

Streetwise in Cyberspace

By Chris Gledhill, Managing Director, PDMS

What is more damaging crime or the fear of crime? A topical question; on the radio last week I heard a pundit claim that children have suffered a 90% reduction in their freedom to roam in a single generation. This, it was suggested, was due to an exaggerated fear of violet crime which is simply not supported by the statistics. The argument (in part) was that children were being inadvertently put at risk because they fail to develop the skills and self-reliance they will need as teenagers / young adults early enough.

Any parent knows how difficult it can be to let go, but in truth the physical world we live in is pretty tightly regulated and children are well furnished with advice about 'stranger danger', the evils of smoking (yes that includes you Aunty Kate) and cycling proficiency.

My point, for those of you who were wondering what any of this has to do with cyberspace, is that the best way to deal with the risks posed by cyber-crime is through education and common sense; staying at home and hiding under the bed clothes is not an option. Besides, it is coming up to Christmas and I feel it is my duty to encourage as many people as possible to do their shopping on line, rather than risk life and limb on the high street this year!

With this in mind, I would like to explain a couple of types of on line malfeasances that have been getting a lot of publicity lately. The first is known as 'phishing' a rather nerdy name for a nasty little con trick also referred to as brand spoofing or carding. The following definition comes from www.webopedia.com.

"Phishing: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information."

Initially these attacks were mainly targeted at banking sites with the objective of acquiring sufficient personal and account specific information to be able to access live accounts and steal cash directly. More recently there has been a proliferation of phishing scams in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the information that the genuine eBay already had. Some of these scams are simply about stealing credit card details but others take a different slant. An aged relative of a colleague of mine recently had her eBay account hijacked by a phisher who used it to sell a few Picassos and a London landmark or two, before disappearing into the night leaving her to take the inevitable 'reputational damage' when the goods did not show up.

For anyone looking for more information on phishing (and how to avoid getting caught) there is a wealth of information available on line but an article entitled 'How Not to Get Hooked by a

'Phishing' Scam' on the Federal Trade Commission Web site is a good place to start (www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm). A simple rule of thumb is never divulge personal information by email and always use the correct web address to access an online business rather than a link in an email.

Distributed Denial of Service (DDoS) attacks on the other hand are targeted directly at online businesses and are often linked to organised crime. This is a sophisticated and highly technical process in which a type of computer virus is used to infect the machines of a large number of unsuspecting users. The virus, a malicious computer program, can be activated remotely. When activated, it is used along side thousands of similarly compromised systems to flood the targeted web site with an overwhelming volume of traffic. This type of attack can completely disable a site for a significant period. It is also about as precise as a B52 bomber in that it tends to result in a fair amount of 'collateral damage'. The flood of traffic aimed at one site will clog up access to other sites in the same segment of the network causing a general nuisance.

This type of attack is sometimes used as the basis for a type of protection racket in which sites are offered 'protection' if they pay or threatened with attack if they do not. For high profile sites the stakes can be very high, interruption to trading at peak times can cost millions and the reputational damage may be even greater.

For the home user the main risk associated with DDoS is being used unwittingly as a host for the virus that generates the malicious traffic. The best defence is to keep your virus protection up to date. It is also worth noting that a computer, which is not switched on, cannot take part in a DDoS attack.

So is the Internet getting too dangerous? Well I certainly don't think so, there are risks on line as there are in all commercial activities, but a few sensible precautions like keeping your antivirus software up to date and never divulging your user names and password are the best defence. Also, it is important to check credit card statements when they come in and report any suspicious transactions. In reality the vast majority of on line business is trouble free, cost effective and convenient and I would like to wish everyone who has made it to the end of this article, a safe and happy Christmas in cyberspace (and anywhere else).