Executive Summary

E-Commerce is the general term for business conducted through the Internet. E-commerce can involve online banking, selling products and making purchases through Web pages, transferring funds, or any other monetary transactions conducted through electronic data interchange (EDI). E-commerce offers consumers a convenient, fast, easy way to conduct many financial transactions.

The bad news is that consumers face dangers while conducting business online. A consumer could fall victim to a traditional financial crime conducted through the Internet, such as fraud or theft, or consumers could become a victim of a cyberattack. The good news is that informed consumers can do a number of things to protect themselves.

The three major steps that consumers can take to protect their personal information and assets are:

- Choose reputable service providers
- Know the threats
- Control access to information and to the computer itself by following Best Practices

Making sound decisions, understanding the threat, and implementing basic security measures will protect the individual consumer and contribute to overall Internet security.

Best practices for computer security and online activity are:

Control Access to Your Computer
- Consider security before making online transactions
- Update operating systems and software regularly
- Use strong passwords, and change them often
- Lock down your system
- Disable all unnecessary services
- Use encryption to protect your communications
- Install and regularly update anti-virus software
- Use intrusion detection systems and firewalls

Control Access to Your Information
- Think about security before you act
- Be Concerned about “social engineering” tricks
  - Be cautious about the possibility of “spoofed” websites and e-mails
  - Beware of giving out your personal information
  - Know with whom you are working or conducting business
- Do not open suspicious or unknown e-mails
- Be cautious about downloading free software and programs
- Look for privacy and security policies

Following these practices protects the consumer’s E-Commerce transactions and helps prevent vulnerabilities that could be exploited to harm others.
Introduction

What is at risk when I conduct financial transactions with my computer?
If you are not protecting your information and transactions, you risk becoming a victim of a crime. Online financial transactions, such as paying bills or purchasing auction items, can be done securely. Most reputable financial institutions and e-commerce services have gone to great lengths to protect your data and transactions online, and many provide details of how this security is achieved.

The threats that online service providers face include:
- Vulnerabilities in their network may allow a hacker to gain unauthorized access and alter or damage systems;
- Hackers may exploit vulnerabilities in the Web page;
- Data transmitted (such as your credit card number) to their network may be intercepted or altered by hackers;
- “Denial of service” attacks, Web page defacements or other cyberattacks may disrupt normal service;
- One or more parties involved in a transaction may repudiate it, denying that it ever happened.¹

Criminals who manage to exploit these threats can steal account numbers, intercept customer information, or even steal money. Reputable service providers invest the resources to ensure that this will not happen.

Choosing reputable service providers is the first step to secure online transactions. The second step is to understand the threat. YOU NEED TO UNDERSTAND WHAT IS AT STAKE BEFORE YOU MAKE TRANSACTIONS. Just as you think about your safety and security when entering a bank to make a deposit, you need to think of information security before you make a transaction online.

The threats that you face include:
- Unauthorized access and control of your personal computer
- Theft of personal information such as social security numbers, account numbers, credit card numbers or other vital information

You could become a victim of identity theft, credit card theft, account theft, or even risk providing information about yourself to stalkers or other criminals. A hacker could gain control of your computer and alter or destroy your data and information. The attacker could use your computer to launch an attack against other computers. People are victimized in these ways daily. You need to make smart decisions about online transactions and take at least the minimum-security precautions in order to protect yourself.

The third step consumers can take is to follow best practices to control access to their information and control access to their computer.

Computers are new tools that can be used to commit old crimes. Criminals use computers to commit online fraud and theft, to gain unauthorized access to information, or to threaten someone’s personal safety and identity. Cyberstalkers use the Internet to find information about their victims. Extremist and terrorist groups use the Internet to spread propaganda or to recruit and organize new members. The Internet also provides access to bomb recipes, child pornography, and ‘how-to’ kits for easy hacking. Cyber attacks or information warfare can be conducted through a computer. Securing your computer is not only important to your financial and personal safety, but has also become a matter of national security.

The National Strategy to Secure Cyberspace draft calls for all Internet users to “secure the portions of cyberspace that they own or operate, because each user of cyberspace must play a role in securing it (NSSC, p. 1).”

