

Common Myths about Computer Security

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.

Myth 1. I have Antivirus Software—that is all I need!

This is the most common Internet myth. Yes, antivirus protection is important and you need it. Nevertheless, just having the software is not enough. New viruses emerge all the time, so you need to update your virus definitions regularly to make sure they are 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. However, hackers are also a threat, and antivirus software cannot 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 does not go out without your authorization.

Myth 2. There is nothing on my computer that a hacker would want.

Most of us believe this to be true. However, the fact is that a hacker may 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. Even if you do not 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 is 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.

Myth 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 have been hacked. If your home computer is always on and you do not 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 a lot harder to hack.

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

Contrary to popular belief, you do not 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.

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

ISPs rarely provide comprehensive protection, but for some reason users think that they do. Therefore, you might want to check with your ISP and ask how safe you are from viruses and hackers. In addition, 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 are online, you are vulnerable to downloaded viruses, because your ISP probably screens email only. That does not protect you from a virus you may download inadvertently yourself.

Myth 6. I am using dial-up, so I do not need to worry about hackers.

It is 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 does not mean hackers cannot 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 are online and vulnerable. It is also possible to pick up a Trojan Horse through an email virus, or you might download it in an infected Internet file. If you have picked up a Trojan Horse, it does not matter whether your connection is broadband or dial-up.

Myth 7. I have a Macintosh

Mac users often feel safe because most viruses are designed for Windows-based platforms. However, to a hacker it does not matter. A computer is a computer. They do not care about the platform you are using, they just look for open ports. Many Mac-specific hacking tools are readily available on the Internet. In addition, 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. Besides, the latest Macs are built to run Windows and Windows applications, alongside the Mac OS!

Protect yourself!

Be smart. Install an antivirus program like Norton AntiVirus to safeguard your computer from virus attacks and to be sure that you do not download a Trojan Horse or other "back-door" program. It is also important that you keep your virus definitions up-to-date. Norton AntiVirus does this for you automatically, so your protection stays current. Moreover, use a firewall program such as Norton Personal Firewall. It protects you from hackers trying to scan your personal files, steal data, or damage your system. Norton 360, Norton AntiVirus, and other essential online protection tools are available together in Norton Internet Security.

Source:

<http://www.symantec.com/norton/products/library/article.jsp?aid=internet iq>