PAYNE HICKS BEACH LLP
10 New Square, Lincoln's Inn, London WC2A 3QG

Telephone: +44 (0)20 7465 4300
Fax : +44 (0) 7465 4400
DX 40 London/Chancery Lane

Social Networking Sites: the good, the bad and the ugly

27 September 2011

Jonathan Gatward, partner in our Company Commercial department, considers the issues surrounding social networking sites.

Power and Problems

Social networking sites (SNS) are one of the greatest success stories of the internet age. Daily the spread of their influence grows as more sites appear and more users log-on. To provide a snapshot of their popularity LinkedIn, the professional networking site, has 100 million users and Facebook has 750 million users who spend over 700 billion minutes per month on its site.

For businesses SNS represent both opportunities and potential problems. For small businesses with minimal advertising budgets they offer an effective, free marketing tool. For other businesses they can represent a drain on employee productivity as staff waste time at their desk surreptitiously checking their online profile. However, all businesses whatever their size or sector, which have employees that use SNS, are at risk of security lapses. These can cause reputational damage, potential litigation by clients and make companies an easy target for corporate espionage.

Word of Mouth the SNS Way

Figures published by Marketing Week (13 June 2011) show that 41% of UK companies are using SNS to win new business and that UK companies as a whole are devoting approximately a third of their marketing budgets towards SNS campaigns. The potential of these ready made networks are enormous. For instance successful viral ad campaigns can generate enormous amounts of publicity. To give one example Old Spice's viral video campaign the "Man Your Man Could Smell Like" has been viewed in excess of 20 million times.

However, marketing experts warn against rushing into this new medium without first developing a coherent strategy. Set out below are a few key pointers to help shape your company's approach.

- Monitor SNS sites to establish whether your company is already being talked about. People use SNS to vent their frustrations about companies but also to tell friends and contacts about good products and services. If people are talking about your business then knowing what they are saying will help you to target your approach appropriately and sensitively.
- Ensure that your online approach is consistent with your general marketing strategy and that SNS material is "on message".

PAYNE HICKS BEACH LLP
10 New Square, Lincoln's Inn, London WC2A 3QG

Telephone: +44 (0)20 7465 4300
Fax : +44 (0) 7465 4400
DX 40 London/Chancery Lane

- Make sure that you have the time and resources to keep updating your profile and keep things fresh so users keep returning.
- Increasing numbers of people are using mobile devices so ensure that your websites and campaigns are smartphone optimised.
- Consider carefully which SNS are appropriate to your company. If you want greater interaction with your customers then consider Twitter where one in two users post content daily, by comparison only one in ten Facebook users post content daily.
- Consider what your aim is in using SNS, do you plan to use it as a sales channel, a customer services forum or more as an online notice board updating users about new products and promotions.
- Remember that unlike conventional advertising you don't have a captive audience and SNS users are just one click away from a more interesting screen so try to make content entertaining as well as informative.

A Hackers Dream

SNS are easy to sign up to as all you need is an e-mail address and internet access. This is part of their appeal but also one of the main issues with their usage. There is no authentication of new members so just about anybody can join which makes these networks extremely insecure. Set out below are the key issues to be aware of.

Impersonation

This can involve individuals, companies or brands and even those with no existing SNS profile can fall victim. As a stunt two researchers created a fake profile for Marcus Ranum who is a well known expert on computer security. All it took was a photo and some basic information available about him online to create an account on LinkedIn and within 12 hours he had 42 connections. The dangers in this are obvious, severe reputational damage to an individual or the company they represent could be caused, or confidential business information could be extracted from a connection, all without the victim's knowledge. Abuses can be reported and fake accounts will be deactivated by the service provider but by then the damage could already be done.

Idle Talk

SNS makes the user feel that they are amongst a cosy circle of friends but given that the average user on Facebook has 130 "friends" and the information they post might also be available for the view of their friends' friends this is a somewhat misleading impression. The most common issue is an employee posting derogatory comments about their place of work. Often when the employer gets word of it the employee is fired such as the case of the, now notorious, disgruntled Argos worker in Wokingham. However, by then the negative impression of the employer has already been disseminated. Client confidentiality lapses can also occur. For instance the employees of Genesis HealthCare System in Ohio violated the rules on patient confidentiality by discussing patients and mentioning their room numbers online. As well as being very unprofessional, a client might sue for damages if there has been a breach of the confidentiality owed to them.

There is evidently much naivety in the manner that people use SNS and this is open to exploitation by unscrupulous individuals. The European Network and Information Security Agency (ENISA) published a paper highlighting the burgeoning threat of "social engineering attacks" using SNS (ENISA Position Paper No. 1, October 2007). This is a strategy adopted by hackers to bypass security and access confidential corporate information. There is no technological sophistication in this method as the hackers are targeting a company's weakest security link - their employees. Commonly attacks of this kind will involve the hacker joining an online community which can have very low security settings and then using the insider information available there to build up a picture of the company. As an experiment, Abhilash Sonwane (VP of Product Management and Technology for Cyberoam) gathered

PAYNE HICKS BEACH LLP
10 New Square, Lincoln's Inn, London WC2A 3QG

Telephone: +44 (0)20 7465 4300
Fax : +44 (0) 7465 4400
DX 40 London/Chancery Lane

information on 20 companies using SNS as the resource. Amongst other disclosures, 14 companies disclosed the whole company profile of their organizations including information about employee and business demographics and customers and 8 of the organisations disclosed confidential information such as financial details and announcements about departures in senior management before they were public knowledge.

