

Your trademark looks phishy

This text first appeared in the *IAM* magazine supplement
'Brands in the Boardroom 2005' May 2005
For further information please visit www.iam-magazine.com

Brands in the Boardroom 2005

Key branding issues for senior executives

A supplement to *Intellectual Asset Management* magazine
www.iam-magazine.com

iam

Your trademark looks phishy

While the internet presents many exciting opportunities for brand owners, there are also a number of perils of which they need to be aware. One of the most serious is the ever-growing number of phishing attacks now taking place

By **Jeff Van Hoosear**, Knobbe Martens Olson & Bear, Irvine

Picture a glossy advertisement sent to thousands of your company's customers announcing the grand opening of your company's newest retail location. Numerous customers go to that location and see the same familiar sign, logo and uniform. In fact, everything is familiar, right down to the colour and size of the shopping bag used. Now realise that this location is not one of your company's stores but a clever counterfeit store. A counterfeit so realistic that many of the customers never realise that the store is not authentic. If this happened to your company, you would take immediate action to shut down this store and pursue those persons responsible for this infringing activity. You would also not allow the continued use of your trademark or service mark to confuse customers into providing valuable personal information.

As many companies, particularly service companies such as banks, credit card companies and e-commerce retailers, have become aware, the internet allows counterfeiters to move beyond copycat handbags and fake watches to copy trademarks, logos, even entire websites. Such activity is used to trick internet users into believing that they are responding to a legitimate email (or visiting an authorised site) so that they will provide personal and financial information. The first victim in this online fraud is the company, whose goodwill is used without permission and whose trademark and copyright rights are infringed. The second victim is the recipient of the fake e-mail message who supplies valuable personal information, such as credit card numbers,

passwords and social security numbers, and becomes vulnerable to identity theft. The internet user provides this personal information, either in direct response to the message (phishing), or after being directed (either overtly or covertly) to a bogus website (pharming). In many cases, there is also a third victim, the bank or credit card company used by the consumer.

Looking for bites

The act of sending an email in an attempt to mislead the user into providing personal information is called phishing. According to Webopedia, an online computer dictionary, the word phishing is derived from the concept that bait is thrown out with the hope that some will bite. The spelling of the word phish comes from the fact that computer hackers often replaced f with ph. For example, the original form of hacking was apparently known in the industry as phreaking. By sending fake emails to a number of recipients, the phisher hopes that a certain number of users will be misled. The term pharming is used to describe the situation where your browser shows you are at the correct domain, but you have actually been redirected to a false site that mimics the real site. The user inputs personal or financial information at the fake site, and the information is then collected to be used or resold. Pharming is much more serious, as not only is it more difficult to detect, it also permits the targeting of large groups of users at one time.

While getting people to respond directly to an email with personal information is the original phish, a more recent form of this fraud is the use of the email to contain software that redirects the user to a fake site. The user may be more likely to provide

personal information in this instance because of the technical credibility that the user went to the site on his or her own. This misdirection occurs by the e-mailing of virus or other malicious code that will rewrite a PC's local files. A PC with compromised files will go to the bogus website even if a user types the correct URL in his or her browser.

In each instance, the spoofed website copies the legitimate trademark, logo and other identifying material of the company, and requests the consumer to enter, or perhaps update or verify, information by requesting certain information be re-entered. For example, a website which claims to be a Microsoft website requests the user to enter its user name, password and credit card number to access his or her HOTMAIL account. Anyone who has used HOTMAIL should know that as HOTMAIL is free, no credit card information should be necessary. Unfortunately, many users probably failed to recognise this. In fact, a 2004 study estimated that approximately 3% of internet users revealed personal information to phishing attacks. Given that the average identity theft nets approximately US\$1,500, even a 3% success rate is enough to encourage the online counterfeiters.

In addition to the actual financial losses caused by this fraud, there is the damage done to the company's brand equity and value. A loss of consumer trust or respect ("why does company X allow this to happen?") may also lead to a loss of company goodwill. As brick-and-mortar retailers know, the proliferation of counterfeit goods causes fewer sales of legitimate goods. Online fraud causes direct losses as well as indirect losses, such as the lack of confidence in online transactions. However, the internet is a way of life. Online banking and e-commerce are here despite the rising problem of online fraud and identity theft.

