Briefing

Fraud and White Collar Crime

April 2016

Cybercrime: a guide to recognition, prevention and protection

Commercial entities are inevitably reliant upon IT to operationally manage their businesses and to deliver services to their customers. This reliance exposes businesses to the risk of falling victim to cybercrime.

Cybercrime will only continue to increase in prevalence and sophistication. It is estimated that 81% of large organisations and 60% of small organisations were victim to a form of cyber-attack last year. For example, Talk Talk's data breach is expected to cost it £35m. However, the threat from cyber-criminals is not just financial – falling victim can lead to reputational damage, the loss of intellectual property or sensitive customer data and business interruption.

Despite this, many companies are not taking cybercrime seriously enough. This briefing sets out some of the types of scams that cybercriminals employ, how to recognise them, and how to make themselves less susceptible to them.

Recognition

Phishing

Phishing attacks involve fraudsters sending bogus communications, typically by email or text message, that purport to be from a well known and trusted source. The message is likely to include company logos and graphics, and originate from a "masked" email address, to give an illusion of authenticity. Couched in professional business language, the message will often make a request that the recipient provides personal and confidential information. Once the personal details have been obtained, fraudsters will either use this information to defraud the victim, be it an individual or an organisation, by stealing from the victim's bank accounts, or by stealing the victim's identity in order to conduct further fraud.

Spear-phishing

Whereas phishing emails are sent to a vast number of randomly generated addresses, spear-fishing involves sending communications to targeted individuals. Again, the attack usually takes the form of a communication seeking access to sensitive and confidential data, usually with a sense of urgency. The emails will, again, appear to come from a trusted source, usually from someone in a position of authority at the recipient organisation, or another well-known company used by the recipient. Spear-phishing attackers will have a deeper knowledge of the recipient's digital footprint – for example, the websites they use or the organisation's key clients. Fraudsters will use this information to carefully target recipients and to add credibility to these attacks.

Whaling

This scam consists of a spear-phishing attack sent by a fraudster impersonating an organisation's "big fish" – typically the CEO or CFO. For instance, the scammer might send a message to a member of staff, posing as the organisation's CEO. The message may, for example, instruct the unsuspecting member of staff to transfer money to a desired account in order to "finalise an urgent business transaction". The email is likely to contain legitimate looking graphics and a masked domain name, to fool the recipient into actioning the urgent task without first checking the background with another member of staff.

Criminals are quickly able to obtain an organisation's structure chart and ascertain the name of the "whale". Fraudsters will also scour social media to understand when the "whale" is out of the office for an extended period. This information presents the fraudster with an opportunity to launch an attack.

System attacks: "Crimeware", hacking, and pharming

Another example of the increasing sophistication of phishing attacks is the use of "Crimeware" (sometimes called "Malware" – malicious software). A typical example is where a recipient receives an email from an apparently trusted source, and clicks on an embedded link. This then automatically infects a victim's computer/smartphone with a piece of software that monitors activity and captures information, either by "key-logging" (where criminals record what you type) or "screenshot-ing" (where an image of your computer screen is captured). Therefore, the next time the victim visits a legitimate website and enters any information, that information is transmitted to the originating fraudster. The software can remain totally undetected on a victim's computer.

Crimeware is also associated with "pharming", a form of online fraud in which the victim, upon entering a legitimate website

continued

address, is diverted automatically to a bogus site of, for example, a bank, and asked to enter account information.

"Hacking" is the primary method of infiltrating networks. Through the injection of specialist software, hackers seek to gain unauthorised access to and take administrative control of computer networks and systems.

How to protect yourself

Preventing, detecting or disrupting the attack at the earliest opportunity limits the business impact and the potential for financial and reputational damage. Prevention is better than cure, so making yourself and your business an unattractive target, and reducing your organisation's exposure to risk, will make your business less susceptible to cyber-attacks. Whilst the scams outlined above are different in nature, they share similar characteristics and there are common steps and precautions businesses and individuals can take to help protect themselves.

