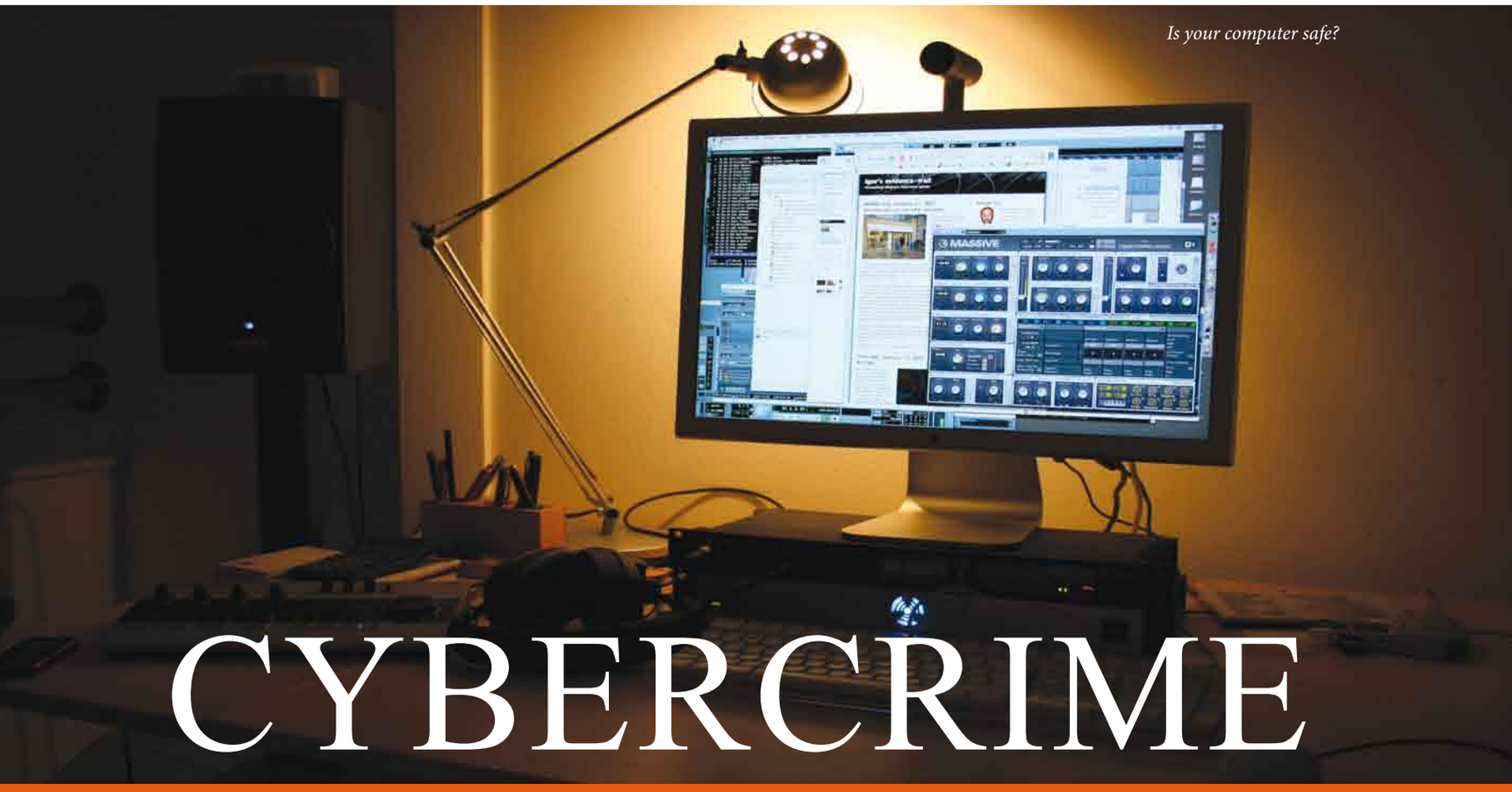
This month, Bernard Collin, Founder, Chairman and Chief Executive Officer of Safecoms Co. Ltd. talks about cybercrime and how you can protect your corporate and personal assets from the bad guys roaming the World Wide Web.



Is your computer safe?