**Who is at risk?**

If you are connected to the Internet, you are at risk.

The Information Technology and Service Alliance estimated in ‘The Digital Planet 2002’ that there are over 500 million Internet users throughout the world. Unfortunately, governments around the world are playing catch-up to write laws and regulations to mandate information security. In some cases, United States law cannot protect you from international criminals, and you must do your best to prevent crimes from occurring. Cybercriminals and cyber attackers are becoming more sophisticated, and the nation has become concerned that acts of cyberterrorism could cause great damage. The Internet and its increasing international use make it a prime concern for security experts in the United States.

No system connected to the Internet is perfectly secure. There are people out there right now working on new ways to breach computer security. Some want your money, some want your identity, and some want the resources on your computer. The people dedicated to protecting you ~ law enforcement officials and computer security experts ~ have come up with technologies and practices to help you protect yourself. One of the smartest decisions you can make about using the Internet is thinking about security first. Check out the security technologies available, new ones come out all the time, and read about protecting your identity and computer.

Many Internet users believe the myth “no one would want anything on my computer.” This is not true. Some hackers want your personal information and could break into your computer to find it. A hacker could break into your computer to access other secure networks (for example, your work network could be exposed if you log-in from home). If the hacker exploits the vulnerabilities of your computer, there is a chance he or she could get to your company’s sensitive information. If you have a computer connected to the Internet, a hacker may want to use your resources or launch an attack from your computer against another computer. For example, the Code Red worm infected a large number of computer users then used these infected

---

machines to launch a denial of service attack against the White House website. Other worms or viruses are programmed to delete files or overwrite your hard drive, and if you are infected, your financial information will be wiped out along with your other information. The recent Bugbear worm installs a “backdoor” that could allow an attacker into your computer, and allow the hacker to record anything you type into certain windows. Additionally, computer security experts from the Honeynet Project found that: “A common home user setup, with Windows 98 and file sharing enabled, was hacked five times in four days.” Unless you take steps to secure your system, criminals hiding in cyberspace will access your computer.

Best Practices: What can I do?

First, Choose Reputable Service Providers.
Computers are a big investment. When you think about making a big purchase, it is important to know that the equipment will work reliably, and that you can do things to improve the equipment as time passes. When you think about installing an operating system and application software, check out the vendors. Do they perform standard security checks before they sell the product? Are they able to respond quickly when a flaw is discovered in their product and release a fix for customers? Do they communicate with their customers about security flaws and how to fix them? Does the vendor provide clear instructions on how to make your Web browser more secure? If the answer is “No” to any of these questions, think about using a different product. On the same note, it is important to install security technologies to help protect your computer and your information. You will need to find anti-virus software, a firewall, and an intrusion detection system that work with your operating system. These technologies should help make your E-Commerce transactions safe.

Before you make a transaction online, check out the online service’s security features and policies. Does the service you wish to use provide a secure environment? Does it use encryption and make use of security technologies such as firewalls? Is your information protected? Is the banking institution FDIC insured? Most reputable financial institutions and e-commerce sites will publish their security precautions, and provide you with information to make a decision about whether or not to do business with them.

Consumers filed complaints with the FBI and the National White Collar Crime Center's Internet Fraud Complaint Center that totaled $17.8 million in 2001. Additionally, during the first half of 2002, the National Consumer's League's Internet Fraud Watch received complaints totaling $7.2 million. The National Consumer League (NLC) found that credit cards are "by far the safest

way to pay online...because your liability is limited to $50 under the Fair Credit Billing Act."\(^7\) Just as there are security technologies to protect your computer itself, some companies have made innovations in protecting your transactions. Some credit card companies offer "perishable credit cards" that provides a consumer with a specific credit card number for each online transaction or for a specific time period. Another security feature is to employ smartcard technology to deny unauthorized access to payment software on a PC.\(^8\)

### KNOW YOUR RIGHTS

**The Electronic Fund Transfer Act**
“The Electronic Fund Transfer Act provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers.”

