportunities – offering big incomes without much work or cash outlay. Many of these are illegal pyramid schemes.

2 Bulk Email – offering large lists of email addresses to which you can advertise your own products or services to. Most ISPs do not allow bulk emails or unsolicited mailings and you could be shut down.

3 Chain Letters – you send a small amount of money to each of 4 or 5 names on a list and replace one of the names with your own. Chain letters have been around for a long time and they are illegal when sent via email or via the post office.

4 Work-at-home Schemes – promises of steady income for minimal labor. For example, "earn $2 each time you fold a brochure and seal it in an envelope". You pay the start-up fee, do the work as requested, but never get paid the money you were promised.

5 Health and Diet Scams – pills, herbal formulas, cures for impotence and hair loss are among the most popular scams flooding email boxes today. These gimmicks simply do not work and you are throwing money away.

6 Effortless Income – these are the get-rich-quick schemes and none of them work.

7 Free Goods – pay a small fee to join a club and recruit others to earn free goods. You pay your money, but never receive the goods.

8 Investment Opportunities – promises of high rates of return with no risk. These are almost always schemes that have no way of paying any kind of investment return as they are not properly funded. Their claims and statistics are mostly lies.

9 Cable De-scrambler Kits – pay a small sum of money and receive a kit to assemble a cable de-scrambler that allows you to receive cable television without paying a subscription fee. These do not work and if they did, it is illegal to use them.

10 Guaranteed Loans or Credit, on Easy Terms – unsecured home loans and credit cards are offered through unsolicited emails. Legitimate financial institutions do not work this way.

11 Credit Repair – offers to erase negative information from your credit file so you can qualify for a credit card, loan or job. If you follow the advice given, you will be committing fraud.

12 Vacation Prize Promotions – "you have just won a fabulous vacation" or "you have been specially selected for a great vacation package". You will find that it isn't what you thought it was or be required to pay additional fees that weren't explained in the first place.

RECOMMENDED ACTION

If it sounds too good to be true, it is almost always exactly that. Don't be taken in by slick sales pitches and be aware that many of these scams can actually result in criminal charges against you. Familiarize yourself with the FTC website and others like it that try to keep consumers informed of the latest scams on the Internet.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.ftc.gov

www.crimes-of-persuasion.com

Legal Issues

ABOUT LEGAL ISSUES

The Internet is a global resource, but the laws governing Internet activities may be different as you cross national boundaries. Some activities, like child pornography or hacking into computers, are universally illegal. Others, like gambling or hate sites, are permissible in some parts of the world but not in others.

Here are some examples of activities that are illegal in many parts of the world:

- Gambling;
- Purchasing firearms;
- Dealing in drugs (prescription as well as illicit) and other medical supplies;
- Hate sites aimed at certain races, religions, ethnic groups, etc.;
- Pornography of all types;
- Encrypting messages so that governments can't read them if they want/need to;
- Hacking;
- Pirating software;
- Writing and releasing virus software;
- "Denial of service" attacks which prevent people from accessing certain websites;
- Intercepting communications;
- Maliciously misrepresenting oneself for financial gain (including Identity Theft);
- Pyramid and Ponzi Schemes.

The first rule you should observe is that if it is illegal or prohibited in the off-line world, it is illegal or prohibited in the online world. You should also keep in mind that the laws governing businesses in the off-line world such as contract law, product liability and advertising also apply in the online world. The Internet is evolving into a serious place of commerce and business should be conducted according to the laws and conventions that have been in effect for many years. The Internet is not the "wild west" or a "lawless frontier". You are expected to know what the legal boundaries are and abide by them.

RECOMMENDED ACTION

Before selling on the Internet, check with your government's international trade department to make sure there aren't restrictions for the products you wish to sell.

Before buying products from international sites, you may want to check first with the appropriate government departments to make sure you are not in violation of any restrictions or regulations.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.eclip.org

www.bmck.com/ecommerce/

www.gipiproject.org/

www.ilpf.org

www.uncitral.org

www.cybercrime.gov

Monitoring Internet Usage

ABOUT MONITORING INTERNET USAGE

MONITORING EMPLOYEE USE: The Internet has become a valuable business tool as well as a powerful distraction in today's workplace. Monitoring employees' Internet use has become a necessary part of a manager's job. To ensure that productivity doesn't decline and to protect your company from unwanted legal challenges, it is important that you become aware of the issues facing all businesses today, from the largest to the smallest, and develop a proactive strategy.

MONITORING FAMILY USE: The Internet offers family members many opportunities for learning, constructive entertainment, and personal growth. Parents, however, are concerned about their young children accessing what they consider to be inappropriate websites. While the Internet is fundamentally a great place for children, there are some areas of cyberspace that are not appropriate, just as there are areas in almost every city that are inappropriate for children. There are also certain activities on the Internet that may be appropriate for adults but not for children, and areas that are suitable for some children and not for others.