CYBERCRIME

Most people have no idea how dangerous the internet can be these days. People have a virus checker and a firewall and they think they are protected. The reality is that cybercrime is a flourishing underground world with organised crime aggressively carving out a share of virtual territory. Exact figures are hard to come by, but a detailed study by the FBI in 2006 found a major shift from traditional to Internet and cybercrime. The FBI study estimated that revenue from cybercrime now exceeds the revenue criminals earn from drugs, prostitution, trafficking and other traditional forms of crime. The big reason cybercrime has become so attractive and so lucrative is that so many people using the Internet are unaware of the dangers. For professional and amateur criminals alike, the risk is so much lower and the potential number of victims so much greater.

FBI research shows that 9 out of 10 companies have suffered incidents involving cybercrime.

The business community in particular is falling victim to attacks of cybercrime. The FBI research shows that 9 out of 10 companies have suffered incidents involving cybercrime and one out of every five organisations has experienced actual break-ins and attempts to steal their data, sabotage their systems or defraud the company in some way. The seriousness of these incidents is getting worse, and higher sums are involved. Companies and organisations keep on responding to known older threats and don't seem to be aware of the growing dangers. Increasingly, companies are turning to specialists like SafeComs to help them protect their data and their systems.

"Many people don't really understand what cybercrime is", says Bernard Collin, SafeComs founder and CEO. Most employers would be surprised to learn that many of their employees are actively engaged in cybercrime. Staff may think it's harmless, but when they are browsing porn sites, chatting with strangers in social networks and downloading music and movies, they are stealing company time, infringing copyright agreements and exposing your entire computer network to the threat of attack by fraudsters, spammers and criminal gangs. The Business Software Alliance (BSA) raids companies daily in search of these pirated activities. As a company owner, you could easily find yourself engaged in a costly court case against powerful institutions, all because you failed to implement a few basic measures to monitor your network and employee activity on the Internet. SafeComs advises companies to at least do a software legalization and Internet security audit.

Most employers would be surprised to learn that many of their employees are actively engaged in cybercrime.

One increasingly common form of cybercrime is "phishing". Fraudsters 'go fishing' on the World Wide Web for people who will give their bank account details and personal information. The victim (you!) get an e-mail that appears to be from a legitimate company such as eBay, Amazon or even your bank. The e-mail then directs the victim to a fake website that looks identical to the legitimate website and asks them to enter debit or credit card details so that a payment of some kind can be credited to their account. One recent example in the UK appeared to come from the Revenue & Customs Department and told recipients they were due a tax refund of £172. People who followed the instructions had their bank accounts emptied or their credit cards charged to the limit. And guess what? There is almost nothing you can do to get that money back or the credit card charges cancelled.

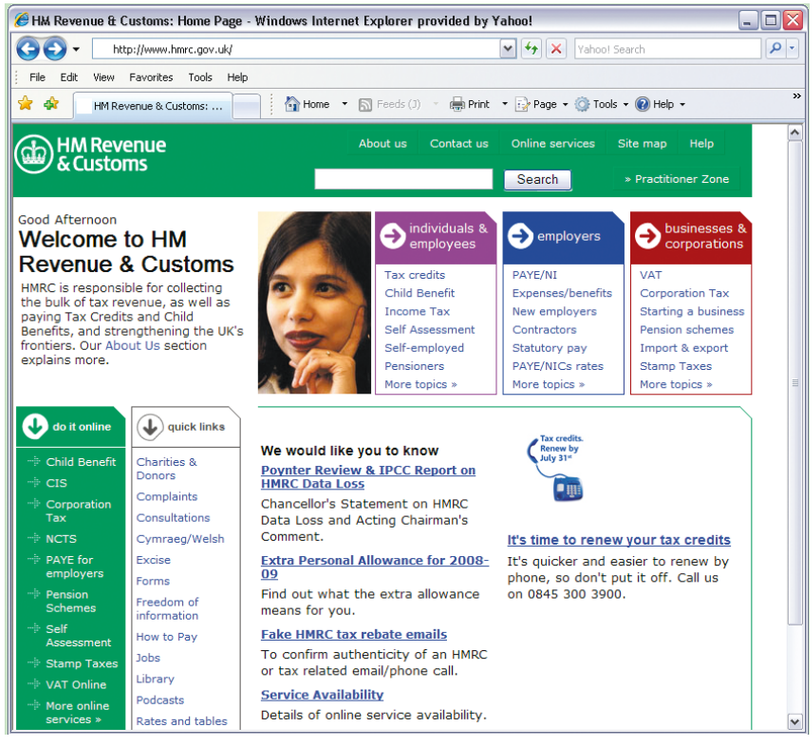
Experts believe that almost half of all phishing thefts are committed by groups operating through the Russian Business Network (RBN), a web hosting company based in St. Petersburg and run by a figure known as "Flyman". Dubbed "the mother of cyber crime", RBN is also been linked to child pornography, corporate blackmail, spam attacks and online identity theft. A report by Veri-Sign, one of the world's largest internet security firms, suspects that the Rock Group, a criminal gang specializing in phishing, used RBN's network to steal about £75 million from bank accounts last year. RBN has also developed fake antivirus software programs to dupe internet users into giving it access to their computers in the mistaken belief that they are protecting themselves. "These are criminal gangs of computer experts", says Bernard Collin, SafeComs founder and CEO. "Companies need experts with equal knowledge and skill to protect themselves, which is what SafeComs is all about."