**The Rights to Financial Privacy Act**
“The Right to Financial Privacy Act provides that customers of financial institutions have a right to expect that their financial activities will have a reasonable amount of privacy from federal government scrutiny. The Act establishes specific procedures and exemptions concerning the release of the financial records of customers and imposes limitations on and requirements of financial institutions prior to the release of such information to the federal government.”

You can read more about shopping online safely in the National Consumer League’s “NCL Warns Consumers: Don’t Get Scrooged Shopping Online This Holiday Season,” published 9 December 2002 and available online at [http://www.nclnet.org/holiday02.htm](http://www.nclnet.org/holiday02.htm).

### Second, Know the Threats.

**What do you have that a criminal or thief might want?**
In order to control access to your information and control access to your computer, it is important to understand the threats. Criminals are eagerly seeking your personal information (social security number, credit card numbers, bank account numbers, passwords to e-mail or shopping sites) and your computer resources. Do not make it easy for someone to steal from you. People with less than honest intentions can gather information over the Internet that can be used to steal your identity or financial assets. Criminals often use “social engineering” to trick people into sharing personal information.

---


E-mails, Web pages, and other forms of electronic communications that look legitimate and seem to be requesting legitimate information may in fact be the work of criminals trying to trick you into sharing your information. Another common social engineering trick is calling someone and pretending to be a network administrator. The criminal will ask for your password and give you some legitimate-sounding reason that he or she needs it. If a lady in a business suit with a clipboard said she needed to work on your computer, would you give her your password? Would you think to ask for identification? Or would you try to be as helpful as possible? This is how hackers conduct social engineering: they exploit your willingness to be helpful and polite.

If criminals use your computer to obtain your credit card numbers or trick you into giving away personal information, they may be able to make transactions (purchase things with your credit card, move money from your bank account) with your money. The Internet also provides an opportunity for criminals to disguise themselves and sometimes even remain hidden from law enforcement officials. It is possible to steal the identity of someone in Chicago while working at a computer in Moscow, and be long gone before anyone discovers the criminal activity.

Controlling access to your information means making smart decisions about the e-commerce institution you choose to do business with, and making smart decisions about sharing your information.

You will need information to make good decisions. Read the security features of the site. Find out what the site does to protect your information. Use a search engine like Google.com to look up information about the e-commerce business to see if they are reputable. Read the Federal Trade Commission’s “A Consumer's Guide to E-Payments,” it will help you make informed decisions about online transactions. The report can be found on the Internet here: http://www.ftc.gov/bcp/conline/pubs/online/payments.htm. It is also wise to read the Federal Trade Commission’s “ID Theft: When Bad Things Happen To Your Good Name,” it will help you understand how to protect yourself and what to do if you are a victim of identity theft. The report can be found on the Internet here: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.
Controlling access to your computer is equally important. Individual or groups of hackers have caused serious security breaches, spread viruses or worms, launched distributed denial of services attacks (DDoS), or used other tools of destruction to cause billions of dollars in lost time, business, or assets.

Additionally, you may store vital information such as account numbers, mother’s maiden name, or social security numbers on your computer. It is important to control access to your computer from unauthorized intrusions. If a hacker, or even someone who works with you, is able to read the files on your computer, will they be able to see your personal information?

SOCIAL ENGINEERING and SPOOFING

Social Engineering: this term refers to the deception skills often used to trick people into doing something (send money, open a worm-infected e-mail, tell their password or personal information).

Spoofing: the ability to make something (an e-mail, a Web page, etc.) look legitimate and reasonable to cover criminal or malicious intention.

One example of Social Engineering and Web Spoofing
The UK’s National Criminal Intelligence Service (NCIS) has shut down a website that appeared to be a legitimate UK bank. The site was created by conmen who used the fake bank accounts they created to trick people into sending them money. The visitors to the site were informed that if they would create a bank account to help move money out of Nigeria, they could have a share of the millions transferred. After signing up, the con artists asked for money to help bribe stubborn officials or for other reasons. Two people reportedly lost more than $100,000 after being conned by the fake website. See the October 8, 2002 BBC story, “Fake bank website cons victims” for more information. See the October 8, 2002 BBC story, “Fake bank website cons victims” for more information.
http://news.bbc.co.uk/1/hi/technology/2308887.stm

Third, Follow Best Practices.
You need to think about your personal information as an asset, something you take care to protect. While some people live in safe neighborhoods where it is not necessary to lock the door, in cyberspace where geography is not a deterrent, there is no such neighborhood. When you take steps to secure your computer, you help yourself and you are becoming a Good Internet Neighbor. For example, if you install anti-virus software and update it regularly, you are less likely to be responsible for spreading malware from your machine. If you install security technologies such as an intrusion detection system and patch your system as necessary, your computer is less likely to be compromised by a cracker and used in a distributed denial of service attack.