RECOMMENDED ACTION

BUSINESS USE: In developing a policy and associated guidelines, the following should be included:

- Establish a written policy that prohibits employees from using company computers for personal email or visiting inappropriate sites.
- Clearly communicate the fact that the company's computer resources are not to be wasted and are strictly for approved business purposes.
- Include guidelines on language and content for emails.
- Manage your Internet policy with monitoring software.
- Reinforce your Internet policy with on-going employee education.

FAMILY USE: The challenge for parents is to educate themselves and their children about how to use the Internet safely. Parents can take advantage of software that audits as well as filters children's Internet usage. Use the website references noted below as a starting point.

WHERE TO GO FOR HELP AND MORE INFORMATION

BUSINESS USE	FAMILY USE
www.email-policy.com	www.getnetwise.org/
www.epolicyinstitute.com	www.wiredpatrol.org/
www.fatline.com	www.childnet-int.org/

RECOMMENDED ACTION

If this happens to you personally or to your company:

- Stay calm and don't get upset.
- Contact the responsible party and calmly discuss the issue. Suggest they withdraw the comments.
- If you don't get the desired results, contact a lawyer familiar with defamation suits.
- Report the offending behavior to your Internet Service Provider (ISP).

Online Defamation

ABOUT ONLINE DEFAMATION

Online defamation is something that everyone needs to understand. Defamation suits have been debated in courtrooms for decades, causing traditional media like newspapers, magazines and book publishers to carefully check their sources before going to print. Recent court cases, however, make it clear that anyone publishing on the Internet could be named in a libel suit. The term "publishing" now encompasses emails, list servers, chat rooms, and websites. We all have to be responsible for what we say and make certain that we don't intentionally or inadvertently spread false or damaging information about individuals or companies.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.onlinepolicy.org/defamation.shtml

www.wiredpatrol.org/law/freespeech/defamation.html

www.spawn.org/marketing/slander.htm

www.cyberlaw.com

To avoid being the target of a lawsuit:

- Make sure you can back up any claims or comments with irrefutable facts, not just opinions or emotions.
- Remember, once an email has been sent you cannot get it back before the recipient reads it.
- Be very careful about what you say in emails, over list servers, in chat rooms, and during instant messaging sessions. Be especially careful what you publish on a website.
- To avoid legal action against yourself, be sure to educate family members and employees of the potential problems associated with publishing in the online environment.
- Before publishing negative statements online, assess why you are doing it and what benefit you will receive from your action. Usually you will find that it isn't worth the risk.

ABOUT ONLINE DISPUTE RESOLUTION

Disputes happen on the Internet, just as they do in the physical world. However, it can be harder to work things out when you've never met the other party face-to-face. The European Union (EU) has been running a pilot project under the name ECODIR, which stands for Electronic Consumer Dispute Resolution, and is designed to enable consumers and online businesses to resolve disputes arising from Internet transactions.

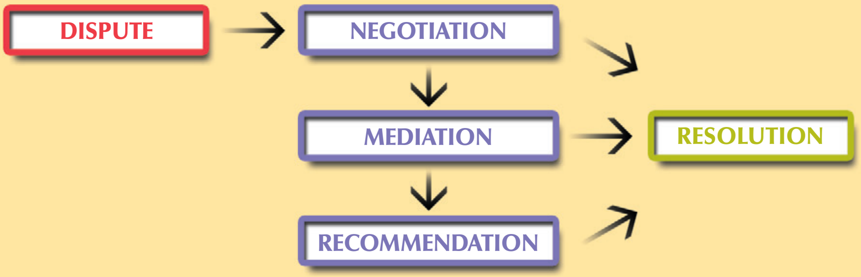
If the parties involved cannot reach a mutually agreed settlement through negotiation, then a neutral third party (Mediator) is appointed to assist. This third party is obligated to sign a "Declaration of Impartiality" and the mediation process is confidential and voluntary. The parties may, at any time, withdraw from the mediation process and take their claims to court.

The whole idea is that through Online Dispute Resolution, a conflict born on the Internet can be resolved using the Internet. With more and more businesses establishing a "store front" on the Internet, this will become a necessary business tool in the not too distant future. This will provide a cost-effective and efficient manner in which to resolve all types of lower value disputes arising from online sales transactions.

The ECODIR project involves government, private industry and academics from Europe and North America. For more information about this project and others like it, refer to the websites noted below.

Online Dispute Resolution

ECODIR is an online process with secure web technology, involving 3 stages:



WHERE TO GO FOR HELP AND MORE INFORMATION

www.ecodir.org

www.adr.org

Online Stalking

ABOUT ONLINE STALKING

To define "online stalking" we first need to understand what "stalking" is. While there are many differing definitions, two points in common are:

1 repeated and unwanted behaviors whereby one individual attempts to contact another individual, and

2 the behavior causes the victim to feel threatened or some sense of fear or dread.

Online stalking, then, occurs when one person harasses another using email, Internet Chat-rooms and instant messaging. This can be very troubling for the person being stalked and some governments have created new legislation or revised existing legislation to include online stalking and in some instances restraining orders can be obtained.