Be vigilant

Owing to the increased sophistication of scams of this type, it is no longer possible to simply spot a bogus email by virtue of the fact that it is littered with spelling mistakes or poor grammar. However, individuals should carefully sense check communications. Is the communication urgent, unusual or unexpected? Is there anything that alerts suspicion? For example, a spelling mistake in the email address, or an atypical or generic salutation?

When receiving communications that appear suspicious, recipients must test the information provided. Check that any phone numbers, website addresses or bank details are the same as those held on record. If the communication involves high risk information, confirm these details. For example, if an email contains payment information, follow this up with a phone call to a known phone number. Finance teams should verify online accounts regularly to ensure that no unauthorised transactions have taken place.

Reduce spam

As many attacks come from unsolicited emails, it pays to be suspicious of emails originating from unknown senders. It is advisable to keep spam filters switched on and to delete any spam you have received, preferably before opening the email. It is important not to open attachments or click on embedded links. Simply clicking on a link can alert the fraudster to the fact that your email address is "live" and can make you the subject of future attacks.

Browse safely

Carefully check the spelling and appearance of URL addresses. Users must remain vigilant that the web browser hasn't redirected to a website with a slightly different spelling, perhaps with an additional letter or with a character swapped around. When executing online transactions, it is important to ensure that the website is secure by checking that the "http" web address pre-fix has changed to "https" (the "s" stands for "secure") and that the website contains a padlock on the address bar.

Keep your IT network safe

Your business's IT department should keep firewalls, anti-virus software, anti-malware, anti-spyware tools and your operating systems updated. They should ensure that data and networks are properly encrypted and that all systems are backed up at regular intervals. Removable media (such as USB drives and CDs) or portable computers (such as laptops and tablets) should be scanned for viruses before being introduced to a secure network. Data should not be kept for longer than absolutely necessary, as data that a business no longer requires may still be valuable to cybercriminals.

Passwords

Ensuring that key systems are protected by strong unique passwords is absolutely essential in protecting yourself from cybercrime. Strong passwords are those with at least eight characters and which include a mix of upper and lower case letters, numbers, punctuation marks and symbols. Every password for every site you visit should be different, and passwords should be changed regularly.

Keeping secrets secret

Disclosing information online regarding your whereabouts, the whereabouts of your CEO, or details pertaining to the completion of a business transaction can all assist fraudsters in assimilating information for use in the scams discussed above. Consider whether you are revealing too much information about yourself or your business, and ask yourself what a scammer could do with the information that you have put in the public domain.

Training

Businesses should raise awareness amongst staff of the common cyber-scams and how to spot them. High risk departments, such as finance, IT or HR, should have extensive training at regular intervals to ensure that their understanding keeps pace with the evolving nature of the risk.

Stress testing

Organisations should consider carrying out "test attacks" to see if any members of staff are duped. If a member of staff falls for the "bait", further training should be urgently conducted.

Insurance

Organisations should review their insurance to ensure that their policy covers cyber-attacks. It is estimated that only 51% of businesses have cyber-insurance in place. For example, a

continued

fraudster, posing as AFGlobal's CEO, persuaded a member of the company's finance team to transfer $480,000 to a bank in China. AFGlobal is currently in litigation with its insurers, who are denying cover.

Should the worst happen

Businesses increasingly accept that it is perhaps inevitable that they will suffer a cyber-breach at some point. The key, therefore, is ensuring that the organisation has a comprehensive response plan in place. It is estimated that only one third of companies have a formal strategy when faced with a cyber-breach. Businesses should give consideration as to who internally is responsible for leading the breach response and the steps that should be undertaken. This response plan should not only deal with remedying the breach and addressing flaws in the business's operations, but also managing the effects of the breach through communicating with stakeholders and, where necessary, self-reporting to regulators.

Contacts

Thomas Webb
Senior Associate

+44 (0)117 307 6976
thomas.webb@burges-salmon.com

Rupert Hyde
Solicitor

+44 (0)117 307 6300
rupert.hyde@burges-salmon.com