AIER | Economic Bulletin

AMERICAN INSTITUTE *for* ECONOMIC RESEARCH www.aier.org Vol. L, March 2010

How to Avoid Internet Fraud

Scammers use the Internet to generate nearly two-thirds of reported frauds. But a little knowledge can go a long way to protect yourself from becoming a victim.

by Kenneth D'Amica, Research Associate

Experts estimate that 200 billion spam e-mails are sent everyday. This is more than 80 percent of all e-mail and more than 100 spam e-mails per Internet user every day. Not all spam contains scams and malicious software, but many do. Scammers no longer have to pay postage; using the Internet they can target millions of people indiscriminately. The anonymity of the Internet also allows scammers to pose as trusted companies, strangers in need, or even friends.

Despite numerous available protections, increasing security efforts, and government agencies devoted to thwarting Internet criminals, hundreds of thousands of Americans are the victims of Internet fraud each year. In 2008, almost two-thirds of the 1.2 million frauds reported to the Federal Trade Commission's *Consumer Sentinel* were initiated via the Internet, mostly through e-mail but also from websites and ads.

Since so many are targeted at once, only the unsuspecting and unprepared become victims. With a little knowledge and a few precautions and protections, Internet users can guard themselves against most cyber thieves and Internet fraudsters.

A cyber thief is not necessarily concerned about the assets of any individual victim. His crime is carried out on such a large scale that even if there is only $50 in your bank account, he is taking money from enough people to make it worth his while. In many instances, a thief won't even use your stolen account information to pilfer your account; he sells it to others who will. Credit card numbers and online banking passwords can be purchased online for a pittance. Stolen credit card information usually sells for between 40 cents and $20 per account, although more complete information can cost thousands.

One important way of protecting yourself online is to safeguard your computer against hackers and viruses that can hijack your computer.

Many frauds are merely updated versions of age-old scams, the most notorious of which is the Nigerian letter scam. In this classic fraud, a person claiming to be a Nigerian prince asks for a sum of money that will enable him to move a large fortune with which he must part for an unknown or fictitious reason. The scammer then promises the sender a large percentage as reward.

The average victim is defrauded out of tens of thousands of dollars after the scammer has convinced him to send larger and larger sums needed to enact the trade, and some have reported losses totaling in the hundreds of thousands. There are some cases where the victim traveled to Africa only to be kidnapped by the fraudsters. In other similar frauds, victims are told of a fake inheritance or that they have won a foreign lottery. The total loss from the Nigerian scam and its many variations is estimated at more than $100 million annually.

The Internet also has facilitated many instances of identity theft, which in 2008 affected almost 10 million Americans and cost $48 billion. However, only one out of every ten victims had their identity stolen via the Internet. Stolen wallets and personal documents remain the most popular means of identity theft.

One important way of protecting yourself online is to safeguard your computer against hackers and viruses that can hijack your computer, not only stealing your information but also using your machine to send more viruses and fraudulent e-mails. Below is a list of steps that can minimize the risk of your computer becoming hijacked.

Regularly update your software. The most common way for malicious software to enter a computer is through flaws in computer programs. Programmers routinely make mistakes or fail to see flaws in their code, which means that software must be updated regularly in order to prevent attacks that exploit these flaws.

Many programs can be set to update themselves automatically as newer versions become available. The Windows operating system can be set to do so using Windows Update. On Apple computers, updates can be installed by clicking Software Update in the Apple menu. Other programs, such as web browsers, word processors, and media players usually can be set to automatically update somewhere in the program's menu bar, under Options, Settings, or a similar heading.

Use an anti-virus program. When malicious software is installed on a computer, it often has clever ways of hiding itself, making visual detection difficult. Anti-virus programs contain a list of known viruses, and scan the computer to find and eliminate them. More so than other programs, anti-virus software must be updated regularly in order to be effective.

New computers often include anti-virus software with a trial subscription to receive free updates. Many people fail to renew their subscription after the trial period lapses, making their computers vulnerable to new viruses. To avoid this risk, either renew your subscription or download one of the many free anti-virus programs available online. If you do install a new anti-virus program, make sure to uninstall the old one.

Many people buy Apple computers with the assumption that they are safer and more secure than PCs. While that may seem to be true, most computers run Windows, so virus writers target them to maximize their reach. As Apple computers become more and more popular, the number of viruses written to target them is likely to increase.

If you notice your computer slowing down or acting strangely, it is a good idea to run an anti-virus program immediately. All of the types of software mentioned here can be safely downloaded from sources such as download.com and filehippo.com. The software found on these websites is guaranteed to be virus- and malware-free.

If your computer is acting strangely, it is a good idea to run an anti-virus program immediately.

