Words of Wisdom

by
Bruce Schneier

News.com, 9 December 2004

ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA

- Turn off the computer when you're not using it
- Especially if you have an "always on" Internet connection

- Keep your laptop with you at all times when not at home
- Treat it as you would a wallet or purse
- Regularly purge unneeded data files from your laptop

- Back up regularly
- Back up to disk, tape or CD-ROM
- Store at least one set of backups off-site
- Remember to destroy old backups

Operating Systems

- If possible, don't use Microsoft Windows
- Buy a Macintosh or use Linux
- If you must use Windows, set up Automatic Update

Applications

- Limit the number of applications on your machine
- If you don't need it, don't install it
- If you no longer need it, uninstall it
- Look into one of the free office suites as an alternative to Microsoft Office

Browsing

- Don't use Microsoft Internet Explorer, period
- Limit use of cookies and applets to those few sites that provide services you need
- Set your browser to regularly delete cookies
- Don't assume a Web site is what it claims to be, unless you've typed in the URL yourself
- Make sure the address bar shows the exact address, not a near-miss

Web Sites

- Secure Sockets Layer (SSL) encryption does not provide any assurance that the vendor is trustworthy or that its database of customer information is secure
- Think before you do business with a Web site
- Limit the 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

Passwords

- You can't memorize good enough passwords any more, so don't bother
- For high-security Web sites such as banks, create long random passwords and write them down
- Guard them as you would your cash
- Never reuse a password for something you care about
- Never type a password you care about, such as for a bank account, into a non-SSL encrypted page
- If your bank makes it possible to do that, complain to them
- When they tell you that it is OK, don't believe them; they're wrong

E-mail

- Turn off HTML e-mail. Don't automatically assume that any e-mail is from the "From" address
- Delete spam without reading it
- Don't open messages with file attachments, unless you know what they contain; immediately delete them
- Don't open cartoons, videos and similar "good for a laugh" files forwarded by your well-meaning friends; immediately delete them
- Never click links in e-mail unless you're sure about the e-mail; copy and paste the link into your browser instead

E-mail

- Don't use Outlook or Outlook Express
- If you must use Microsoft Office, enable macro virus protection
- 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

Antivirus and anti-spyware

- Use it — either a combined program or two separate programs
- Download and install the updates, at least weekly and whenever you read about a new virus in the news
- Enable automatically updates feature and set it to "daily"

Firewall

- Spend $50 for a Network Address Translator firewall device
- It's likely to be good enough in default mode
- On your laptop, use personal firewall software
- If you can, hide your IP address
- There's no reason to allow any incoming connections from anybody

Encryption

- Install an e-mail and file encryptor (like PGP)
- Encrypting all your e-mail or your entire hard drive 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