It is important to recognize that this new war on terrorism will require increased vigilance from everyone, particularly those who are entrusted with maintaining critical information assets. But each individual can participate, can be a Good Internet Neighbor, and can improve the overall security of our critical infrastructures. These basic steps will go a long way toward preventing successful cyberattacks.

---

CYBERATTACKS

Cracking: the ‘cyberattack’ process of exploiting vulnerabilities in software or the lack of security of computers or systems.

Viruses and Worms: sometimes referred to as ‘malware,’ viruses and worms are autonomous programs of malicious code that are programmed to exploit the vulnerabilities of specific operating systems. Once the malicious program has entered the computer, it may alter or destroy data, send itself to other computers, or cause other damage.

Trojan Horses: software that appears to have a legitimate purpose, but contains malicious programs (such as a virus or a backdoor).

Backdoors: programs that bypass security features (such as passwords) and allow an attacker access (most of the time through the Internet) into a computer system.

Distributed denial of service attacks: these attacks involve the coordination of many different, compromised machines to attack a website or computer system by flooding the resources of the machine with packets.

The best practices listed are the minimal steps you need to take to lock the door; also, best practices for secure computing are not specific to online transactions, but are important to follow as a standard practice. You need to have layers of security. The more layers of security you have, the safer your online transactions will be. You can begin by deciding to install security technologies, such as firewalls and anti-virus software, and to use strong passwords. You can educate yourself about threats from fraud and identity theft. These are the beginnings of following best practices.

**Follow Standard ‘Best Practices’ for Computer Security and Online Activity:**

**Control access to your Computer**

- Update your operating systems and software regularly: Many computer software products have flaws in programming language that may allow outsiders to enter without authorization; insiders to access restricted information for illicit purposes; or those skilled in breaking through programs to ‘hack’ their way into the sites or systems. Chances are, you own some of this software. You need to take the initiative to update your software and apply patches to the system. If you have a home network, it is important to keep all of the computers secure, not just the “important” ones. Your home network is only as secure as your least secure computer. Vulnerabilities are discovered daily, and you need to stay informed about the vulnerabilities that affect you. One good way to do that is to visit Carnegie Mellon University’s CERT Coordination Center for information about vulnerabilities and security concerns, [www.cert.org](http://www.cert.org).

- Use strong passwords: hackers can use automated cracking programs to identify your password. One such program runs through dictionary words to guess the password. Simple English words or combinations like ‘football’ or ‘Balletdancer’ are not good passwords and are easily cracked. Additionally, do not use passwords that are identifiable.

---

TOM RIDGE, Director of Homeland Security, said:

Protecting this infrastructure is critically important. Disrupt it, destroy it or shut it down, and you shut down America as we know it. This is an enormously difficult challenge because we must always remain one step ahead of the hackers.

to you, like the name of your dog or the date you were born. Use passwords that are difficult to crack and include combinations of letters (upper and lower case), numbers, and symbols. It is not a good idea to write the password down and put it somewhere anyone else can find (post-it notes on your screen or under your keyboard will definitely not do), and do not save them on your computer. This may be convenient, but it increases the chances of someone finding your passwords and gaining access to your private information. If you need a clue about your password, write down a statement or a question that will help jog your memory about the password. Change passwords often, and use different passwords for different devices and applications. If someone can crack your password (or look over your shoulder and watch you type it), you will need the extra layer of security that having different passwords may give you. For example, make sure you have different passwords for your logon and for your e-mail; if someone gets the password to your computer, they will not be able to logon to your e-mail account. To read more about passwords, see Iain Thomson, “Passwords too easy to crack,” VNUnet, 13 December 2002. Retrieved 13 December 2002 <http://www.vnunet.com/News/1137600>. Another good article about passwords is, Rob Lemos, “Hackers can crack most in less than a minute,” C-Net News 22 May 2002. Retrieved 10 October 2002 <http://news.com.com/2009-1001-916719.html>.