Monitoring intellectual property

Much of the success of the phishers depends on the credibility of the company targeted and the gullibility of the user. Because the gullibility of users may be on the decrease, as they become more savvy in detecting fake emails, online criminals now forego the mass attack approach of spammers and focus more on exploiting the technical vulnerability of PCs, browsers and the internet. Thus, while the technical means by which they get information may change, the criminals must still rely on the credibility of the company targeted. This is why companies should be vigilant in monitoring the internet for abuse and

infringement of their intellectual property. If the online counterfeiters are denied the use of well-known and respected trademarks, their scams are less likely to prove successful.

The Anti-Phishing Working Group (APWG) is an industry association, comprised of the owners of well-known trademarks, which focuses on the problem of phishing. The APWG, whose website can be found at www.antiphishing.org, is an excellent source of information to help companies eliminate (or at least control) the problem of fraud and infringement on the internet. Another group working to control the phishing problem is Digital PhishNet (www.digitalphishnet.org), which is a coalition of companies (Microsoft, AOL, VeriSign, Earthlink) and government agencies (FBI, FTC and the United States Postal Service).

According to APWG, phishing became known in late 2003 and has risen exponentially since that time, with an average monthly growth rate of between 35% and 50%. In April 2004 alone, APWG identified 1,125 unique incidents of phishing. It estimates that between 75 and 150 million phishing emails are sent every day. Thus, the rise of phishing is a serious threat to service providers, their goodwill and their marks.

It appears that credit card companies, which have long battled credit card fraud prior to the use of the internet, have been better equipped to deal with the emergence of online fraud. Banks, and e-commerce retailers such as PayPal, eBay and Amazon.com, have been the hardest hit. Not only do these companies have highly regarded brands, but the type of information these companies would legitimately require from their customers is exactly what the phishers want. The phisher counts on the fact that a consumer will think it normal to give credit card information to Amazon.com in response to a request.

Phishing has reached a very high level of sophistication. The emails no longer contain the obvious misspellings and bad grammar they did just a year ago. For example, the phishers now know that it is eBay and PayPal not Ebay and Paypal. However, the typical messages still include statements that are urgent or upsetting to the recipient, such as "your account will be suspended", "your account has engaged in unauthorised activity", or "a complaint has been filed against your account", in order to get an immediate reaction. The phishers hope that before you have time to realise the email is a scam, you may have taken the bait.

Many phishers must still use awkward grammar or references in order to get past

filters and other protective software. For example, the email may say "online banking information" rather than "your bank account" to avoid being stopped by a spam filter or virus protection software. Being a trademark attorney, I was confident that I could recognise phishing scams, but even I had to admit that the email "Thank you for your order! Your bank account will be charged \$39.95 per month per your authorisation" got an immediate reaction from me. Luckily, I do not have an account at the bank named so I didn't panic, click on the link and subject myself to fraud. I have no doubt that this link would in some manner have attempted to verify my credit card number, security code and billing address. I also have no doubt that many hundreds, if not thousands, of other recipients were tricked by this message. Banks, in fact, are probably the most vulnerable – who doesn't have a cheque account, savings account and debit card? – in phishing scams. In fact, the APWG estimates that 15 of the top 20 scams are aimed at the banking industry. Such activity clearly weakens the brand images of financial institutions.

Taking action

While phishers and pharmers can be prosecuted under wire fraud or other criminal statutes, such prosecution can occur only after the criminal activity has occurred and some consumers have been defrauded. In addition, review of FTC cases to date does not give much confidence that this is an effective procedure to combat phishing. Like store counterfeiter, an online fraud only exists for a few days and moves on. This makes it very difficult to track down and prosecute the online criminals under the more traditional criminal statutes.

In what appears to be a new method of pursuing phishers, Microsoft recently filed lawsuits against 117 phishers using trademark law as a basis for the actions. Microsoft is claiming trademark infringement from the unauthorised use of Microsoft trademarks such as MSN and HOTMAIL in the phishers, fraudulent emails and websites. These suits will permit Microsoft to issue subpoenas to determine the John Does who sent the deceptive emails or were involved in the creation of the fraudulent websites. Hopefully, the success that Microsoft has in these legal actions will permit others to go forward with similar suits to curtail trademark infringement and fraud.

