
The following article, written by Bruce Schneier, appeared in his CRYPTO-GRAM Newsletter dated May 15, 2001.

The original article can be found at <http://www.schneier.com/crypto-gram-0105.html#8>

Safe Personal Computing

I am regularly asked what the average Internet user can do to ensure his security. My first answer is usually "Nothing; you're screwed." But it's really more complicated than that.

Against the government there's nothing you can do. The power imbalance is just too great. Even if you use the world's best encryption, the police can install a keyboard sniffer while you're out. (If you're paranoid enough to sleep with your gun and laptop under your pillow, this article is not written for you.) Even big corporations are difficult to defend against. If they have your credit card number, for example, there's probably no way to make them forget it.

But there are some things you can do to increase your security on the Internet. None of these are perfect; none of these are foolproof. If the secret police wants to target your data or your communications, none of these will stop them. But they're all good network hygiene, and they'll make you a more difficult target than the computer next door.

1. Passwords. You can't memorize good enough passwords any more, so don't bother. Create long random passwords, and write them down. Store them in your wallet, or in a program like Password Safe. Guard them as you would your cash. Don't let Web browsers store passwords for you. Don't transmit passwords (or PINs) in unencrypted e-mail and Web forms. Assume that all PINs can be easily broken, and plan accordingly.
2. Antivirus software. Use it. Download and install the updates every two weeks, and whenever you read about a new virus in the media. Some antivirus products automatically check for updates.
3. Personal firewall software. Use it. There's usually no reason to allow any incoming connections from anybody.
4. E-mail. Delete spam without reading it. Don't open, and immediately delete, messages with file attachments unless you know what they contain. Don't open, and immediately delete, cartoons, videos, and similar "good for a laugh" files forwarded by your well-meaning friends. Turn off HTML mail. Don't use Outlook or Outlook Express. If you must use Microsoft Office, enable macro virus protection; in Office 2000, turn the security level to "high" and don't trust any sources unless you have to. If you're using Windows, turn off the "hide file extensions for known file types" option; it lets Trojan horses masquerade as other types of files. Uninstall the Windows Scripting Host if you can get along without it. If you can't, at least change your file associations so that script files aren't automatically sent to the Scripting Host if you double-click them.
5. Web sites. SSL does not provide any assurance that the vendor is trustworthy or that their database of customer information is secure. Think before you do business with a Web site. Limit financial and personal data you send to Web sites; don't give out information unless you see a value to you. If you don't want to give out personal information, lie. Opt out of marketing notices. If the Web site gives you the option of not storing your information for later use, take it.
6. Browsing. Limit use of cookies and applets to those few sites that provide services you need. Regularly clean out your cookie and temp folders (I have a batch file that does this every time I

boot.) If at all possible, don't use Microsoft Internet Explorer.

7. Applications. Limit the applications on your machine. If you don't need it, don't install it. If you no longer need it, uninstall it. If you need it, regularly check for updates and install them.

8. Backups. Back up regularly. Back up to disk, tape, or CD-ROM. Store at least one set of backups off-site (a safe-deposit box is a good place) and at least one set on-site. Remember to destroy old backups; physically destroy CD-R disks.

9. Laptop security. Keep your laptop with you at all times when not at home; think of it as you would a wallet or purse. Regularly purge unneeded data files from your laptop. The same goes for palm computers; people tend to keep even more personal data, including passwords and PINs, on them than on laptops.

10. Encryption. Install an e-mail and file encryptor (like PGP). Encrypting all your e-mail is unrealistic, but some mail is too sensitive to send in the clear. Similarly, some files on your hard drive are too sensitive to leave unencrypted.

11. General. Turn off the computer when you're not using it, especially if you have an "always on" Internet connection. If possible, don't use Microsoft Windows.

Honestly, this is hard work. Even I can't say that I diligently follow my own advice. But I do mostly, and that's probably good enough. And "probably good enough" is about the best you can do these days.

CRYPTO-GRAM is a free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography.

CRYPTO-GRAM is written by Bruce Schneier. Schneier is founder and CTO of Counterpane Internet Security Inc., the author of "Secrets and Lies" and "Applied Cryptography," and an inventor of the Blowfish, Twofish, and Yarrow algorithms. He served on the board of the International Association for Cryptologic Research, EPIC, and VTW. He is a frequent writer and lecturer on computer security and cryptography.