- ‘Lock down’ your system: it is important to physically restrict access to your computer from unwanted users. No computer security technology in the world will help if someone can walk in the front door and steal your machine. When you leave your computer on, un-locked, and walk away, you risk any passer-by accessing all of your information. Remember to secure all of your devices as well, for example, if you do not have password protection on your palm pilot, you risk someone using this device as a “backdoor” to get to your information. You can read more about security mistakes in Alan S. Horowitz, “Top 10 Security Mistakes,” Computer World 9 July 2001. Retrieved 10 October 2002 <http://www.computerworld.com/securitytopics/security/story/0,10801,61986,00.html>.

- Disable all unnecessary services: Disable the file-sharing options for your software, especially if you use Microsoft software, as it creates a vulnerability that may expose these files to unwanted access. Disconnect from the Internet when you are not online. High-speed, always-on Internet connections are fast and convenient, but without security, this service is like leaving your car running with the door unlocked at a car thief convention. You leave yourself open to cyberattack if you allow file-sharing and remain always-on. Not only is your personal information exposed, but leaving your computer open places your Internet neighbors at risk because your computer could be used by a hacker to attack other systems. A hacker can break into your computer, and with your fast and always-on connection, can launch attacks or let worms loose from your computer. There are many good references on computer and network security in the SANS Reading Room. Three good examples are: Barry Dowell, “Basic Self-assessment: Go Hack Yourself,” SANS 11 September 2001. Retrieved 10 October 2002 <http://rr.sans.org/securitybasics/hack_yourself.php>; Alan Davies, “Security from Scratch …How to Achieve It,” SANS 4 September 2001. Retrieved 10 October 2002 <http://rr.sans.org/securitybasics/scratch.php>; and Lyde Andrews, “OK, So I Need Security. Where Do I Start?” SANS 28 August 2001. Retrieved 10 October 2002 <http://rr.sans.org/securitybasics/need_sec2.php>.
• Use encryption to protect your communications: this technology will protect your e-mails or other transactions from uninvited eyes. Even if a hacker intercepts an encrypted communication, it is highly unlikely that he/she will be able to read it. For background information about encryption, see Melis Jackob, “History of Encryption,” SANS 8 August 2001. Retrieved 10 October 2002 <http://rr.sans.org/encryption/history.php>. Information about encryption for e-mail can be found, Neil Lindberg, “Email – Exploring The Encrypted Solution,” SANS 4 October 2001. Retrieved 10 October 2002 <http://rr.sans.org/encryption/email_solution.php>.

• Install and regularly update anti-virus software: it is important to install anti-virus software to protect your computer from worm or virus “infection.” Some worms can affect the smooth running of your computer, while some damage or destroy files and applications. Worms and viruses can spread in a number of different ways, including through e-mail, through malicious Web pages, through instant messaging services, through file-sharing services, and others. Installing anti-virus software will help protect you against damaging worms and viruses. It is also important to regularly update your anti-virus software. These software vendors create “definitions,” or a list of known worms, and will inform you when a known worm is detected. Virus and worm writers release their malicious code on a regular basis, and anti-virus software vendors update their definitions to protect your system against these new worms. If you do not update this software regularly, you will not be protected against malicious programs like worms and viruses. See the Carnegie Mellon CERT Coordination Center resource called “Home Computer Security” <http://www.cert.org/homeusers/HomeComputerSecurity/> for more information.

• Use intrusion detection systems (IDS) and firewalls: intrusion detection systems and firewalls will help protect your computer from unauthorized access. These technologies will restrict suspicious incoming (and outgoing in some cases) traffic. While cost considerations are important, not taking the proper steps to secure your information and computer could result in a much greater loss than you would have spent on security technologies. Preparation and prevention will pay off in the long run. See the SANS reading room for articles on Firewalls & Perimeter Protection, <http://rr.sans.org/firewall/firewall_list.php>, and Intrusion Detection, <http://rr.sans.org/intrusion/intrusion_list.php>.

