

Cut and Paste: Home Internet Security

America's collective mind is on security and safety. While most of America is thinking about airport security, you should turn your thoughts to home Internet security. In a report published the day of the September 11 attacks, the U.S. government suggested more attacks could come, including cyberterrorism. Cyberterrorist attacks are politically motivated and aim at shutting down critical systems—like an air traffic control system, that could have devastating consequences. Although cyberterrorism has been theorized, no attack has occurred to date.

It is highly unlikely that you will be the victim of a cyberterrorist attack. But, you should examine your home Internet security to see that your data is safe from hackers and that you don't unwittingly become the launching point of a cybercrime.

Hackers—clever programmers who used their talents in criminal ways—can get into unprotected computer systems, poke around and look at files, and can take information before being detected. They can also use an unprotected computer as a point of departure for an attack, such as spreading a computer virus or worm.

Before you throw your hands up in despair, take comfort: there are simple ways to make your system less vulnerable—and you don't have to become a techno-geek to understand them.

How do these people get into my computer anyway?

You let them. But once you understand how they're getting in, you can take the steps to keep them out. Hackers look for unprotected systems, or use Trojan horses, or bots (programs designed to cause a disturbance and catch you off guard), to commandeer your computer to launch attacks on other systems. You may not even know that you've given a hacker access to your system. Just by visiting a Web page or opening e-mail from a friend you could unwittingly download some programming code that has your computer performing commands that you never authorized.

Dial in accounts less vulnerable to attack

If you dial in to reach the Internet, you may be less vulnerable to hackers. That's because your connection to the Internet is available to hack only when you're connected. When you disconnect, no hacker can find you.

If you have an "always on" connection via cable modem or another broadband technology, you will want to investigate ways to protect your data. An always-on connection means:

- Your system is "always available" to be hacked.
- Hackers who locate your static IP can find it again—much like a crank caller who calls the same phone number again and again.

So how do you keep them out? Consider installing:

- A firewall

- Visit Steve Gibson’s site to read a good explanation of firewalls, how they work, and why you might install one: <http://grc.com/su-firewalls.htm>

■ Antivirus software

- Antivirus software won’t keep an intruder out of your system but might protect your system from infection from malicious pranks, such as computer viruses and worms. Although we don’t know which software is right for your system, you can visit CNET and create a comparison chart of available antivirus software. To create the chart, check the boxes next to the product name, and click the “Compare selected products” button when you’re ready (see illustration).

For each product you want to include in your chart, check “Compare.” When you have finished making your selection, click the “Compare selected products” button.

The screenshot shows the CNET Software website interface. On the left, there is a 'FILTER RESULTS' sidebar with dropdown menus for 'Low Price' (set to 'any') and 'Compatibility' (set to 'any'), and a 'Filter' button. The main content area is titled 'Compare selected products' and shows a list of three antivirus products. Each product entry includes a checkbox, the product name, a rating (e.g., 9/10), and a 'Check latest prices' link. The products listed are: Norton AntiVirus 2001 Pro Edition (9/10 rating, price range \$29-62), Norton AntiVirus 2001 7.0: Win9X/ME/NT 4 SP4/2K Pro/NT4 (8/10 rating, price range \$29-46), and Norton AntiVirus 2002 (8/10 rating, price range \$43-64). A 'Compare selected products' button is visible at the top of the product list. An advertisement for a Dell Notebook is also present in the sidebar.

Visit the site at: <http://reviews.cnet.com/>

But don’t think you are safe just because you installed antivirus software six months ago. Hackers see the latest security software as a mountain to be climbed, a challenge to their skills, and they are always diligently working to beat the latest security available, to demonstrate their hacking ability. Fortunately, the companies who sell the software provide users with updates. To safeguard your system, though, you are responsible for installing the latest updates—do so at least once a month!

It’s the same with any application. If the software company becomes aware of vulnerabilities in the software, they create “patches” that cover the “holes” in the application. It is the user’s responsibility to install these patches as they become available.

Don’t expect a program to protect you! Take control of your security. Certainly you can’t be expected to maintain a hypervigilance, but you can take steps to keep yourself out of harms way:

■ Passwords:

- Create passwords that are not easy to figure out and that incorporate numbers as well as letters
- Change your passwords regularly
- Do not give anyone your password
- Virus-scanning Software:
 - Install a good antivirus software
 - Keep it current by downloading the latest updates—at least once every month

Break the Chain: Chain letters = SPAM

As a public service, The Computer Incident Advisory Capability (CIAC) maintains a collection of Internet hoaxes and chain letters that spread viruses, clog mailservers, “and that generally do not have any basis in fact.” So, before you send that e-mail to your twenty closest friends in hopes that Bill Gates will write you a check for \$20,000, visit <http://hoaxbusters.ciac.org/>!

Kidding aside, the “Information About Hoaxes” section at <http://hoaxbusters.ciac.org/HBHoaxInfo.html> makes clear that passing along chain letters slows mail server processing to a crawl. The site also gives good clues that will help you spot a hoax or a chain letter and tells you what to do if you think you’ve received a hoax.