Hackers and Spam

Hackers and spammers may be using your computer right now. They invade secretly and hide software to get access to the information on your computer, including your email program. Once on your computer, they can spy on your Internet surfing, steal your personal information, and use your computer to send spam — potentially offensive or illegal — to other computers without your knowledge.

Computers that are taken over this way often become part of a robot network, known as a "botnet" for short. A botnet, also known as a "zombie army," usually is made up of tens or hundreds of thousands of home computers sending emails by the millions. Computer security experts estimate that most spam is sent by home computers that are controlled remotely, and that millions of these home computers are part of botnets.
Spammers can install hidden software on your computer in several ways. First, they scan the Internet to find computers that are unprotected, and then install software through those "open doors." Spammers may send you an email with attachments, links or images which, if you click on or open them, install hidden software. Sometimes just visiting a website or downloading files may cause a "drive-by download," which installs malicious software that could turn your computer into a "bot." The consequences can be more than just annoying: your Internet Service Provider (ISP) may shut down your account.

It can be difficult to tell if a spammer has installed hidden software on your computer, but there are some warning signs. 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 suddenly may operate more slowly or sluggishly.

Botnets are not inevitable. You can help reduce the chances of becoming part of a bot — including limiting access into your computer. Leaving your Internet connection on and unprotected is just like leaving your front door wide open. The FTC encourages you to secure your computer by:

Using anti-virus and anti-spyware software and keeping it up to date. You can download this software from ISPs or software companies or buy it in retail stores. Look for anti-virus and anti-spyware software that removes or quarantines viruses and that updates automatically on a daily basis.

Setting your operating system software to download and install security patches automatically. Operating system companies issue security patches for flaws that they find in their systems.

Being cautious about opening any attachments or downloading 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.

Using 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 firewall is different from anti-virus protection: while anti-virus software scans incoming communications and files for troublesome viruses, a properly-configured firewall helps make you invisible on the Internet and blocks all incoming communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection because the connection is always open. Most common operating system software (including Windows XP and Vista) comes with a built-in firewall, but you may have to enable it.

Disconnecting from the Internet when you're away from your computer. While anti-virus and anti-spyware software, along with a firewall, are critical protections when you're connected to the Web, they're not foolproof. Hackers just can't get into your computer when it's disconnected from the Internet.

Downloading free software only from sites you know and trust. It can be appealing to download free software like games, file-sharing programs, customized toolbars, and the like. But remember that many free software applications contain other software, including spyware.

Checking your "sent items" file or "outgoing" mailbox for messages you did not intend to send. If you do find unknown messages in your out box, it's a sign that your computer may be infected with spyware, and may be part of a botnet. This isn't foolproof: many spammers have learned to hide their unauthorized access.

Taking action immediately if your computer is infected. 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 and anti-

spyware software. Report unauthorized accesses to your ISP and to the FBI at www.ic3.gov. If you suspect that any of your passwords have been compromised, call that company immediately to change your password.

- Do NOT respond to unsolicited e-mails, IMs, text messages, phone calls, etc, from sources that are unknown to you.
- Do NOT provide ANY personal\financial information, account passwords, PIN numbers, etc, to anyone whose affiliation with a known institution cannot be verified. Remember, it is the policy of most reputable businesses that they will NEVER ask for such information, without full verification as to the legitimacy of such a request. If in doubt, personally contact the requestor.
- Contribute to KNOWN charities ONLY, by going directly to the organization's Web site, rather than following links to "related" sites.
- Verify the legitimacy and status of non-profit organizations, by using Internet-based government resources, or contacting local newspapers or television stations for information.
- NEVER open e-mails or e-mail attachments from unknown senders.
- Ensure that you have a reputable virus-detection installed and properly configured on your computer, and that it is updated regularly.