The Rock Group, a criminal gang specializing in phishing, stole about £75 million from bank accounts last year.

So is there anything you can do to protect yourself short of unplugging your internet connections? Fortunately, SafeComs can suggest some simple steps companies and individuals can take to protect themselves and their computers from the many threats online. The first, and perhaps most important, is awareness. Reputable companies never (not ever) ask customers for passwords or account details in an e-mail. No matter how convincing that e-mail sounds or how real that website looks, do not respond. Never click on links within a dubious-looking e-mail. Instead, go to your web browser and type in the address by hand (do not cut and paste). If you don't see any news about this wonderful offer on the official website, you can be 99.9% sure someone is phishing for suckers, which is a rather dumb kind of fish.

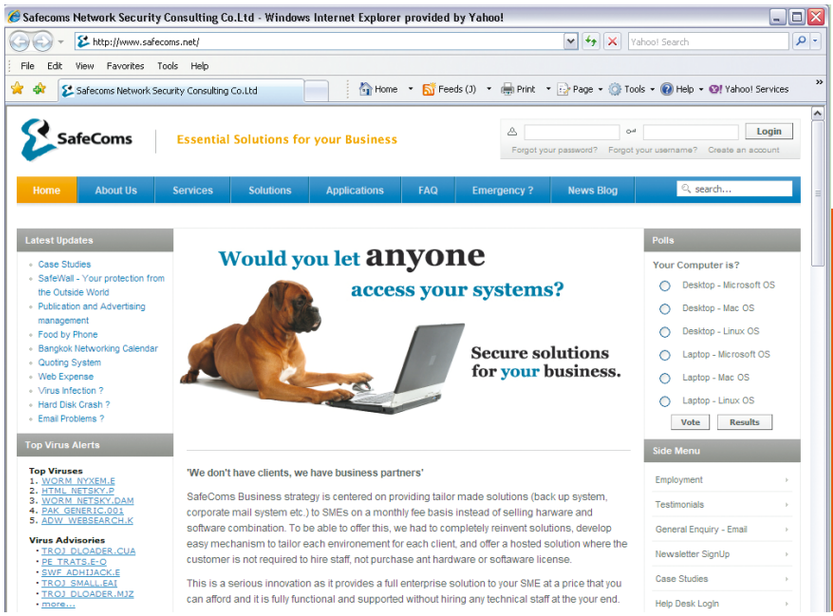
Learn to look for telltale signs. The URL on most phishing websites differs from the genuine version.

You can also learn to look for telltale signs that an e-mail or website is a forgery. Look also at the URL or internet address that appears at the top of a web browser. The URL on most phishing websites differs from the genuine version. For example, the site purporting to be Her Majesties Revenue and Customs Department, UK (HMRC) started with the web address "gastagerweltreisen. de", suggesting that it is hosted in Germany, rather than the legitimate site, "hmrc.gov.uk".



