New Threats in 2005.

It looks like 2005 is gearing up to be a bumper year for the anti-virus and security technology companies.

We are seeing new types of threats coming at us in the first 3 months of 2005, and more of them than ever before. The main thrust of these new threats is phishing and identity theft emails, Instant Messenger delivered malicious code and malicious code on new platforms.

There has been a lot of publicity recently over the increased number of phishing attacks that organisations in Ireland, and the rest of Europe are coming under. These are getting more advanced and each one is better designed that the previous one. The branding and terminology used can be very good, and hard to detect as being malicious. One thing to bear in mind; a reputable financial institution will NEVER ask for personal details via an email. One particular area of increased activity is that of phishing for user's authentication details for supermarket loyalty schemes or purchasing systems. With these details, there is often enough information for a theft of an individual's identity. Many of these schemes are also affiliated with financial institutions, and loans can be applied for via the scheme, and funds withdrawn. The application for a loan is one of the ways that the identity theft fraudsters actually steal more money than the victim has in their accounts! The National Hi-Tech Crime Unit in the UK has warned many large retailers that they believe these schemes will be targeted this year by identity theft fraudsters.

During the first quarter of 2005, there has been an almost exponential growth of the number of pieces of malicious code that use Instant Messenger (IM) technologies to propagate. In most instances, they actually require a user to click on web link or download a piece of code that installs itself on the infected machine. This is often accomplished using the same social engineering techniques as used for email borne viruses. This malicious code then sends itself to all the other IM contacts from the infected machine. As yet, people are more trusting of messages they get from their IM contacts, as the same awareness of the risks that exist in email does not exist. One of the issues that this introduces is the link to other portable devices such as mobile phones. IM is used by many people today to communicate from a PC to someone with an advanced mobile phone. Once a piece of malicious code comes along that can infect both a PC and a mobile phone, there will be a very rapid spread. An organisation needs to make a number of decisions around the use of IM technology. Is it appropriate? Should desktop policies prevent users from accessing and installing IM software? Are the perimeter controls in place to prevent IM communication if a user manages to activate it? Does the organisation's acceptable usage policies reflect the use of IM in the way that web-browsing and email policies do today? These are all issues that need to be resolved to help prevent issues as a result of IM threats. In 2005, the Gartner Group has predicted that email will be supplanted as the main communications method by IM for most people, with Symantec claiming that IM security threats will grow 100% every 6 months.

This brings us to the 3rd point mentioned in the introduction; the spread of malicious code on new platforms. As mentioned above, the use IM across platforms will lead to viruses and other malicious code being spread to these platforms. Very few organisations are installing anti-virus or other security technologies on PDAs and

Smartphones. The rise of IM and mobile email on these devices means that it is only a matter of time before we see widespread outbreaks. We have already seen some small outbreaks on the Symbian operating system that is used on many Nokia and Sony Ericsson mobile phones. An example is the recent Drever-C Trojan horse. It attempts to remove any anti-virus software that is installed on the phone, and then attach itself to some of the Symbian operating system files. While this outbreak was relatively small, it shows that the techniques learned by the PC virus writers are being used for other platforms. In this instance, if the anti-virus signatures on the phone were not up to date, the Trojan could infect the phone, disable the anti-virus software, and any future updates with the relevant signature would be ignored. The speed with which signatures are applied to these platforms can be even more important than on the PCs. It is going to be very important to have prevention software such as firewalls installed on these devices in the future.

Lastly, there has been a lot of attention in the recent weeks to the Apple operating system, OS X, as a target for the hacking community. A lot of this attention is due to what is known as the “Halo” effect of the iPod music player. So many non-Apple users have purchased an iPod and been so impressed with the device that they have actually switched to using an Apple computer, or bought one in addition to their traditional PC. This has increased the Apple market share, and with that, attracted the attention of the hacking community. Many of the anti-virus vendors are making predictions that 2005 will see a large increase in the amount of malicious code being created for the Apple platforms, a strange sort of flattery for increased market presence!