Stalking can also extend to vandalism of computer systems if the security precautions identified in this booklet are not followed. While it is possible to stop a cyber-stalker, prevention is definitely the best policy.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.cyber-stalking.net

www.wiredpatrol.org/stalking/

www.privacy.net

RECOMMENDED ACTION

If you are being stalked:

- Delete any identities you have created in chat rooms and instant messaging systems.
- Immediately change your email address. Use gender-neutral references.
- Consider using an anonymous re-mailer.
- Contact your Internet service provider (ISP) or chat room moderator with evidence of harassment.

To reduce the risk of online stalking:

- Ensure that the name you choose as your "handle" or "screen name" is genderless.
- Ensure that your personal details are not made available anywhere on the Internet.
- Strengthen your passwords. Refer to the password section of this booklet for recommendations.
- Do not create an online biography. If one exists, remove it immediately.
- Most importantly, follow the security recommendations identified throughout this booklet. This is your best defense and can prevent it from ever happening.
- Don't use abusive language in chat rooms or instant messaging exchanges.
- See guidelines section for further recommendations.

Passwords

ABOUT PASSWORDS

You go out one day and inadvertently leave the door unlocked. A stranger comes in and looks around but doesn't take anything. Even though nothing has been stolen, how does it make you feel to know that someone has looked through your private things? People can do the same sort of "snooping" in your computer unless you protect yourself. Passwords are your first line of defense, but only if you use "strong" passwords. Your passwords are as important as the key to the front door and they should be of the highest quality, like a deadbolt lock.

Hackers use "password crackers," a type of software that is capable of uncovering a simple password in as little as 1 hour. A "strong" password, on the other hand, can take 10 to 20 years of processing time to "crack".

RECOMMENDED ACTION

Considering these statistics, it is well worth your time to follow these simple "do's and don'ts" when creating passwords:

- Don't use any word that can be found in any dictionary (any language) including scientific terms.
- Don't use any word in reverse that can be found in any dictionary (any language).
- Don't use any word that can be associated with you, i.e. address, phone number, birth date, pet's name, nicknames, favorite sports activity or hobby.
- Don't use consecutive letters or numbers like "abcdefg" or "234567".
- Don't use adjacent keys on your keyboard like "qwerty".
- Do make it simple enough that you can remember it without writing it down.
- Do use a combination of letters, numbers and special characters in random order.
- Do use upper and lower case and include special characters (* @ #).
- Do use at least 6 characters and the longer the better.

Now you must protect this password:

- Don't write it down anywhere.
- Don't give it to anyone for any reason.
- Don't select the "remember my password" feature associated with some websites and disable this feature in your browser software.
- Don't use the same password for everything – have one for non-critical activities and another for sensitive or critical activities. (Remember that logging onto your computer is a critical activity).

Privacy of Personal Information

ABOUT PRIVACY OF PERSONAL INFORMATION

Every day you share personal information about yourself with others. It's so routine that you may not realize you're doing it. During the process of paying bills, making travel arrangements, using a credit card for purchases in shops or restaurants, etc., personal details are divulged to strangers and we have no idea whether we can trust them. For some reason, though, many people tend to think of the online environment as being more of a risk than the physical environment, causing them to stay away from the Internet altogether.

While you need to be serious about protecting your personal information, there is no reason to panic, especially if you follow the simple recommendations in this booklet. Keep in mind that the electronic environment is really not all that different from the physical environment. It is more a matter of becoming aware of the types of problems specific to the online world and learning how to prevent them in the first place. It is an educational process and so it was with early credit card use. For many years credit cards were used with little or no concern for what happened to the carbon papers. However, once we became educated to the fact that information taken from carbons was being used for fraudulent purchases, we quickly learned the importance of ripping them into tiny pieces before discarding.

Financial information isn't the only area of concern for consumers. The ability to profile our shopping preferences, website viewing preferences, online health records, credit history, etc., is just as important and needs to be addressed as well. To maintain your privacy and to protect your personal information, follow all recommended security steps in this booklet and make a habit of taking the following action.

RECOMMENDED ACTION

Managing your personal information starts with recognizing the fact that some websites incorporate technologies intent on collecting your personal information and using it in ways you may find objectionable.

Once you understand this vulnerability, the next step is to take action by checking each and every website you visit and particularly those you intend to do business with, for a policy statement regarding how they will use your personal information. Two very important things to look for in a privacy statement are:

- How the company uses your email address – do they sell or trade email lists?
- Does the company collect personal data and use it without your knowledge or consent?

WHERE TO GO FOR HELP AND MORE INFORMATION

www.privacyfoundation.org

www.oecd.org

http://epic.org

www.privacy.net

ABOUT PUBLIC ACCESS POINTS

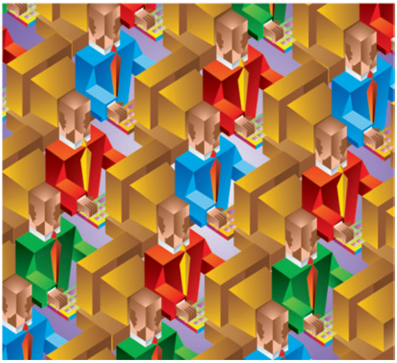
Many people around the world do not have a computer of their own but nevertheless want access to the Internet. People on vacation and not traveling with a laptop need to use the Internet to remain in touch with friends, family and business associates. Business people who prefer to travel without a laptop computer, but still need to access their email and exchange important business documents. These are all reasons for connecting to the Internet from a public access point, and examples of popular public access points today include Internet cafes, airport kiosks, and publicly available computer systems in hotels and libraries.