Use an anti-spyware program. In addition to viruses, software flaws can be exploited to install what is known as malware or spyware. While not always directly related to illegal activity, malware can expose your computer to additional risk while slowing down your computer, creating errors, and generating pop-up ads that may lead to dubious websites.

Like anti-virus programs, there are many effective anti-spyware programs available online. If your computer is slow and your virus scanner fails to find any infections, it is likely that one of these programs will uncover hidden malware. Keeping an anti-spyware program updated and using it regularly is a vital part of maintaining a computer.

Use a firewall. A firewall prevents unauthorized connections from reaching a computer. Most operating systems have a built in firewall, and you should make sure you have one enabled.

Use strong passwords. A study of password habits showed that 20 percent of all passwords come from a list of 5,000 possibilities, the most popular of which is "123456." When a computer is attacked, the assailant can attempt thousands of passwords per second, sometimes spanning a whole dictionary.

For important accounts such as banking or e-mail, passwords should be longer than six characters and contain a mix of letters and numbers. Avoid simple words, and include numbers in the middle of words to make guessing more difficult. One good technique is to create acronyms based on phrases or song titles that can be easily remembered.

When writing passwords down, it is important that they be stored in a place that is not easily located or accessible. Ten percent of all identity theft is perpetrated by someone the victim knows. It is best not to write them down at all.

Use e-mail scanning. Outlook and similar programs download e-mails onto your computer before you read them, so make sure your virus scanner scans all incoming e-mail. Even if you don't open any attachments, your computer can be infected by a virus embedded in a graphic just by displaying the e-mail.

An alternative is to use a browser-based e-mail service, such as Gmail. This way, attachments are not downloaded directly to your computer unless done manually. Such services have built-in virus scanners that will prevent users

Reported Losses of Internet Crime

Year	*Millions*
2001	$18
2002	54
2003	126
2004	68
2005	183
2006	198
2007	239
2008	265

Source: Internet Crime Complaint Center.

from downloading viruses. Many are adept at filtering out most fraudulent e-mails altogether, though some still get through.

Turn off your computer when it is not in use. By keeping your computer connected to the Internet at all times, the risk of a malicious attack is increased.

While many attacks target technical flaws and vulnerabilities, the most dangerous and effective type of attack targets the victim directly through e-mail, ads, or websites. Many scams and frauds are designed to appeal to a person's emotions, while others present victims with an opportunity to make money with relatively little work by letting them in on an exclusive deal.

However, with a little bit of awareness and a healthy amount of suspicion, anyone should be able to know a fraud when they see one. You can protect yourself from many threats through caution and know-how. (If you do receive a scam e-mail, be sure to forward it to SPAM@uce.gov. The FTC investigates scammers and educates the public on what to watch out for.)

If it sounds too good to be true, it is. While just about anyone would like to become instantly rich through some lucky event or opportunity, it almost never happens. Long before the invention of the Internet, scammers have tricked people into believing they were being let in on an exclusive deal and that a minimal investment would yield large returns. By using e-mail, these scams have been deployed on an unprecedented level. If just one in many thousands of people is tricked, the scam will have paid off.

Many scam e-mails contain numerous spelling and grammatical errors, which should be an immediate warning sign. Some, however, look very official. The scammer may include a fake address and credentials, and the letter may be well written or even eloquent. But regardless of presentation, unsolicited e-mail offers are almost uniformly fraudulent.

There are many types of frauds being perpetrated on the Internet. In addition to the Nigerian letter, foreign lottery, and inheritance scams, scammers often use phony job offers and advertisements for products, usually cheap pharmaceuticals. There are even cases of scammers developing online friendships through dating and social networking sites only to trick the victim into giving them money by claiming to have had some personal catastrophe.

Be wary of impersonators. Another popular way of gaining a victim's trust is to pose as a well-known organization or as someone the victim knows.

In the first case, the e-mail or website will be designed to look like that of the trusted organization. One way of discerning a fraud is to look at the address from which the e-mail was sent. If the part after the "@" and before the suffix, called the domain, is not that of the organization, then the e-mail is fraudulent. For instance, a scammer could send out a message claiming to be from AIER, using the address offers@aier.badguy.com. While the name of the organization is included in the address, it is only the part directly preceding the suffix (.com, .org, .co.uk, etc.) that matters.

Even this way of checking, however, may not be enough. Frauds get more sophisticated all the time. If an organization initiates contact with you, it is best to go directly to their website by typing in their web address or using a search engine rather than following the link provided. Be aware that links can be made to look as though they are directing you to a legitimate site but actually bring you elsewhere.

The most common instance of this is phishing, where someone posing as a bank or other organization sends an e-mail asking for a username and password. They often claim that something bad will happen if the person does not comply or that it is for maintenance or an upgrade. **No legitimate organization will ever ask you for your password.** Any e-mail that asks for your personal information comes from a malicious source.

