

IT security

Computer Security

Most people and businesses rely on computers to store personal and confidential information. This information may be business critical thus making computer security one of the most important factors in IT.

Security in the home

Security tends to be very costly, but there is a wide variety of FREE products for home use. For example you can get a great personal anti virus from <http://free.grisoft.com> or good anti spyware for personal use at <http://www.superantispyware.com>. Apart from the anti virus and anti spyware all you need is a decent router with firewall (about £60 - £100) and to have common sense. Don't go downloading everything that is sent to you via email and be careful with P2P file sharing programs such as Limewire.

Security at work

Security can be very expensive. Since security has become one of the most important issues in computing a lot of businesses invest heavily in to this and a lot of other businesses make a very wealthy gain out of it. Companies like Cisco and Symantec are hardware and software security corporations respectively and they are both very successful in a multi-million market. Licenses for a good antivirus package can cost from £200 - £500 per computer per year. Cisco Firewall routers can range £200 - over £10,000 and maintaining this hardware can also be very expensive. Some companies do not require expensive hardware and can do fine with a decent router with firewall

and self managed switch but a good antivirus package is essential.

Wireless

Wireless is been used more and more and is great for home use. For businesses it is still recommended to use structured cabling for better data integrity and security. Wireless signals travel through the air and can be caught by anyone and wireless encryption can be found using various techniques such as weak packet sniffing or simply via brute force. Some of these techniques can be undetectable since wireless network cards can be set to listen passively until the encryption keys are found.

Are the costs justified?

It all depends on how important your data is. What can a competitor achieve by retrieving your data? What can a fraudster do with your personal information? A very important thing to remember is that your intellectual property can be stolen without leaving a trace since the original will still remain intact.

Keep a balance

Even though security is very important, productivity is more important. Do not let security constraints hinder your

productivity. Be wise.

Passwords

A big mistake that a lot of people make is using weak passwords. These passwords are not only weak but they are also used to protect access to emails and several applications, which means that a lot of information can get stolen or altered if this password is compromised. Keep a strong password and change it every 3 - 4 months. Do not write this password down everywhere so that you remember. For more info on strong passwords visit <http://www.microsoft.com/protect/yourself/password/create.mspx>.

The Weakest link

All security experts know that a system will never be 100% secure simply because of the weakest link in all security systems. Which is the Human Factor. All systems are used by and administered by human beings and human beings can always be tricked. Most of the major hacking heists in history have been done via the art of Social Engineering. Social Engineering is an art, which entails retrieving the required information to hack into a system by using social skills, understanding human thought and habit patterns.

The best example of Social Engineering is the case of Stanley Mark Rifkin and how he deceived the employees of Security National Bank back in 1978 using only his social skills and a telephone. Rifkin managed to steal over \$8 million dollars and made it to the Guinness Book of World Records in the category of "biggest computer fraud"

Learn More

I recommend anyone interested in understanding business security to read the books *The Art of Deception* and *The Art of Intrusion* both by Kevin Mitnick (A very famous Social Engineer). These books are not only for computer people; they are a good read for anyone and will help you view security from a different and better perspective.

Dylan Lucas
n-wss ICT Ltd