A viable and convenient solution for many, but one that has to be used carefully. By keeping in mind the open nature of these systems and carefully following the recommendations below, you can safely access the Internet from a public location.

Public Access Points

RECOMMENDED ACTION

- Be wary of people sitting or standing close to you – they could potentially look over your shoulder to see your login ID, password, or personal data as you actually type it in.
- If you use public access points regularly, be sure to change your password often.
- Clear the browser's "cache" when you leave. This helps to minimize the chance that someone else might be able to access your personal details.
- Clear the browser's "history settings".
- Close any and all browsers you have used before you leave.
- Do not allow the computer to "remember passwords" - this is a setting that you need to de-select.
- Never enter private or sensitive information while using a public access computer.



ABOUT SECURE WEB PAGES

If you want to buy something on the Internet you will be asked to supply your credit card number and personal details. Before you actually proceed with an online purchase, you should of course do everything possible to determine that the website you are dealing with represents a legitimate business and employs best practice policies for online commerce as outlined in this booklet.

Let's say you feel confident that you are dealing with a trustworthy enterprise and are ready to transact business. You are about to submit your personal details and credit card number and you want to make sure this information will be transmitted in a secure manner. The following set of recommendations outline the simple tests you can perform prior to submitting your personal information.

Secure Web Pages

RECOMMENDED ACTION

There is a simple test to determine if a web page is secure: On a Microsoft Windows based system, click the right mouse button while your cursor is positioned in any blank area of the web page and select "properties". This will bring up a screen with information about that page. Click on "certificates". If the page is not secure, it will let you know that no certificates exist for that page. If, however, the page is secure, you will be told what the "size of the key" is for the page and ideally you want a 128-bit key. This is a simplified explanation of a rather complex and highly technical subject, however the simple test does let you know that your sensitive information will in fact be transmitted securely.

There are two other ways to determine if a web page is secure, but they are not as reliable. One is to check in the "address" field at the top of your browser for "https" instead of the normal "http". The "https" designator tells you IF a page is secure, but not HOW secure it is (as in the 128-bit key).

The other method, and the one most often suggested to new users, is to look along the bottom of your browser for an icon that indicates you are on a secure web page (e.g. closed lock, closed padlock or unbroken key). This technique can't tell you HOW secure the page is either and these icons aren't displayed on certain types of web pages (i.e. frames-based).

WHERE TO GO FOR HELP AND MORE INFORMATION

To find out more about certificates, secure web sites and using secure web pages, look at the help section of your browser.

Software Updates

ABOUT SOFTWARE UPDATES

The software running on your computer could be a source of security problems if you don't keep it up to date. After a program has been in use for a while, small problems are discovered and the manufacturer will need to create "updates" or "patches" to fix them. Additionally, with each new version of a software program you can count on new security measures being introduced, as reputable software manufacturers are working hard to make the online environment safer for users. This is especially true for operating system software, be it Windows, Mac or Linux. It is in your best interest to run the most up to date version of your operating system and to regularly check for program updates. Application software should be kept up to date as well.

WHERE TO GO FOR HELP AND MORE INFORMATION

http://windowsupdate.microsoft.com/

www.apple.com/swupdates/

RECOMMENDED ACTION

- If using Windows XP or Windows 2000, it is best to specify the "NTFS" file system rather than the "FAT32" system. This will enable much stronger security on your machine as well as provide the capability of encrypting sensitive data on the disk to ensure confidentiality.
- Check to make sure you are running the latest version of your operating system (e.g. Windows 2000, Windows XP, Mac OSX)
- Check to make sure your browser software is the latest version (e.g. Internet Explorer 6, Netscape 6.2)
- Office application software is important since they produce files that are often shared or distributed through emails, floppy disks and file sharing (e.g. word processing, spreadsheet, database, calendar)
- Your email software is extremely important since you use it to regularly to communicate with people you know as well as strangers. You want the benefit of the latest security measures. (e.g. Outlook Express, Netscape Mail, Eudora).
- Make sure you have the latest version of your anti-virus software (e.g. Symantec, McAfee) and most importantly, make certain you update the virus definitions regularly.
- In order for your firewall to fully protect your computer, it too needs to be kept up to date (e.g. ZoneAlarm, Black Ice Defender, Symantec).
- And the most important recommendation of all is that many of the software products listed above give you the option of selecting an "automatic update" option. This is definitely the best way to manage the update process for all your software products.

Spam

ABOUT SPAM

Most of us get junk mail. Our mailboxes tend to fill up with advertising we didn't ask for and typically throw away without even reading. The equivalent is now happening with electronic mail or "email". Unsolicited messages end up in our electronic mailboxes almost daily and have become quite a nuisance.

