

E-CRIME - KNOW THE RISKS

HACKING

Hacking is an offence under the Computer Misuse Act 1990 and is the unauthorised access or modification of computer systems or data.

Traditionally, hacking was used to target big corporate and government systems – it was done by the stereotypical ‘computer nerd’ who carried out this activity just to show they could. Times have changed, criminals have seen an opportunity and organised crime gangs are now employing these people and using their skills and expertise to get people’s money. Hackers themselves have become organised and share their skills online via internet forums (See ‘Internet Forums’ below)– that are accessible by invitation only and often in Russian, making it difficult for the UK to target.

Hacking might be just an attack of vandalism or it might be a calculated attack to disrupt or destroy your systems or to steal personal data and information.

SCANNING

Scanning is the use of an automated tool that looks for unprotected systems. These tools are easily accessible and can be downloaded from the internet. The software will search for corporate and government networks or individual computers connected to the internet. The scanners sweep through ranges of IP addresses looking for unprotected systems. People do these scans then sell the information on unprotected networks to whoever is willing to pay for the information. The targeted systems may be exploited immediately or stored with other vulnerable systems for later use.

SPAMMING

Spamming is the bulk distribution of unsolicited commercial e-mail. It is usually just a nuisance, but it can have more serious connotations. It is a primary delivery method of various scams and is also used to distribute malware – that is software that has a malicious content and is capable of tracking everything you are doing whilst online.

Sometimes sensational headlines on e-mails compel you to open them. Opening this type of e-mail and then any of the links contained therein gives open access to your computer

and potentially someone can then take control of your system and you will be completely unaware. **It is always the link in an e-mail that contains the malware.**

The majority of e-mail messages worldwide are now spam delivered by infected computers. To combat this you should have filtering processes in place.

WORMS AND VIRUSES

No longer are these just invertebrates and micro-organisms that cause many common human infections! Worms and viruses in the computer world are self-propagating malware. There are a range of spreading mechanisms including e-mails containing malware as an attachment or link. As stated previously, opening the attachment/link executes the code and infests the machine.

A worm is different from a virus. A virus seeks to destroy your system, whereas a worm does not alter files or programmes. However, the worm is a cyberbeast with a dark-side. It lives in your active system and makes clones of itself, reproducing to the point where your system is so infected that it becomes inexplicably slow – probably the first realisation you will have that all is not well. Its' mission in life is to go forth and infect as many systems as possible and so it lurks and waits for you to connect to the internet. Once this online connection is achieved it will happily open your address book and forward itself to all your contacts.

Other than the nuisance value, worms can wreak havoc on your business, not only by causing your systems to grind to a halt, but increasingly spammers and those who write the worm programmes have joined forces, the intention being to take over your computer systems without your knowledge and manipulate them for their own gain.

Protect yourself by having up-to-date anti-viral, anti-spam and anti-spyware installed on your systems. **Up-to-date is the keyword!** As soon as a new worm is detected the 'good side' writes programmes to kill it. This software updates itself on a daily basis against any new threats, which is why it is so important to keep this software current.

INTERNET FORUMS, DDOS ATTACKS, 419 FRAUD AND PHISHING

It's like learning a new foreign language isn't it? Don't despair; just remember that knowledge is power.

Let's start with Internet Forums – I mentioned these briefly under the 'Hacking' heading. Internet Forums are organised and populated by virtual crime groups – a virtual crime group can be either individuals or teams of e-criminals –(e-criminals being like e-crime in the sense that they are using information and communications technology for criminal purposes). These internet forums are getting huge and, make no mistake, although we use the terminology 'virtual crime groups', there is nothing 'virtual' about the criminals,

they are very real. They do their crime online and the forums provide a secure environment to do their business. They meet online to coordinate their activities and exchange information and tools and also to buy and sell information – remember, it could be your information. The clever ones collect the information and then sell it on rather than using it themselves. Every credit card with a security number and name and address has a ‘dollar’ value so please be conscious of this and keep all personal information stored on your systems locked down and secure.

And here’s another little word of caution... there is something on the web known as ‘Peer-to-Peer’ networks. They offer free downloads and allow you to connect to another persons computer anywhere in the world to share files – these networks are riddled with malware. Therefore, businesses that do not have a policy in place to prevent their staff accessing these sites are leaving their systems wide open to abuse. If your staff need to use the computer for legitimate business purposes fine, just be aware of the potential hazards of allowing unrestricted use.

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Criminals will target a particular system - usually systems acting as servers on the web - and flood the bandwidth or resources of that system with so much traffic that it simply can’t cope and goes down. Malware can carry DDoS attack mechanisms. There are instances when large companies have been held to ransom by these criminals and have paid out in order to get their systems up and running again.