As the Lanham Act allows for statutory damages up to US\$100,000 per mark, or up to US\$1 million per mark if the court deems the fraud to be wilful, this could be a powerful deterrent to online fraud. In addition, in

exceptional cases, the courts may also award attorneys' fees. Certainly one would hope that courts would find that the fraudulent use of trademarks to steal personal and financial information is exceptional.

Another tool that could become available to trademark owners is the Anti-Phishing Act of 2005, introduced in March by Senator Patrick Leahy. This bill calls for criminal penalties for two of the essential elements of phishing: (1) the creation or procurement of websites with the intent to gather information to be used for fraud or identity theft; and (2) the creation or procurement of email that represents to be from a legitimate business. The bill would impose fines as high as US\$250,000 and also impose jail terms of up to five years against criminals creating fake websites or email designed to defraud consumers.

Practical measures

What can you, the trademark owner, do to prevent phishing? The best line of defence is to educate your customers on certain basic facts, such as legitimate e-mails will always be addressed personally, not generically to "Dear User" or "PayPal Account Holder". You can also look at services provided by those familiar with trademark protection. For example, NameProtect (www.nameprotect.com) offers a product called VigilActive which monitors the internet to uncover fake websites as soon as possible after they are launched.

According to Mark McGuire, NameProtect's founder and president, NameProtect is currently working with several financial companies and a number of luxury brands to protect against fraud and counterfeiting in the online environment. Thomson & Thomson (www.thomson-thomson.com), another well-known name in the trademark protection field, also offers a product called Web Monitoring to help companies protect their trademarks from abuse and infringement on the internet.

Companies need to be proactive in warning their clients and customers of fraudulent e-mails and websites, as well as providing details of what their own legitimate e-mail content will (and will not) contain. Good examples of such consumer education can be found on eBay (look for Email and Websites Impersonating eBay, under eBay Policies), US Bank (check out Email Fraud: Information and Help) and Citicorp (Learn About Spoofs). The companies, which have been the focus of many phishing scams, are working diligently to stop online fraud.

Steps the trademark owner should take to help detect and prevent phishing activity include:

- Educate your consumers that emails will always be personalised.

- Remind your consumers that sensitive information is never solicited by email.
- Provide an easy-to-use address for your consumers to forward what they think are suspicious emails so you can investigate (ie, spoof@ebay.com).
- Consistently monitor the use of your company's trademarks and other key content (such as slogans) on the internet either in-house or via a company (like Thomson & Thomson or NameProtect) which can provide such services for you.
- Monitor the internet for fraudulent variations of your company's name and domain name.
- Register similar domain names so that consumers do not confuse them with the legitimate website.
- Establish your domain name as a trademark of your company to take advantage of provisions in the Anticybersquatting Consumer Protection Act (ACPA).

Steps which the trademark owner should take to respond to phishing activity include:

- Contact the ISP of the illegitimate website and demand it be shut down immediately and the identity of the owner be disclosed.
- Report the incident to the Federal Trade Commission (FTC).
- Report the incident to the Internet Fraud Complaint Center (which is a collaborative effort between the FBI and the National White Collar Crime Center).

The time and money it takes to prepare and send fraudulent emails, or set up fraudulent websites, are so minimal that companies need to pursue the online criminals aggressively to help deter this activity. Microsoft's recent example of legal action may send out the message that trademark owners will step in to curtail the attack on their brands and goodwill.



Knobbe Martens Olson & Bear LLP

2040 Main Street, 14th Floor,

Irvine, CA 92614, USA

Tel: +1 949 760 0404

Fax: +1 949 760 9502

Other offices:

San Diego, San Francisco, Los Angeles,

Riverside, San Luis Obispo

www.kmob.com

Jeff Van Hoosear

Partner

jvh@kmob.com

Mr Van Hoosear is head of the trademark department and a partner at Knobbe, Martens, Olson & Bear, LLP. He specialises in international trademark and unfair competition matters. Mr Van Hoosear has spoken extensively in the field of trademark and copyright law including presentations for the Computer Law Association/ILATID conference and AIPLA. Mr Van Hoosear published a series of articles on trademark issues in both World Trade magazine and the International Trade and Business newsletter.