In addition to impersonating organizations, e-mails can be sent through hijacked accounts, often contacting everyone in the infected account's address book. If you receive an e-mail from someone you know directing you to an unknown website or with an unknown attachment, it is possible that their account has been compromised and that your computer will be infected by opening that

This Fraud Can Kill

More than two-thirds of all spam contains advertisements for cheap pharmaceutical products claiming to come from Canada or the European Union. These companies are actually based in Russia and use fake logos and phony credentials in order to appear legitimate. Many claim to be certified by the American Drug Administration, a nonexistent institution, or sponsored by the magazine Men's Health. The drugs they offer are often dangerous. In many cases, the product is a placebo made to look like the real thing, but it can also contain the active ingredient in doses very different from that which is advertised. In any case, the drugs offered can be fatal.

attachment or visiting that link.

One should also be wary on social networking sites such as Facebook or Myspace. Accounts on these sites can be hijacked by hackers, who post cries for help or send scams. In one particularly successful scam, the hijacker claims that they have been robbed while traveling abroad and asks friends to wire money.

People you know may be unwittingly spreading computer viruses. Many people put the security of their friends and family at risk by spreading chain e-mails that contain pictures and videos. While the videos may play and the pictures may be funny, they often have viruses embedded in them. Under no circumstances should these chain e-mails be opened or forwarded.

Only download programs from well-known and trusted sources. Many programs found on the Internet are bundled with malware or other forms of annoying and invasive software. Be suspicious of screensaver bundles, file sharing programs, and toolbars. Even if they do not explicitly contain malware, they can slow down your computer significantly.

Never reply to unsolicited e-mails. If you recognize an e-mail as a scam, you may be tempted to reply. This is a mistake. The e-mail will let the sender know that his message is reaching someone and being read, and your address will be put on lists to receive even more spam e-mails. Never respond to e-mails from unknown sources.

Be careful when using public computers. There is no way of telling what kinds of malware are installed on public computers in places such as Internet cafés and airports. Most of the time imprudent guests will have installed it accidentally, but deliberate installations by scammers is not impossible. Even in the absence of malware, strangers can access user information in a public computer's temporary files, which are less temporary than one would think. In addition to viruses, malware can install keyloggers. These record every keystroke and mouse click on the computer and transmit personal information to remote computers used by scammers.

To protect yourself, avoid using public computers for tasks that require personal information such as credit card numbers. If you do enter a password, make sure that you've disabled any automatic login features as these will save your login information. When you are done, remember to log out.

In addition, always be aware of low-tech threats. An overcurious neighbor can be just as dangerous as any malware. Computer security software means nothing to the skilled thief who watches you type your password.

When using a public (or private) wireless connection, make sure that any website that requires personal information is encrypted. An encrypted website will have "https" instead of "http" at the start of the address.

All this may seem like a lot to remember, but with a little mindfulness you will start to spot the scams as they come, and these rules will become second nature. The time spent learning to protect your computer will be less than what you would spend waiting for an infected computer to load web pages, and far less than the time it takes to sort things out after being the victim of an Internet scammer.

Computer Repair 101

Many people think of their computers the same way they think of their car in that when something seems wrong, it is best to bring it to a repair person. With computers, however, many of the tools needed to repair it are freely available online. Most unexplained problems can be solved simply by updating and running anti-virus and anti-spyware programs.

If you get an error message when you start your computer or run a program, you can find out how to fix it by typing the exact message into a search engine. If you are seeing a message, chances are that others have had the same problem and sought online help.

For instance, suppose you are a Windows user and that when you turn on your computer a box appears saying, "The file 'program.dll' could not be found." Instead of clicking "OK" and ignoring it, type the exact message into a search engine. Your search will turn up a number of online forums, such as Techsupportforum.com, that offer free technical help. You'll find that someone has asked the web experts about this error, and they will have offered a step-by-step solution. If Microsoft turns up in your search, they likely also will have step-by-step instructions on how to proceed.

When seeking advice, you may see offers for free software that claim to fix or clean up your computer. Do not download these; they often contain spyware or other unwanted software.

Many problems, of course, require more technical knowledge and may not be so easily solved, but by learning a few tricks you can save time and money.

Economic Bulletin (ISSN 0424-2769) (USPS 167-360) is published once a month at Great Barrington, Massachusetts, by American Institute for Economic Research, a scientific and educational organization with no stockholders, chartered under Chapter 180 of the General Laws of Massachusetts. Periodical postage paid at Great Barrington, Massachusetts and additional offices. Printed in the United States of America. Sustaining memberships: $59 per year. POSTMASTER: Send address changes to ***Economic Bulletin***, American Institute for Economic Research, Great Barrington, Massachusetts 01230.