Actually, spam is far more insidious than junk mail. While you can easily "delete it" from your system, you should think about the more far-reaching issues regarding spam. With junk mail, the costs are entirely with the sender. Companies pay to have advertising circulars printed and posted to you. With spam email, on the other hand, all recipients of a message pay to receive it, while the sender pays the same amount regardless if the message is sent to one or a million email addresses. Spam is costing individuals and companies time and money in the following ways:

- In most situations you have to download all messages in your mailbox, not just the ones you are interested in reading.
- Many users are subject to hourly connection fees and it will obviously cost more if you have to download a lot of spam emails.
- It takes time to sift through a pile of emails and time is money.
- Spam emails are clogging the mail servers around the world, resulting in higher costs and slower connections for everyone.

While it is unlikely we will be able to completely stop spam emails, we can hopefully reduce the incidence by following the recommended actions.

RECOMMENDED ACTION

1 Never, ever, respond to spam. By responding to spam you are actually confirming your email address and making yourself more of a target.

2 Don't use your normal email address on subscriptions, newsletters, mailing lists, etc. Reserve it for those people you communicate with regularly, such as business associates, friends and family. Create a separate email address to be used for everything else. In other words, maintain a private address and a public address.

3 Never buy anything advertised in a spam email. It only encourages the sender to continue this selling tactic.

4 Use a spam filter. There are many available so choose one that best meets your email needs.

5 Report "spammers" to anti-spam web sites and to government consumer authorities.

6 Remember to check the privacy statement of all the websites you interact with to see how your email address will be used.

WHERE TO GO FOR HELP AND MORE INFORMATION

http://spam.abuse.net

www.cauce.org

ABOUT SPOOFING

There are two types of "spoofing". The first happens at the technical communications level and is called "IP Spoofing". Good quality Internet Service Providers protect their users against this type of threat and therefore most home and small business users have no need to worry about it. However, if you are running a network with routers, talk to your equipment supplier to discuss how to protect yourself.

RECOMMENDED ACTION

- You may be alerted to an event of "email spoofing" from your email recipients or by investigating "bounced email" error messages. If so, be sure to collect as much information as possible about the messages in question and forward these details to your ISP for further investigation.
- If you have concerns about whether your emails are from known sources, you might consider using digital signatures to ensure that all messages are authentic. Refer to the section on Digital Signatures for more information.

Spoofing

The other type of spoofing is "email spoofing". This can happen in various ways but the result is that a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords or personal information).

- Many forms of trickery are being used to get users to disclose sensitive information such as passwords. The deceptive ploy may be in the form of "spoofed" emails, an interactive session on a website, a telephone call or even a written letter sent via the post office. Before responding to any requests for your password or other personal details, verify that the request is coming from a known and authenticated source. For examples of the type of ploys we are referring to, the website noted below is from the Computer Emergency Response Team (CERT), and they receive "spoofing" incident reports from around the world.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.cert.org/tech_tips/email_spoofing.html

Spyware

ABOUT SPYWARE

Spyware is any software that uses your computer and Internet connection to send your personal information to an individual or organization without your knowledge or consent. Spyware enters your computer as a software virus, from a web page you are viewing or from an email.

Spyware ranges from "third-party cookies" (see Cookies) to very intrusive programs that report back to software manufacturers on how you use their programs. Software downloaded from the Internet is particularly susceptible to this practice. For the manufacturer, they want to learn more about user preferences for purposes of customizing current programs and to assist in developing future programs. The consumer, however, generally objects to this form of surveillance, considering the practice to be intrusive and a violation of privacy. A number of lawsuits have been filed against companies engaging in these practices, resulting in most programs being modified to cease this form of intrusive data collection.

There are, however, some companies that continue to secretly gather personal information, making it prudent to carefully read all information made available to you during the download process. In many cases you can "opt out" of these "features" but you have to read the information very carefully to notice that you are actually being asked whether you will allow the information to be reported back to the manufacturer. Some companies are determined to collect personal information and do their best to cover-up the fact that they are installing "spyware" on your computer.

Another form of "spyware" is called "web bugs". These little programs show up as tiny image files embedded in a web page or an HTML-formatted email message. In most cases they are invisible and therefore not noticeable, but they work in conjunction with "cookies" to gather information about your web viewing habits. Your best defense against "web bugs" is to make sure you set your "cookies" preference at the highest level you are comfortable with.

RECOMMENDED ACTION

- Check the "cookies" setting on your browser.
- Download "spy check" software, such as "Ad-aware" (www.lavasoft.de)
- For all websites you interact with, look for and read all policies and statements regarding the use of your personal information and whether spyware is used to collect information.
- Make sure you install firewall software and keep it up to date.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.bugnosis.org

http://grc.com/optout.htm

www.spychecker.com

ABOUT TROJAN PROGRAMS

A "Trojan Program" comes into your system without your knowledge and works in the background, making it very hard to detect. Typically, a Trojan program comes "attached" to another program. That is why they are called "Trojans" – they come in an innocent looking package much like the Trojan Horse of ancient Greek mythology. Trojan programs can be attached to files sent via email, shareware exchanged in chat rooms, files on floppy disks, pirated software and a host of other devious means. Trojan programs can cause considerable damage and should be taken seriously. There are 3 primary types of Trojan programs:

- "Remote Access Tools (RATs)" – allow a hacker access to everything on your computer;
- "Key-loggers" – saves every keystroke you make and then sends a file containing this information to a hacker;
- "Password Retrievers" – collects your password files and sends them to a hacker.