You can easily infect your computer with malicious spyware or viruses by opening attachments and downloading files from e-mails or the internet. Spyware is software that infiltrates your computer. A tiny program then monitors your activity, scans personal information and sends it back to fraudsters or hackers who can actually take control of your system. Your entire system can be knocked out permanently by some of these malicious invaders, which is why SafeComs strongly advises companies to invest in proper backup systems.

Ensure that your computer has a firewall, intrusion prevention and virus protection software and that these programs automatically and frequently update their databases. Companies such as Norton, McAfee and Symantec sell automatically updated firewalls and virus protection software. For non-commercial use, there are free alternatives such as Grisoft's and AVG, available for downloading at www.free.grisoft.com. For other options visit www.GetSafeOnline.org or better still, talk to the people at SafeComs.



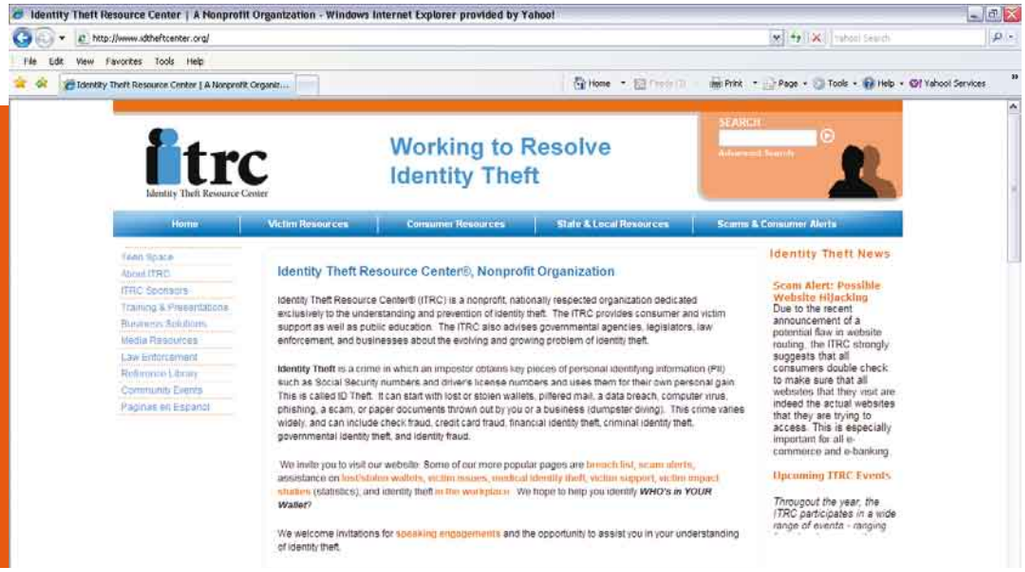
WANT TO KNOW MORE?

Internet Security

SafeComs
http://www.safecoms.com, www.safecoms.net

SafeComs is a Bangkok based company specializing in network security for computer systems and for unique security solutions delivered over the Internet. SafeComs can provide Internet security audits, license legalization audits, critical backup solutions and anti-spam services.

Identity Theft



Identify Theft Resource Center®, Nonprofit Organization
http://www.idtheftcenter.org/

Identity Theft Resource Center® (ITRC) is a nonprofit, nationally respected organization dedicated exclusively to the understanding and prevention of identity theft. The ITRC provides consumer and victim support as well as public education. The ITRC also advises governmental agencies, legislators, law enforcement, and businesses about the evolving and growing problem of identity theft.

Computer Scams and Hoaxes

Hoax-Slayer
http://www.hoax-slayer.com/

Hoax-Slayer is dedicated to debunking email hoaxes, thwarting Internet scammers, combating spam, and educating web users about email and Internet security issues. Hoax-Slayer allows Internet users to check the veracity of common email hoaxes and aims to counteract criminal activity by publishing information about common types of Internet scams. Hoax-Slayer also includes anti-spam tips, computer and email security information, articles about true email forwards, and much more. New articles are added to the Hoax-Slayer website every week

SafeComs Network Security Consulting Co., Ltd.
21/16 Premier Condominium,4th Floor, Unit 401,
Sukhumvit 24 road, Klongton, Klongtoey,
Bangkok 10110, Thailand Tel: 02-259-6281-3
www.sefecoms.com, www.sefecoms.net
e-mail : info@sefecoms.com