



Protect Your Personal Identification

DANVERS POLICE BENEVOLENT ASSOCIATION

Investment Scams - Identity Theft - Telemarketers Foreign Lottery - Internet Fraud

Listed are a number of web sites to help you protect your
Identity, credit report, and more

If It Sounds Too Good To Be True, It Probably Is!

- MA Attorney General's Consumer Guide to the Internet
<http://www.ago.state.ma.us/filelibrary/internetguide.pdf>
- MA Attorney General's Office on Canadian Telemarketing Scams
<http://www.ago.state.ma.us/sp.cfm?pageid=1607>
- Identity Theft Information
<http://www.ou.edu/oupd/idtheft.htm#INTRO>
- Elderly Targeted In Investment Scams
http://www.usatoday.com/news/nation/2003-09-04-seniors-scammed_x.htm
- Shunning Spam
<http://www.cbsnews.com/stories/2003/07/10/sunday/main562630.shtml>
- How To Tell If You're A Victim of Identity Theft
http://www.usatoday.com/money/perfi/credit/2003-03-06-identity-theft-signs_x.htm
- Nigerian Scam Defined
<http://home.rica.net/alphae/419coal/>
- Nigerian Fraud Email Gallery
<http://www.potifos.com/fraud/index.html>
- Foreign Lottery Scam
<http://www.cbsnews.com/stories/2002/12/13/eveningnews/main533033.shtml>
- National Check Fraud Center
<http://www.ckfraud.org/identity.html>

- Get Real or Get Taken
<http://www.bep.treas.gov/cd042500/start.html>
- International Lottery Scams
<http://www.ftc.gov/bcp/online/pubs/alerts/intlart.htm>
- Federal Trade Commission Consumer Alerts
<http://www.ftc.gov/ftc/consumer.htm>
- Massachusetts General Law – False Impersonation and Identity Theft
<http://www.mass.gov/legis/laws/mgl/266-37e.htm>
- National Fraud Information Center
<http://www.fraud.org/>
- Identity Theft, Forgery and Other Fraud
<http://www.preventcrime.net/fraud.htm>

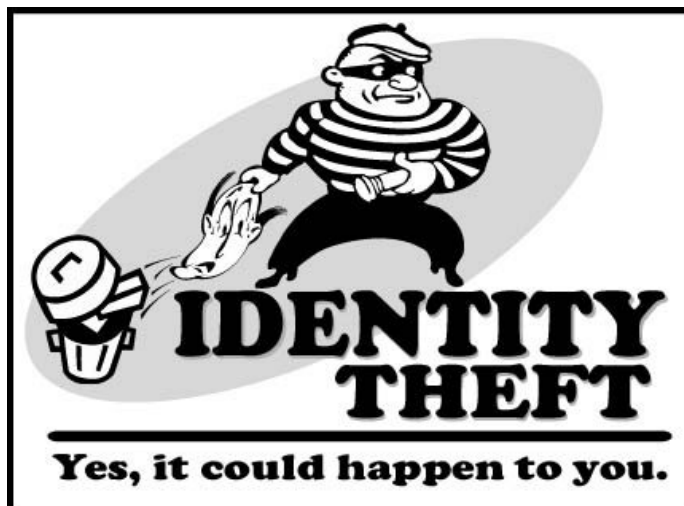
People who believe they may have been victims of identity theft are advised to contact:

**Federal Trade Commission at 1-877-IDTHEFT
In Massachusetts - State Attorney General's hotline 617-727-8400.**

CREDIT REPORTING AGENCIES

- TRANS UNION – <http://www.tuc.com>
- EQUIFAX – <http://www.equifax.com>
- EXPERIAN – <http://www.experian.com>

Federal Trade Commission – Your National Resource About ID Theft
<http://www.consumer.gov/idtheft/index.html>



What to Do If Your Identity Is Stolen

Contact all 3 principal credit reporting agencies

Report the theft of your cards

Ask to flag your account

Ask to contact you by phone, writing, or fax before approving any credit request

Ask the credit bureau for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information

Contact all creditors with whom your name or identifying data may have been used. This includes all credit cards, department stores, loan agencies, etc. You may be asked to fill out affidavits stating that it was not you who made the purchases

Contact your local police department and file a police report

Contact the Department of Motor Vehicles to see if a license was issued in your name. Ask them to put a fraud alert on it and you may need to change your license number

Never pay or partially pay any portion of a bill that is a direct result of identity theft

Get a copy of all fraudulent applications and contracts

Keep a log of all contacts with law enforcement and financial institutions



Protect Yourself from Identity Fraud

Purchase a crosscut paper shredder and shred all personal information before throwing it away

Protect your personal data. Watch what you throw in the trash

Be careful of shoulder surfers while using ATM's and phone cards

Mail bills at the post office or use locked mailboxes

Cancel all credit cards that you no longer use

Empty your wallet of all extra credit cards

Do not carry your Social Security card, birth certificate or passport

Never give your credit card number or personal information out over the phone unless you initiate the call and know the person or business

Do not put your Social Security number, telephone number or any unnecessary information on your checks or credit receipts

Monitor your bank and credit card statements for any irregularities

Establish an unlisted telephone number or use an initial instead of your full name

Have your checks sent directly to your bank and pick them up yourself

Do not use your Social Security number as a license number

Request a state assigned number from your Department of Motor Vehicles

Passwords and PIN's - Do not use the last 4 digits of your Social Security number or date of birth
Use fictitious names or non-consecutive number sequences

Remove your name from promotional lists



Phishing



Phishing is e-mail fraud where the perpetrator sends out legitimate-looking e-mails that appear to come from well known and trustworthy Web sites in an attempt to gather personal and financial information from the recipient. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.

Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims. In one fairly typical case before the Federal Trade Commission (FTC), a 17-year-old male sent out messages purporting to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the "AOL Billing Center" link, however, they were taken to a spoofed AOL Web page that asked for personal information, including credit card numbers, personal identification numbers (PINs), social security numbers, banking numbers, and passwords. This information was used for identity theft..

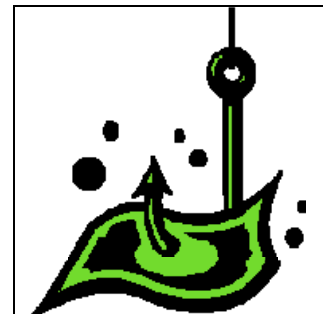
The FTC warns users to be suspicious of any official-looking e-mail message that asks for updates on personal or financial information and urges recipients to go directly to the organization's Web site to find out whether the request is legitimate. If you suspect you have been phished, forward the e-mail to uce@ftc.gov or call the FTC help line, 1-877-FTC-HELP.

Source: SearchSecurity.com

How Not To Get Hooked by a “Phishing” Scam

Have you received email with a similar message? It’s a scam called “phishing” — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation’s consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.



The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

If you get an email or pop-up message that asks for personal or financial information, do not reply. And don’t click on the link in the message, either. Legitimate companies don’t ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself. In any case, don’t cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.

Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It’s especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software “patches” to close holes in the system that hackers or phishers could exploit.

Don’t email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s website, look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL for a website that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer’s security.

Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you’ve been scammed, file your complaint at ftc.gov, and then visit the FTC’s [Identity Theft website](http://www.consumer.gov/idtheft) at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can’t entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

You can learn other ways to avoid email scams and deal with deceptive spam at ftc.gov/spam.



Who's Spamming Who? Could it be You?

Spammers may be using your computer to send unsolicited — and possibly offensive — email offers for products and services. Spammers are using home computers to send bulk emails by the millions. Indeed, computer security experts estimate that as much as 30 percent of all spam is relayed by compromised computers located in home offices and living rooms, but controlled from afar.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, spammers can compromise your computer in several ways, depending on what kind of Internet connection you have. All computers connected to the Internet are potential targets, but those with broadband connections are especially attractive to spammers because they are "always on." Spammers scan the Internet, searching for points of entry and then install hidden software that allows remote access to your data and programs. That, in turn, allows the spammer to send messages from your computer. Remote access software also can be installed by a virus: A spammer sends email with a virus in the attachment. If you open the infected attachment, a virus is released that installs the hidden software. The person who sent the virus now can access the data and programs on your computer, or take over many computers and use them to send spam.

It can be very difficult to tell if a spammer has installed hidden software on your computer, but there are some warning signs. For example, you may receive emails accusing you of sending spam; you may find email messages in your "outbox" that you didn't send; or your computer is using more power than it has in the past to run the programs you use.

If your computer has been taken over by a spammer, you could face serious problems. Your Internet Service Provider (ISP) may prevent you from sending any email at all until the virus is treated, and treatment could be a complicated, time-consuming process.

To avoid becoming an unwitting culprit, the FTC encourages you to:

- **Use anti-virus software and keep it up to date.** You can download anti-virus software from the Web sites of software companies or buy it in retail stores. Look for anti-virus software that recognizes current viruses, as well as older ones; that can effectively reverse the damage; and that updates automatically.
- **Be cautious about opening any attachment or downloading any files from emails you receive.** Don't open an email attachment — even if it looks like it's from a friend or coworker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.
- **Use a firewall to protect your computer from hacking attacks while it is connected to the Internet.** A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files. A firewall is different from anti-virus protection: Anti-virus software scans incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection.

Some recently released operating system software (including Windows XP) comes with a built-in firewall. Because it may be shipped in the "off" mode, check your online "Help" feature for specifics on turning it on and setting it up properly. If your operating system doesn't include a firewall, you can install separate firewall software that runs in the background while you use your computer and surf the Internet. Several free firewall software programs are available on the Internet. (You can find one by typing "free firewall" into your favorite search engine.) Or you can buy a hardware firewall — an external device that includes firewall software. Like anti-virus software, a firewall needs to be updated regularly to stay effective.

- **Check your "sent items" file or "outgoing" mailbox to see if there are messages that you did not intend to send.** Many spammers have learned to hide their unauthorized access, so even if there are no illegitimate messages in your outbox, you can't be sure that your computer hasn't been used to send spam.
- **If your computer is infected, take action immediately.** If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with fully updated anti-virus software. Report unauthorized accesses to your ISP. Also, if you suspect that any of your passwords have been compromised, call that site's company immediately and change your password.
- **Learn more about securing your computer at www.ftc.gov/infosecurity.**

Source: Federal Trade Commission

What Is SPAM?

Electronic junk mail or junk newsgroup postings. Some people define [spam](#) even more generally as any unsolicited [e-mail](#). However, if a long-lost brother finds your [e-mail address](#) and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a [mailing list](#) or [newsgroup](#).

In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of [network bandwidth](#). Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the [Internet](#) is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

There is some debate about the source of the term, but the generally accepted version is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam..." Like the song, spam is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the [University](#) of Southern California who gave it the name because it has many of the same characteristics as the lunchmeat Spam:

- Nobody wants it or ever asks for it.
- No one ever eats it; it is the first item to be pushed to the side when eating the entree.
- Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people.