Hackers may use the information gleaned from these attacks in any number of ways: theft of information about products still in the R&D stage; spying on potential acquisitions, sales and new deals; extracting information in order to hack into corporate networks and cause damage; blackmailing employees; or even accessing physical assets of the company. For such an unsophisticated attack the damage to a company may be extremely high.

Malware and Rogue Applications

The computer security provider, Symantec, warned in its annual threat report that SNS are increasingly being targeted by cyber criminals. In particular, Facebook, Twitter and Google's mobile operating system (Android) are vulnerable to malicious software downloads. Weblinks within SNS encourage users to enter sites that contain malware and rogue applications and what many people don't realise is that you can infect your computer simply by visiting a rogue website. A survey by Sophos, another computer security provider, found that of those SNS users questioned, 40% had been sent malware such as worms, 67% had been spammed and 43% had been subject to phishing attacks, all via SNS. Using these methods cyber criminals collect personal information about an individual or a company which they then use to extract further information or money from the victim.

The potential scale of the problem is demonstrated by the "onMouseOver" Twitter worm, labelled by Sophos as the largest SNS security incident of 2010. This episode was caused by cross-site scripting (XSS) which is the practice of placing code from an untrusted website into another one. In this case, users submitted javascript code as plain text into a Tweet that could be executed in the browser of another user. Pop-up boxes with text appeared when someone hovered over a link in a Tweet. This was developed further by the addition of a code that caused people to retweet the original Tweet without their knowledge. The scale and speed at which the problem developed was astonishing and high profile victims included Sarah Brown and the press secretary to Barack Obama.

A Silver Bullet

Unfortunately, as ENISA concluded in its paper, there is no silver bullet for identifying an attack before it leads to serious damage. The best policy is prevention and ENISA recommends that employers increase employee awareness about their vulnerability in this area and establish a security policy. Many firms block employee access to SNS. However, given that employees are still likely to use SNS at home and reveal details about their professional lives, this isn't really solving the problem and tactics such as this can be seen as heavy handed by employees.

There are a number of precedent security policies that can be downloaded from the internet but the policy must be tailored to fit your company. Below are the main considerations that any company needs to bear in mind when drafting its policy.

- What is the company's overall strategy - is this purely an exercise in damage limitation or does the company want to promote the responsible use of SNS recognising that the networks these create can add value to the company.
- In the context of your company's working environment is the use of SNS by employees likely to impact on their productivity - if the answer is yes you may wish to consider an outright ban (bearing in mind that this could impact negatively on employee morale) or suggest what the company deems to be acceptable use i.e. SNS can only be accessed during lunch breaks.
- How do you wish to define SNS - SNS can encompass a wide range of sites including those that you might not immediately place in the SNS category such as web forums and blogs. Also new

sites are constantly appearing so the wording of your policy should be sufficiently broad to include future as well as current SNS.

- Do you want employees to keep the company name out of their interactions - if the answer is yes then state clearly that employees are not permitted to list the name of the company on any of their SNS and must never register with an SNS using a work e-mail address or set up a blog using a work e-mail address. You also need to be aware that making a distinction between social and professional SNS might not be effective as somebody can easily make the link between the social and professional profiles of an individual.
- You need to identify the information you want kept out of the public domain. This should certainly include any information in respect of which the company is bound by confidentiality undertakings i.e. confidential information about clients, patients etc. However, you may also wish to include information as to the company's clients and business partners as well as all other information that is commercially sensitive such as financial information, product development or research information, intellectual property, potential deals and so forth.
- More generally you may need to remind employees to comply with the law (for example copyright legislation) and the contractual terms of service when using an SNS. They also need to be aware of the dangers of malware and, if accessing SNS from work computers is permitted, then prohibiting the downloading of software or applications might be a sensible precaution.
- Finally you need to state what the consequences are likely to be of any breach of the code i.e. formal disciplinary action and the potential for severe breaches to culminate in the termination of an individual's employment.

A robust security policy is helpful but only effective if employees actually read it and comply with it. Therefore taking the time to educate employees about the real dangers that face your business through inappropriate use of SNS is vital. There are insurance policies available to cover damage caused by attacks of this nature and in some cases litigation might be appropriate. However, it may be impossible to identify the perpetrators as a clever cyber criminal will have no difficulty concealing their real identity in what some are labelling the "SNS Wild West".

September 2011

---

10 New Square, Lincoln's Inn, London WC2A 3QG

DX 40 London/Chancery Lane
Tel: 020 7465 4300 Fax: 020 7465 4400 www.phb.co.uk