It is important to note that simply downloading a file to your computer won't activate a virus or Trojan program. You have to execute or run the infected program to actually initiate the virus or Trojan. Be very careful when dealing with word processing or spreadsheet files, as they could contain executable macros that have been intentionally or unintentionally infected with a virus or Trojan. Considering the devious nature of Trojan programs, how can you actually protect yourself? Prevention is your best protection and is as easy as following the recommended action. While Trojan programs are different from and shouldn't be confused with viruses, anti-virus software includes Trojan detectors and is a critical part of your defense.

Trojan Programs

RECOMMENDED ACTION

- Install a personal firewall.
- Maintain your anti-virus software by regularly downloading virus definitions.
- Be sure to use your anti-virus software to manually check all programs before installing.
- Perform a virus scan on your entire system at least once a week.

These preventive measures will provide significant assurance that you will not be attacked by Trojan software.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.cert.org

Viruses

ABOUT VIRUSES

What is a virus? Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer much like a biological virus passes from person to person. Before the Internet became popular, computer viruses were mainly spread through the sharing of infected floppy disks. This made it relatively easy to pinpoint the source of the infection. Today, however, viruses come from a multitude of sources, including emails, word processing and other application files, computer games and software programs downloaded from the Internet. The good news is that even though there are more viruses today than ever before, we now have a way of preventing viruses from entering our computer systems in the first place.

What can a virus do to your computer? Viruses are software programs, and the actual effect of any particular virus depends on how it was programmed by the person who created the virus. Some viruses are deliberately designed to damage files on your system or in some way interfere with your computer's operation. All viruses can potentially destroy or damage files, even those considered to be relatively "harmless". What viruses can't do is damage your hardware. No matter what you hear to the contrary, viruses can't melt down your CPU, burn out your hard drive, cause your monitor to explode, etc. Warnings about these types of viruses are hoaxes, not legitimate virus warnings.

You might also receive an email from a friend or business associate telling you about a dangerous virus. In most cases these are virus hoaxes passed on by well meaning, but misguided, people. Do not forward hoax messages. All that does is clog up the Internet with useless emails, which is exactly what the "hoaxers" want. If you keep your virus program up to date, there is no reason to even look at these messages.

RECOMMENDED ACTION

- Make sure you have the latest version of your anti-virus software installed.
- Make sure you update your virus definitions every couple days or better still, take advantage of the "automatic update" option available on most anti-virus software programs. This facility automatically checks for new virus definitions each time you log on to the Internet.
- Never open unexpected files from anyone unless you can positively verify what it is, who sent it, and why it was sent to you. Check all files and make no exceptions. An email could identify the sender as your best friend, but actually have been sent by a hacker who got your email address by hacking into your best friend's computer. Refer to the section on Firewalls to learn how to protect your computer from hackers. All files should be checked by an up-to-date anti-virus software program prior to executing them.

WHERE TO GO FOR HELP AND MORE INFORMATION

www.symantec.com

www.mcafee.com

www.europe.f-secure.com/news/hoax.htm
(additional information on virus hoaxes)

Safety Net

Guidelines for:

- Unless you have installed either a hardware or software encryption device, you should assume that messages exchanged over the Internet are not secure. If it isn't appropriate on a postcard, then it isn't appropriate for email!
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are forwarding it on to an individual or a group, you should ask permission first.
- Never send chain letters via electronic mail as they are clearly forbidden on the Internet. Your network privileges may be revoked. Should you happen to receive one, notify your Internet Service Provider (ISP) immediately.
- Try to be brief with your messages, but at the same time be careful you aren't so brief as to be terse. A terse message can often be considered rude or angry.
- Use the subject line to express some sense of what your message is about. This makes it easier for the recipient to effectively sort through incoming mail, set priorities in terms of critical messages requiring immediate attention and filing of messages for future reference.

Guidelines for Email Messages

- Be careful when addressing a message or when replying to an email address, as some addresses appear to be that of an individual but are actually being distributed to a list of recipients.
- For people who routinely have to deal with a heavy load of emails, they appreciate being made aware of any specific emails that are lengthy and might require extra time to deal with them. Generally speaking, a message over 100 lines is considered long and it is a good idea to use the subject line to notify the recipient of this fact.
- Use both upper and lower case. It has become convention that if you use all upper case, YOU ARE SHOUTING.
- Some people like to use "smiley faces" to indicate a tone of voice or an attitude. A happy face is :-) and an unhappy face is :-(and is achieved by combining keyboard symbols. It is best to use them sparingly if you are going to use them at all and keep in mind that some cultures may not understand their meaning.
- You may not always have time to respond fully to a message at the time you actually receive it. Far better to send a brief email to let the sender know you did receive the message and a quick note to indicate that you will send a longer reply later.
- Unsolicited email advertising is unwelcome and in some contexts illegal.
- Avoid sending large files. A file over 150 Kilobytes is generally considered to be too big.
- To avoid creating long and unwieldy email recipient lists, use the "blind carbon copy" (BCC) convention when sending messages to large groups.

