

## Re: A question for the group

---

*Source:* <http://sci.tech-archive.net/Archive/sci.electronics.design/2006-07/msg00913.html>

---

- *From:* David Brown <[david@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:david@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* 5 Jul 2006 22:59:01 +0200
- 

Nico Coesel wrote:

kensmith@xxxxxxxxxxxxxxxx (Ken Smith) wrote:

In article <44ab6d79\$1@xxxxxxxxxxxxxxxxxxxx>, David Brown <[david@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:david@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote: [...]

A real firewall/router will cost about \$30, and do a vastly better job of protecting your network or PC from trojans and other nasties.

They don't protect you from trojans. Trojans are named after that Greek horse that the idiots in Troy downloaded to inside their firewall.

And your ISP should be able to virus-scan your emails for you – again,

I want my ISP to keep its hands off my e-mails. We really don't want the status of ISPs to be changed. Today, very like the phone company, they are not responsible for what is said over their system. I want ISPs to keep this protection.

Funny, today I made a forecast on another forum that ISPs may become more than just a telco and also offer protection to their customers given the importance of internet nowadays. Not that I want this to happen, but there are already signs that governments want to regulate internet in order to protect their citizens.

they will (should!) do a better job than a home system.

As far as I know, there are no viruses for Apples. I think that this is in part because they are very well defended. The problem with the PC is

## Re: A question for the group

This is not quite true. The Apple OS is as vulnerable as any OS to trojan horses and other malware. Don't even think 'user mode' is going to help you (this is a very, very false assumption).

Rubbish. It's a false assumption if you think "user mode" will protect you entirely, but it helps enormously. On \*nix systems (including Apple OS), a program running with a normal user level clearance cannot corrupt other programs. Even on windows, careful use of NTFS permissions and user level clearances can limit programs' damage to some extent, but on the majority of windows setups, any program can pretty much do what it wants to any files, including vital OS files. Add that on \*nix systems, it is hard to get malware programs to run without user intervention, and you have an inherently much safer system (although never completely safe, obviously).

However, a malicious program would normally be able to access and damage your data files, which is often more of a problem – programs can be re-installed, while data files have to be replaced from your backups. And malware running as a user might have access to other user data, such as website logins. Finally, malware running as a user might be able to exploit software bugs to gain root access. So "user mode" is not a brick wall, but it is a very useful hinder against malware.

Clever criminals want to make money with your computer. They don't need root or administrator privileges to do so. All they need is a user with enough rights to download and run a program (even if it sits inside a corrupted JPG, PDF document, activeX control, executable, etc, etc) on a computer.

That's why on \*nix systems, websites and emails can't "download and run" programs (Java applets is the nearest, and they are sandboxed by the browser) without user intervention, and why \*nix browsers don't support things like ActiveX. They also don't support such absurdities as executable code embedded in wmf files and font files.

There is always the possibility of bugs in code leading to buffer overflow attacks and the like. \*nix systems can protect against such attacks in three ways that are better than windows systems. First off is the "user mode" limitation, limiting possible damage. Many serious linux distributions have stack randomisation, making it extremely difficult to make working buffer overflow attacks. Finally, on \*nix systems, the concept of shared libraries works properly, so bugs in library code can be updated once (by a download from your distro's website), and all your programs are fixed. With windows, if a bug is found in something like a MSVC run time library, practically every program on your system needs updating.

Regardless the OS, you'll need a virus scanner and a malware detector.

Regardless of the OS, you need to think about your security risks and take appropriate precautions. Even windows can be locked down pretty securely – if you set IE to maximum security then never use it again, and stick to decent browsers and email programs such as Firefox, Opera, and Thunderbird, with Java disabled unless you really want it, combined with a hardware firewall to block worms and direct attacks, and use some

## Re: A question for the group

common sense about the sites you visit and the programs you download, then you will not get hit. On the other hand, if you believe your virus scanner and other malware detectors make you impervious, then sooner or later you *\*will\** be hit.

.