419 FRAUD

This is a scam that has been on the go for a long time –centuries in fact – but it reached an all time high in the mid-eighties when Nigerian criminals started to exploit it in earnest using traditional letters, faxes and the telephone as a means of making contact. Thus it became known as a ‘419 fraud’ after the relevant section of the Nigerian Criminal Code – 419; is also known as ‘advance fee fraud’. Like anyone trying to grow their business, criminals have moved with the times and are now using e-mail to increase their distribution network. It is a con trick in which the target is persuaded to advance relatively small sums of money in the hope of realising a much larger gain. Essentially, all of these frauds involve requests to help move large sums of money with the promise of a substantial share of the cash in return. The criminals use social engineering to extract information from would-be victims to help them make their scams as realistic as possible. They are currently targeting professional groups i.e dentists, accountants etc. by pretending to be from a similar professional backgrounds and seeking assistance to set up a business abroad.

Protecting yourself against this type of scam is relatively easy – do NOT respond. It is important to remember that the fraudster has not targeted you personally. They will have sent out thousands, possibly hundreds of thousands of e-mails, having acquired the addresses randomly. Just remember, rarely in this life do you get something for nothing

and it is highly unlikely that you will ever get a massive return on a very small investment.

Phishing

This is a good 'new' descriptive word for the technological era – Phishing is, quite simply, where criminals have a hook, they put on the bait and cast their rod far and wide in the hope that someone will bite. The phishers will attempt to fraudulently acquire sensitive information such as usernames, passwords and credit card details. It is typically carried out by email or instant messaging and often directs users to give details at a website, although phone contact has been used as well. EBay and Pay Pal are two of the most targeted companies as are online banks. The phishers will use official-looking logos from real organisations and other identifying information taken directly from legitimate websites; they may also place a link in them that appears to go to the legitimate website, but it actually takes you to a fake look-a-like site or possibly a pop-up window that looks exactly like the official site. Once you're at one of these spurious sites, you might unwittingly send personal information to the con artists.

WHAT TO LOOK OUT FOR

If you see any of the following phrases in an e-mail, start to be suspicious:

Verify your account

Businesses should not ask you to send passwords, login names or any other personal information via e-mail. .

If you don't respond within 48 hours, your account will be closed

These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishers will also try and con you into thinking your response is required because your account might have been compromised. This type of scam is also used via telephone contact – if in doubt, do NOT divulge any personal information and contact the company yourself, using a telephone number you have found yourself and you know to be legitimate,

Dear Valued Customer

Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

Click the link below to gain access to your account

These may look genuine and take you to a website or form that looks entirely genuine. But beware! The links that you are urged to click may contain all or part of a real company's name, but are "masked," meaning that the link you see does not take you to that address but somewhere different, usually a fake look-a-like website. Try resting your mouse pointer on the link – if it shows a string of cryptic numbers that does not look anything like the company's web address then it is a Phishing attempt.

IDENTITY THEFT

If you have read all or some of the above criminals are increasingly looking for ways to steal your identity so they can use it for their personal gain. From a business perspective, it is important to be aware that this type of criminality is not limited to individual victims; companies and their directors can also be targeted. The following is an excerpt from the businesslink.gov.uk website, which also has other useful links for businesses to assist them in protecting their online business activity:

If a fraudster can get sufficient information about a business and a person, they may be able to apply for a corporate credit or debit card and go on a spending spree. Such cards can be readily used in electronic transactions.

As part of your security policy, you should implement guidelines on what personal information should be divulged to third parties, particularly by electronic means such as email.

Corporate identities can also be stolen. This type of identity theft can have appalling consequences for businesses. For example, it is possible to submit forms to Companies House that will:

- *change the registered address of a business - form 287*
- *change the company secretary or director - form 288c*
- *appoint new directors - form 288a*

Unfortunately, Companies House will not notify the true company secretary or directors that these forms have been lodged. Neither will they check any of the details for validity.

The "new" directors can open new bank accounts, have goods delivered to the "new" address, and effectively ruin the credit rating of the business and leave it with massive charges to clear.

*To avoid this form of corporate identity theft, you can use the Companies House PROOF scheme of electronic filing. You can **[find out about the Companies House PROOF scheme at the Companies House website](#)**.*

GENERAL TIPS:

- Make computer security a priority by learning the facts about cyber threats – if in doubt get professional advice – it will be worth the investment. Assess the risk and manage it according to your business needs. A comprehensive business security plan is worth the time and effort
- Business critical information should be restricted to the people who truly need it - do NOT store it on a web server. Encrypt your network and limit access. A detailed internet acceptable use policy and a contract defining what access is permitted to sensitive data will significantly protect you business from internal threats whether they are executed through ignorance or malicious intent.
- Regular training of employees and reminders on what to avoid doing when using e-mail or the Internet, can significantly reduce vulnerabilities online.

- Use strong passwords and change them regularly. Do not use a word found in a dictionary (any dictionary/any language). Hackers will use software programs to run dictionary attacks to discover passwords. Use a mixture of letters, numbers and characters.
- Have firewalls in place, install anti-virus, anti-spam and anti-spyware software and keep them updated.