**SECURITY MEASURES**

Passwords: many computers require log-in passwords that ‘authenticate’ a user and allow that person to use the resources of the computer if they can provide the correct password that matches the log-in or user name.

Encryption: the process of translating human readable text or data into secret code by using an encryption algorithm. Encryption can be used to secure data in a financial transaction.
Control Access to your Information

- Think about security before you act: Your personal information is a critical asset. Your social security number, bank account information, credit card, or other financial information could be used by another person to steal your identity, money, or cause damage to your reputation and credit history. Theft of this information is becoming more common as people connect to the Internet without taking security precautions to protect themselves. Worse yet, if your personal information is insecure and open to random theft, how much more vulnerable are you if you leave it open to someone who is targeting you specifically? There has been an increase of cyber-stalking and use of the computer to help commit more traditional crimes, and controlling access to your personal information may be a matter of personal safety, not just financially important.

  - Be cautious about the possibility of “spoofed” websites and e-mails: hackers are sometimes able to make an e-mail appear to be from someone, or somewhere legitimate. An e-mail could arrive in your in-box and look like it is from your software vendor, your boss, or your bank. A Web page could appear just like the online auction site you like to use. Sometimes, this is a trick: the e-mail or website may actually have been created by a hacker to trick you into telling him/her your password or other important information. Viruses can be spread in this way, including the recent W32.Gibe@mm worm that arrived through e-mail and appeared to be from Microsoft warning of a security patch, but would install a backdoor in a user’s system if they opened the attachment.
  - Beware of giving out your personal information: the old saying “it looks too good to be true” should be a warning. When you are deciding whether to participate in a survey or provide your information, ask yourself what the company/person could want with the information. Is your personal information going to be sold to...
marketing companies? Are you providing a hacker with your billing address and credit card number? If you did not initiate the transaction, be especially cautious of giving out any information.

- Know with whom you are working or conducting business: check out the e-commerce business or financial institution’s reputation and legitimacy before you initiate a transaction. Is this business or person trustworthy?

- Do not open suspicious or unknown e-mails: delete unwanted or suspicious e-mails. One of the most common ways worms and viruses are spread is through e-mail. It is important to be cautious of e-mails that do not come from trusted sources, and never open attachments from unknown or unsolicited e-mail addresses.

- Be cautious about downloading free software and programs: some free software programs are legitimate and are very useful. Open source firewalls and intrusion detection systems are two examples of very useful free software that serve legitimate purposes. However, some free software programs, including downloadable games and file-sharing software, contain “spyware” or “adware.” Spyware installs itself, generally without your permission, on your computer, monitors your Web browsing habits or information on your computer, such as credit card information, and reports this data back to a third party. Adware is software that monitors your Web browsing habits, reports the information back to a third party, and uses this information to generate advertisements that target your habits. To read more about Adware and Spyware, see: John Borland and Rachel Konrad, “PC Invaders, They’re camping out in your hard drive -- with your express consent,” C-Net News 18 April 2002. Retrieved 10 October 2002 <http://news.com.com/2009-1023-885144.html>.

- Look for privacy and security policies: before you make a financial transaction online, make sure that your privacy is protected and that security measures have been taken. Do not take it for granted that your information will not be used for purposes other than those you intended. Sometimes you will need to “opt-out” of having your information sent to marketing partners or receiving unwanted mail.

These suggestions are not new, and there are many resources and software products that can help. However, there is no magic security solution to turn your computer into a fortress. The best you can do is try to understand the risks, and then decide which risks are worth taking and how you can minimize your risks.

