Sunburnt
Internet Business Platform

News Features Pricing FAQ Contac

Home » Help » How To Keep Your PC Secure

How To Keep Your PC Secure

28 August 2007

In this article we consider what motivates people to break into your computer system, and offer a few essen pieces of advice that, if followed, will minimize your chances of being compromised.

Keeping the Bad Guys at Bay

For many people, the word 'hacker' conjures an image of a geeky teenager in a dark room harmlessly fiddlir his or her computer in an attempt to impress their friends. Perhaps this was the case once upon a time, but thanks to the Internet the stakes are much higher, and the competition much more fierce. It's so serious, we even started to see hacker turf wars [1], with groups of hackers attacking each other in a bid to gain more sh the cyber-crime market... but why?

Money and power

Hackers are generally either financially or politically motivated. Politically motivated hackers attack networks steal data, overwhelm services (denial of service), deface websites, or embarrass an organisation. Financial motivated hackers earn money by breaking into bank accounts (directly, or by phishing - i.e. trickery), selling credit card numbers, selling personal information, or renting botnets and other malicious software networks.

A botnet is a network of compromised computers which a hacker can control remotely and is often used for sending massive amounts of spam, or coordinating distributed denial of service attacks. Some estimates pu total number of zombied machines on the Internet belonging to botnets at 100 - 150 million [2]. Is your comp one of them?

How did it get so bad?

While there is a growing trend for attackers to try to exploit people using trickery, it remains that the easiest most common avenue of attack is to target software defects. Unfortunately for consumers, many software ve have been horrendously slow in responding to the Internet security threat. For some, their software was so unprepared for the Internet that they are still patching 15-year old defects.

The biggest attack vectors for hackers are through defects in operating systems, web browsers and email cl As more network applications become widely used (e.g. instant messaging, video chat and file sharing) they are becoming targets.

Security capabilities of different products is quite difficult to evaluate, however a simple indicator might be th number of programs which have been written to attack each one. The table below shows the number of kno viruses for the most widespread operating systems in use.

Operating system	Number of known viruses	Reference
Windows family	~140,000	2005, [3]
Mac OS X	1	2006, [4]
Linux	30	2005, [3]

These statistics should be taken with a grain of salt, as they refer only to viruses and not all common vulnera and exposures (CVEs). Other important security factors include how many vulnerabilities remain unpatched how quickly a vendor fixes their problems. It is, however, a useful statistic to demonstrate how several produ security can differ by an order of magnitude.

Tips for keeping your PC secure

- Use a secure operating system. The operating system manages access to all the resources on your co If it can be easily compromised, attackers may gain unrestricted access to all the data, software and ha in your machine. Additionally, secure operating systems do not require antivirus software which often ca performance problems.
- Use a secure web browser. The Web is the most frequently used Internet service and as such, web bro look a lot like the front door to malicious software. Insecure browsers may allow such software to install on you system simply by viewing an especially crafted web page, script or image.
- Install security updates. All modern operating systems have an automatic update mechanism. At the ve least, install updates marked as security updates.
- Don't send sensitive information by email. Email is a lot less private than you might imagine and your er can be intercepted or read by many people (for example, your ISP's staff).
- Only submit sensitive data to secure websites. Secure websites start with **https://** and are usually indica your browser with a small lock icon. Data sent to these websites is encrypted and can only read by the destination website.
- Learn to recognize fake websites. The biggest giveaway is that they use an incorrect or numeric domai (e.g. http://anzbank.example.com or http://166.293.34.22). Another hint is they send you an email askin your password!

The above advice doesn't refer you to any specific products since this would not be lasting commentary. Ho here at Sunburnt Web Services, our choice of operating system is Ubuntu (for our servers and desktops), ar use the Firefox for web browsing. We've also never had a single problem with viruses, spyware, adware or b In contrast, your author's unfortunate mum was robbed online of $3,000 using Windows XP and Internet Exp (although ANZ eventually bore this cost after involving the local police).

References

[1] The Register: Rival malware gangs wage turf war
[2] BBC: Criminals 'may overwhelm the Web'
[3] Techworld: Interview with Virus Expert, Mikkon Hypponen
[4] Sophos: First ever virus for Mac OSX discovered

terms of service | server load | server status

Sunburnt Technology | %{unsubscribe} %{ox_beacon}