

Test Your Internet IQ: Top Seven Security Myths

Many of us surf the Internet, even shop and bank online, without really understanding that if we can get out to the world from our home computers, the world can get in. Test your knowledge of home computing security issues; you might be surprised by some commonly held misperceptions.

1. I have antivirus software—that's all I need.

This is the most common Internet myth. Yes, antivirus protection is important and you need it. But just having the software isn't enough. New viruses emerge all the time, so you need to update your virus definitions regularly to make sure they're current or, better yet, use software that does that for you automatically.

Furthermore, antivirus software only provides one type of security (stopping viruses from infecting your system) when you go online. But hackers are also a threat, and antivirus software can't deflect a determined hacker (see Myth #4). You need a firewall to stop hackers from getting into your system, and to make sure your personal information doesn't go out without your authorization.

2. There's nothing on my computer that a hacker would want.

Most of us believe this to be true. But a hacker could want the private data you store on your computer.

Hackers might search for personal information stored on your system—your Social Security and bank account numbers, for example—which they could use to make fraudulent purchases in your name. Identity Theft is the fastest-growing white-collar crime in the U.S. today (see related article, "Beware of Identity Theft"). And even if you don't do any financial work on your home computer, you may keep a resume on your hard drive in a desktop file conveniently named "resume." Your resume lists your name, address, where you went to school, your work experience. That's exactly the type of information you need when you apply for a credit card or a loan. Once hackers get hold of your personal data, especially your Social Security number, they can do all kinds of damage.

3. Only big corporations—not home computer users—are targets for hackers.

This is another common myth. "Why would they bother with me when all I do on my home computer is play games and send email?"

Hackers usually are looking for easy prey, and your home computer is much simpler to break into than a large corporate network would be. Hackers can infiltrate your system by using a number of tools readily available online. Broadband connections are particularly vulnerable because they have an "always-on," static IP address that can more easily be accessed, and it might take you a while to realize you've been hacked. If your home computer is always on and you don't check it frequently, you could be an ideal target.

Big corporations, on the other hand, have invested heavily in their Information Technology departments. They have huge antivirus programs on their gateway and very effective firewalls. In other words, they are harder to hack.

4. It takes a lot of technical knowledge to be a hacker.

Contrary to popular belief, you don't have to be a genius to hack into a computer. Hacking actually takes very little technical knowledge because any search engine queried about "hacking tools" will list site after site. The tools are readily available and can be downloaded in a few minutes. They even come with directions.

5. My ISP provides protection (antivirus and/or firewall) to me when I'm online.

ISPs rarely provide comprehensive protection, but for some reason users think that they do. So you might want to check with your ISP and ask how safe you are from viruses and hackers. And even if your ISP does provide a certain amount of protection, you should still install good antivirus software on your own computer.

Why? When you're online you're vulnerable to downloaded viruses, because your ISP probably screens email only. That doesn't protect you from a virus you may download inadvertently yourself.

6. I'm using dial-up, so I don't need to worry about hackers.

It's true that broadband users are more vulnerable to attack. A high-speed (broadband) connection means you have a static Internet Protocol (IP) address, so once hackers know where to find you, they can come back. They know where you live.

With a much slower, dial-up access, your IP address is changing all the time. This random access address allows dial-up users to enjoy a false sense of security, but that doesn't mean hackers can't find you anyway.

And if you have a dial-up connection, a hacker who does break into your system could install a back-door Trojan Horse, which lets the hacker see you each time you log in. The Trojan flashes a beacon that says, "Hey I'm here, come and get me"—so they know you're online and vulnerable. It's also possible to pick up a Trojan horse through an email virus, or you might download it in an infected Internet file. If you've picked up a Trojan horse, it doesn't matter whether your connection is broadband or dial-up.

7. I have a Macintosh

Mac users often feel safe because most viruses are designed for Windows-based platforms. But to a hacker it doesn't matter. A computer is a computer. They don't care what platform you're using, they just look for open ports. Many Mac-specific hacking tools are readily available on the Internet. Also, the new OS X is Unix-based. Unix computers have been around for so long that many of the hacking tools available to Unix users are now applicable to Macintosh.