- Before you actually get involved in a mailing list or newsgroup, it is a good idea to spend one or two months getting to know the group before you post anything.
- Inappropriate behavior by users is not the fault of the system administrator. However, it is the responsibility of the system administrator to take action if someone has overstepped the boundaries of proper behavior.
- Once you press the "send key" it is too late to rescind your comments. Be very careful not to post comments that you might regret later.
- If by some chance you do accidentally send a personal message to the entire group, be sure to immediately send an apology both to the individual and to the group.
- If you have strong feelings about what someone else has posted, express your feelings in personal emails.
- Don't get involved in what is often called "flame wars." Avoid posting or even responding to incendiary material. Leave this type of problem to the list administrator.
- Avoid non-standard fonts, as they will display differently on different systems, making it difficult to read text files.
- Send subscribe and unsubscribe messages to the appropriate address.

Guidelines for Mailing Lists

- Keep your messages brief and to the point.
- Some lists welcome advertising while others have strongly stated rules against it.
- When replying to a message or posting, it is always best to make sure you include enough of the original text to provide context. Otherwise your response may not make sense.
- Be careful when sending personal responses. If you simply click on "reply to sender" you are most likely sending your reply to the entire mailing list and not to a single recipient as intended.
- Consider unsubscribing or setting a "no mail" option (if available) when you cannot check your email for an extended period.
- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting.
- Never give out your user ID or password. System administrators that need to access your account for maintenance or to correct problems will have full access to your account without having to request information from you.
- Avoid misunderstandings about dates by using the following date format: 11 Feb 2002.
- Acronyms can be used to abbreviate when possible, however messages that are filled with acronyms can be confusing and annoying to the reader. Some common acronyms are:

IMHO	=	in my humble/honest opinion
FYI	=	for your information
BTW	=	by the way

Guidelines for Consumer-friendly Websites

ABOUT YOUR BUSINESS

Do you clearly describe the nature of your business?

Do you include the following pertinent details?

- physical business address
- email address or telephone number consumers can use to contact you directly

ABOUT YOUR INFORMATION PRACTICES

Do you clearly state what your information collection practices are, including what you collect, how you use it and whether and with whom you share it?

Do you clearly state how personally identifiable information is used and whether it is shared with others?

Do you explain the security measures you employ to secure transactions on your website?

Do you understand the laws governing the transmission of personal data across national boundaries?

ABOUT YOUR ADVERTISING AND MARKETING PRACTICES

Do you provide accurate and truthful information about your products and business practices on your website?

Can you back up any and all claims you make about your goods and services?

Do you disclose all sponsors of ads on your website?

Do you respect consumers' decisions to not receive email advertising?

Do you take special care when advertising to children?

ABOUT THE SALE

Do you clearly identify what you are selling, with enough details that consumers know exactly what they are buying and the conditions of the sale?

Do you provide a list of total costs (including shipping and handling charges) and identify the currency used?

Do you clearly explain any additional charges that might apply to the sale?

Do you indicate any restrictions or limitations imposed on the sale?

Do you provide information regarding warranties or guarantees that are associated with the sale?

Do you provide an estimate of when the buyer should receive the order or alternatively, provide a tracking code and the website address of your transport operator so the buyer can track the shipment?

Do you clearly explain payment options?

CONSUMER PROTECTIONS

Do you explain your return policy, including instructions on how a consumer returns an item to get a refund, credit or make an exchange?

Are you clear about all conditions related to returns?

Do you provide the necessary contact details for how a consumer should contact you regarding complaints or problems?

Do you provide the consumer with a record of the transaction either through your website or a follow-up email?

Do you have clear policy statements on your website to inform consumers about the privacy of their personal information. Do you give consumers the opportunity to decide whether or not they wish to participate in certain programs like email newsletters and unsolicited email offers from other merchants?

Do you provide information on how you would resolve a dispute? Do you participate in any recognized online dispute resolution programs?

Guidelines for Safe Online Buying

Shopping on the Internet can be easy and convenient, however, consumers want to make sure it is also safe and reliable. Use these guidelines to protect yourself when shopping on the Internet.

- Be sure you are dealing with a company you can **trust** and respect. A friend recommends the site or international programs like BBBOnline (www.bbbonline.org) can verify that the company demonstrates ethical online business practices.
- Check for **merchant details** like physical address and phone number to make sure you have a way of contacting the merchant if you have a question or a complaint.
- Read and make sure you are comfortable with the company's **refund and return policies**, as not all companies accept returns or issue refunds. Some will only offer a credit for future purchases, some charge a "restocking fee" and most will not refund shipping and insurance costs. For online businesses that also have physical locations, you may be able to return products to the nearest shop to save shipping costs.
- For some products, like electronics or refurbished computers, it is very important to read and clearly understand the terms and conditions of the **warranty**.
- Be sure to sign in with **strong passwords** (refer to section on Passwords). Never disclose your passwords to anyone and it is best to de-select any website options for "remember my password".
- Before you finalize your online order, very carefully **check order details**, including item description, size, amount, shape, color, etc. Check that you have correctly typed in the shipping and billing addresses and make sure that all calculations are accurate, including shipping, handling and tax. The best shopping sites show you the exact amount they will charge you before the sale is finalized.