Here is a quick reference on possible vulnerabilities and mitigation strategies:

**Vulnerability: Unauthorized access to your computer**
- Install a firewall
- Install an intrusion detection system
- Update your software regularly and apply any security patches that are available
- Disable unnecessary services
- Use strong passwords
- Think about the physical security of your computer

**Vulnerability: Worms, viruses, and Trojan horses**
- Install anti-virus software
Update anti-virus software regularly
Think twice about downloading free software such as games or file-sharing software
Do not open e-mails from unknown sources
Do not open suspicious e-mail attachments
Remember that viruses and worms can spread through instant messaging services and file-sharing services

**Vulnerability: Adware and spyware**
Think twice before downloading free software such as games or file-sharing software
Read the fine print in the agreement before installing such software and be sure you are not agreeing to download adware or spyware

**Vulnerability: Identity theft**
Do not give out personal information such as your mother’s maiden name or social security number to unfamiliar sources
Beware of scams and spoofed e-mails and websites, if you did not initiate contact, think twice about giving out any information

**Vulnerability: Making online financial transactions**
Choose reputable service providers
Use a credit card rather than checks, money orders, or a debit card as consumer liability is more limited with credit card use
Use a provider who offers encryption when transmitting financial or personal data
Look into use of other security technologies

**Vulnerability: Social engineering**
Confirm the identity of someone before you offer him or her your personal or financial information; do not be fooled by someone claiming to be your company’s network administrator or your Internet service provider
Confirm the validity of any request for personal or financial information

**Resources and Further Information**

**Online Resources:**

- **Tech Talks** - [http://www.staysafeonline.info/techtalks.adp](http://www.staysafeonline.info/techtalks.adp)
- **Protect Your Computer, Protect Your Country's Cyber-Infrastructure** - Link available on the Tech Talks Page
- **FDIC (Federal Deposit Insurance Corporation)**
  - **Safe Internet Banking** - [http://www.fdic.gov/bank/individual/online/safe.html](http://www.fdic.gov/bank/individual/online/safe.html)
  - **Correcting Problems and Errors** - [http://www.fdic.gov/consumers/consumer/information/shoppot.html](http://www.fdic.gov/consumers/consumer/information/shoppot.html)
- **American Banking Association** - [http://www.banking.com/aba/](http://www.banking.com/aba/)
Investigative Research for Infrastructure Assurance (IRIA) Group –
Institute for Security Technology Studies

More Consumer Tips to Avoid Becoming a Victim of Identity Theft - 
http://www.aba.com/Consumer+Connection/idtheft_moretips.htm

The Federal Trade Commission enforces federal antitrust and consumer protection laws. The Bureau of Consumer Protection works to protect consumers from unfair, deceptive, or fraudulent practices. They provide information on several topics including e-commerce and the Internet: http://www.ftc.gov/bcp/menu-internet.htm


TransUnion - http://www.transunion.com/index.jsp - Order a Credit Report -- $9.00, most states, fees will vary by state of residence.

Current Vulnerabilities and Cyber Security Information:

National Infrastructure Protection Center - http://www.nipc.gov/
The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response.

Internet Storm Center - http://isc.incidents.org/
SANS - http://www.sans.org/top20/
SANS provides their “Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts’ Consensus”

The Institute for Security Technology Studies provides a daily news summary of on cybercrime, cyberterrorism, malware, vulnerabilities and other information security issues.

The CERT® Coordination Center provides “Home Network Security” with a valuable discussion of risks and ways to protect yourself while online.

Appendix 1~ Case Studies: Cyber Events and Incidents that Have Affected the Financial Sector

CASE STUDY I: USER ERROR
User actions can have a damaging effect on the financial sector. In one such incident, it was suspected that huge fluctuations in the London Stock exchange market were caused when a bank employee trying to post one large transaction, posted it three times. This type of incident is uncommon, but the important point is that human errors do occur, and monitoring any accounts and credit cards for mistakes is a smart user practice.

~A twenty-minute burst of activity in Britain's 100 biggest companies stock market resulted in £3.2bn worth of shares changing hands. The FTSE 100 blue chip index experienced its record
busiest trading day on September 20, 2002. It is possible that a trader mistakenly entered a £1.2bn order two or three times into his bank's dealing system, and the resulting volume of trading pushed the system almost to collapse. Regardless of the cause of the initial swell, as the market gained 250 points, the rise caused “computer systems across the City to begin automatic trades, which in turn exacerbated the market movement.” The London stock exchange, however, stated that the volume of business did not overwhelm the systems, and the bank in question denies that a mistake in posting occurred. There have been other incidents of stock market fluctuation due to human error, such as a different London Stock Exchange incident when someone mistakenly posted a £300m trade instead of a three million pound trade.


