Global Information Assurance Certification Paper

Basic Home Computer Internet Protection for Free!
Ted Tang
November 18, 2000

Home and SOHO users with full time or near full time Internet access now and never before need to secure their systems. The secured system should be able to detect and protect against unknown software such as viruses and spyware; detect and protect against unauthorized access such as port scans; and protect their privacy to avoid identity theft, SPAM, and Internet tracking.

Assuming you are running the Microsoft Windows operating system, Internet Explorer browser, and a 56Kb modem ISP dialup plus backing up regularly, follow these instructions to secure your system. Plus, since all of the following can be done for free, there is absolutely no reason it should not be done.

Please note, this is an overview of securing your system and does not provide detailed configuration instructions.

Benchmark

Before you begin securing your system, benchmark it to compare with later on. First, test your port vulnerabilities by accessing Steve Gibson's Shields Up! port scanner at http://www.grc.com. His site will detect your IP address, scan TCP and UDP ports, and report any services detected on the ports. If all of your ports are listed as "stealth", you are already way ahead of the game. His site also contains helpful information regarding port scans in general, personal firewalls, and spyware information.

Next, evaluate web tracking and browser performance by accessing WebWasher's advertising banner test page at http://www.webwasher.com/en/products/wwash/testpag1.htm. Banners can report back to sites IP addresses who are accessing them plus they degrade your browser performance because they need to get sent across your 56Kb line. The WebWasher site contains information regarding internet tracking, cookies, and web bugs.

Finally, try to download the test virus "eicar.com" from http://www.eicar.org; if your system does not warn you of a virus, take heed! Although this is just a test virus and does no harm, all anti-virus software should be able to detect it and demonstrate to you what happens when a virus is found. If you have anti-virus software installed and did not receive a warning, check its configuration and error log. Alternatively, you can replace it with the anti-virus software described below.

Secure your system

The first step in securing your system is not obvious: create a "public" login ID and password. This should be different from your "private" login ID and password. Your public ID should be used by default, and your private ID should only be used with those you trust.

Next, obtain a free Internet email account using your public ID. This will help protect your real email address, conceal your identity, and filter out SPAM; you will usually need an email address to register at most web sites to download software. Recommended are Yahoo.com and Hotmail.com because they are fairly easy to use, reliable, and free. Use this email account for everything. Only when you trust a recipient, give them your private email address. The idea is to keep your private email address private.

Next, apply the latest patches for your operating system and browser. This will increase system stability and close known vulnerabilities. Microsoft patches are available at http://windowsupdate.microsoft.com.

Next, install antivirus software. This will protect against email viruses and downloaded viruses. Recommended is Computer Associates InoculateIT Personal Edition available at http://antivirus.cai.com because it is from a major software publisher, works on Windows 95 to Windows 2000 Professional, and is totally free including signature updates. Make sure to configure it to automatically download new signatures. Their site has good information on viruses.

Next, install a personal firewall. This will protect against port scans and spyware that the antivirus software is not designed to detect. Recommended is Zone Labs' free Zone Alarm available at http://www.zonelabs.com. Besides alerting port scans, it asks you for permission if an application on your system wants to access the Internet. Grant those applications you know and trust and deny those you are uncertain of. Their site has information on port scans.

Optionally, install a public key digital signature and encryption software. This allows you to authenticate the source of email such as those sent by Microsoft Security (http://www.microsoft.com/technet/security) and SANS NewsBites (http://www.sans.org), keep your personal email messages private, and protect personal data on your hard drive. The later is crucial for laptop users when their laptop is lost or stolen. Recommended is PGP Freeware available at http://web.mit.edu/network/pgp.html and PGPdisk hack available at http://www.pgpi.org/products/pgpdisk. PGP Freeware allows you to create a digital signature, and a private and public key. It will also publish your public key on MIT's free PGP key server. You can also search the key server for other people's public key. PGPdisk allows you to create a virtual drive encrypted with your key. Use this drive to store sensitive data; if your laptop with this drive is ever lost or stolen, the virtual drive will not be accessible unless someone can manage to decrypt your key.

Next, optionally install a personal web proxy. This will help filter out undesirable content including advertisers, web cookies, and web bugs, and increase browser performance. Recommended is WebWasher available free at http://www.webwasher.com. This may be a first in security: increased security and performance since performance usually takes a hit with increased security.

Benchmark your secure system

Finally, benchmark your system again. Your port scan should come up full stealth and you should be alerted of them, your browsing should be faster with fewer advertising banners, and your system should alert you of the "eicar.com" test virus. Your total cost: nothing!

Of course, do not forget to backup your system regularly and make sure your virus signatures are updated.

References

Gibson, Steve. "Internet Connection Security for Windows Users." Shields UP!. 1 Dec 1999. URL: http://grc.com/su-explain.htm (18 Nov 2000).

Gibson, Steve. "The Anatomy of File Download Spyware." 14 Jul 2000. URL: http://grc.com/downloaders.htm (18 Nov 2000).

webwasher.com. "solutions." Keep Your Web Clean. 18 Oct 2000. URL: http://www.webwasher.com/en/solutions/index.htm (18 Nov 2000)

Zone Labs. "Easy to use, Always-On Internet Security." URL: http://www.zonelabs.com/zonealarm.htm (18 Nov 2000)

Network Associates. "An Introduction to Cryptography." Oct 1999. FILE: IntroToCrupto.pdf