- To protect your privacy and to guard against possible unauthorized use of your personal information, read and understand the **privacy policy** on the website. This policy should disclose what information is being collected on the website and how that information is being used. If you can't find a policy, send an email or written message to the website to ask about its policy and request that it be posted on the site. Many companies give you a choice as to whether you will allow your personal information to be used or not. You should be given the option to decline or "opt-out" of having personal information, such as your email address, used for marketing purposes or shared with other companies.
- Ensure that the transaction is taking place over a **secure web page** (refer to section on Secure Web Page).
- It is very important to **save a receipt** of your transaction. Print the web page that includes order number and order details. Some websites actually instruct you to print at a certain point in the process and others advise that you will receive a receipt via email. If you are purchasing an online subscription (e.g. newspaper, magazine, list server), make sure you print out the contract and understand the procedures to unsubscribe from the service.
- The best shopping sites include an integrated **shipment tracking** capability to keep you informed about where your package is and when you can expect delivery. Other sites provide you with a tracking number and the address of the transport operator's website. If neither is provided, you may need to contact the company via email or telephone to specifically ask for this type of information.

Guidelines for Online Auctions

BEFORE YOU BID ON OR PURCHASE AN ITEM:

- Make sure you clearly understand what you are bidding on. Carefully read the item description, payment terms, shipping and handling costs, warranty, and refund policy. If you don't understand something or have a question, don't hesitate to contact the seller by sending an email message. You should be wary of any seller who refuses to reply to your emails or doesn't respond to your satisfaction.
- If possible, research the item, using both online and offline sources. Try to get an idea of fair market price before you bid.
- Closely examine photos to learn more about the item's condition.
- Check out the seller's feedback history (most online auction sites provide this information) and make sure you understand the rating system used by individual auction sites. It is also a good idea to find out how long a seller has been involved in the auction site. If you are dealing with a seller who is new to online auctions, you may want to establish email communications and ask direct questions before bidding.
- Read everything associated with the listing, including information at the end of the listing page, as this is often where the seller indicates their business policies and conditions of sale.
- To avoid a misunderstanding, get a definite delivery time.
- Make sure you are not buying dangerous or illegal items as defined in your jurisdiction. Check appropriate government sites for details.
- Before placing a bid, it's a good idea to set a bidding limit to avoid "buyer's remorse" or finding that you have the winning bid, but can't afford to pay for the item. When you place a bid on an auction site, you are actually entering a contract and could be legally bound to pay.
- When bidding on a high priced item or if you have doubts about a transaction, most auction sites provide escrow services. Refer to the individual auction site for more details.
- It is good practice to save all relevant web pages and emails associated with an auction in the event you need to follow-up with the seller.
- Immediately report suspected fraud to administrators of the auction site.
- Be very careful not to disclose personal information when communicating with sellers.

Asia-Pacific Economic Cooperation
An APEC Telecommunications and Information Working Group Project
APEC Publication #202-SO-01.1
www.apecsec.org.sg

AOEMA
Asia Oceania Electronic
Marketplace Association

Prepared by AOEMA
www.aoema.org

FMMC
Foundation for
MultiMedia Communications

Funded by FMMC (Japan)
www.fmmc.or.jp

With special thanks to the Australian Department of Foreign Affairs and Trade and AusAID for supporting the APEC E-commerce Awareness Workshops presented by AOEMA in Vietnam, the Philippines, Indonesia and China in 2001-2002. This publication responds to needs and priorities identified during these workshops.

www.dfat.gov.au

With special thanks to the Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan (MPHPT) for their support of the AOEMA Awareness Seminar Program since 1996, with seminars held in 14 economies. This publication responds to needs and priorities identified during these workshops and builds on the work of the E-Japan Forum (EJF) in developing a similar guide for use in Japan.

www.soumu.go.jp

The information and URLs contained in this booklet are accurate at the time of printing.

Please email us at info@aeoma.org for feedback, comments or more information.

August, 2002.

Consumer Protection

Cookies

Digital Signatures

Firewalls

Identity Theft

Instant Messaging, Chat Rooms, etc

Intellectual Property Rights

Internet Dumping

Internet Scams

Legal Issues

Monitoring Internet Usage

Online Defamation

Online Dispute Resolution

Online Stalking

Passwords

Privacy of Personal Information

Public Access

Secure Web Pages

Spam

Software Updates

Spoofing

Spyware

Trojan Programs

Viruses

Guidelines for Email Messages

Guidelines for Mailing Lists

Guidelines for Consumer-friendly Websites

Guidelines for Safe Online Buying

Guidelines for Online Auctions