CASE STUDY II: SEMANTIC HACKING

You need to be aware that people are manipulating information for their own personal gain. The Internet is a convenient way of finding news and information, but it is also full of scammers and schemers trying to make a profit. It is important to “consider the source” before you make decisions about investments and spending money. Are you reading about stock trends from a reputable news source or a financial analyst, or has the information you are reading been released for someone’s own personal gain. The following is an example of using misinformation to affect the financial sector:

~The British Columbia Securities Commission barred from trading an accounting student who made false claims in an Internet chat room to boost stock prices. The commission was alerted to Jesse J. Hogan's 'pump and dump' scheme by the U.S. Securities and Exchange Commission. Hogan argues the electronic bulletin boards he used “warned readers not to believe much of the information they were reading.” He purchased shares in five U.S. tech firms and posted hundreds of anonymous Internet messages stating the companies were going to be purchased by well-known firms. He made $42,000 on the scheme, but has had to give up the profits and has been fined C$25,000.


CASE STUDY III: IDENTITY THEFT

Meridien Research estimates that identity theft will cost banks $8 billion a year by 2006. What that means to you is: more and more people are becoming victims of identity theft. The Federal Trade Commission has provided excellent resources to learn more about identity theft and how you can protect yourself. The FTC asks: “How can someone steal your identity? By co-opting your name, social security number, credit card number, or some other piece of your personal information for his or her own use. In short, identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft.” Read more about identity theft here: http://www.consumer.gov/idtheft/.

The Federal Trade Commission warns of a scam involving someone claiming to be an official and soliciting personal information, “E-Mail from Bogus FTC Investigator Sought Personal Data.” In this case, the FTC investigated a man who pretended to be one of its own employees, and e-mailed hundreds of victims of another scam asking for personal information that could be used as evidence in the investigation.


CASE STUDY IV: ADWARE HIDDEN IN AN E-CARD
Users should be wary of downloading free software. In the following example, Canada-based Cytron Communications Ltd. tricked users into downloading free software to view an electronic greeting card that they supposedly received. The free software does not help a user read the e-card, it is an adware program.

A new Trojan horse program named “Cytron” uses social engineering techniques to appear legitimate to unsuspecting users. An e-mail that appears to be egreetings@yahoo.com (forged address) arrives in the user inbox, and if they open the link to surprisecards.net (sounds legitimate) they are asked to install an e-card viewer plug-in in order to view a card waiting for them. When the ActiveX control is installed, signed with a credibility boosting digital certificate, users begin receiving racy pop-ups ads for adult websites. The user never does get a greeting card. The Trojan horse program then scans the websites the victim is viewing for key phrases like "hard core" and then serves pop-up ads based upon a phrase-matching algorithm. Even though the user has chosen to install the plug-in, "it could still be illegal under the Computer Fraud and Abuse act," says Jason Catlett of anti-spam company Junkbusters. The plug-in has been associated with the Internet porn company, Cytron, which also owns the domain name surprisecards.net.


CASE STUDY V: SOCIAL ENGINEERING
The following case study is an example of “social engineering” used by those seeking to steal identities. Identity theft scammers have a new venue for mining personal information: resumes and data from online job services. A job posting to Monster.com appeared to be from a legitimate company, Arthur Gallagher. One man applied online for the position and was contacted and asked to provide personal information for the necessary background check. The man complied. He provided his social security number, date of birth, mother's maiden name, a four digit number to be used as a password (which scammers may have assumed would be the same number their targets use as their pin number or password), and other vital information to the personal address of a man claiming to be a human resource director, Levinski. When the job posting disappeared from the site, the man called Arthur Gallagher and was informed that there was no Levinski at the company. The FBI and several state law enforcement authorities are investigating the incident, which was reported a few times to Arthur Gallagher. Experts recommend that online job applicants be extremely wary about providing personal information to
any website, and many fear that as national unemployment rates are 5.7 percent, unemployed applicants will be willing to comply with many requests for information in the hope of getting a job.