Comdex Technology Ltd.

Internet security advice (abbreviated version)

Cyber Crime is very big business. It is worth €millions and has a very small overhead. It generally is not personal and the criminal usually has no idea you even exist. It is also exceptionally hard to trace. So no wonder criminals use this as a tool of their trade.

You may ask how can you protect yourself from something you cannot see or feel or from somebody you do not know and that most likely does not know you? The honest answer is you cannot. But you can take all the precautions to help protect yourself, your business, your school or maybe your identity.

Simple as it may sound it starts with YOU. It is up to you to be careful who and what information you give out. It is up to you what you look at and what files you open on your computer. If you do not do that, then the rest is a waste of time.

Computer viruses have come a long way from some King wanting to give you half his Goldmine in return for your bank details. Modern viruses can come from the Internet, USB Devices, Printers, etc. They can be money related, blackmail related, data or identity related. Getting a virus on a computer system has the capacity to permanently close a company or indeed damage a Government organisation. Since it is done anonymously the size of the organisation does not usually matter to the criminal.

As I say, unfortunately there is no absolute 100% sure way to prevent it so you must take a number of realistic precautions.

1. Be vigilant and tell others to be vigilant – and don’t assume they are being vigilant
2. Put a proper Firewall in place
3. Put a proper Internet Security in place

The most obvious thing to do – or not to do – is open files you are not expecting or that look suspicious. Victims normally get caught by opening something like the following attachments:-

“Invoice as requested”
“Proof of Delivery”
“Purchase Order as requested”
“If this invoice is not paid legal action will pursue”
“Brilliant joke I thought you might like”
“look what this guy did”

If I can just give a few very simple common sense tips regarding emails.

- Never open an email such as the ones above unless you are expecting it.
- Always check the exact spelling of the email address it has come from.
- Be careful forwarding emails when going on holidays as the person receiving your post may think you were expecting it.

Windows has its own inbuilt Firewall but it is a basic version. It also has the issue of being inbuilt in the PC that you are actually trying to protect. It is recommended using a proper external Managed Firewall that will prevent access to the PC in the first case. The Firewall must be capable of handling the traffic throughput in your organisation.

If you are on the Internet then your PC is vulnerable. With Broadband being connected 24/7 it means criminals have access 24/7. Also, as they are using technology to beat technology, just because they did not get you this time around it does not mean you are not on their radar the next time around. Microsoft regularly bring out security patches which you should install. Backup your machine regularly and keep more than one backup.

Internet Security is far more than simple Anti-Virus. It can be Anti-Spyware, Anti-Spam and Intrusion Prevention. All of which effects our computers. It is recommended using a Managed version of your Internet Security as it ensures you always have the latest protection running. Internet Security runs locally on your computer and can protect the ports (USB) from unwanted programs. Be warned viruses can come from such devices as Printers, Photocopiers, USB sticks, etc.

Many people now connect to their computer network with mobile phones and tablets. You should be running protection on these devices as well. In short anything that connects to your network should be protected.

Remember a virus can sit dormant on your PC so by wiping your hard disk and reinstalling everything you may be reinstalling the virus. We strongly advise you never pay Ransomware. What proof have you they will unlock your computer or that when, and if, they do unlock it they have not left the virus to act again?

With the new General Data Protection Regulation (GDPR) coming into force you need to ensure your computer system and the data on it is very secure.

Unfortunately we all depend on Computers and the Internet these days so it is very important that you take proper precautions. Proper Internet Security costs far less than the grief and possible repercussions of a computer hacker.

For advice please contact Joe Halpin on 046 9077086