



# Kaspersky Lab White Paper

## Hook, Line and Sinker

### *Phishing scams and how to avoid getting caught!*

Hardly a day goes by without some online news reference to 'phishing', sometimes also known as 'carding' or 'brand spoofing'. But what is it, how does it work and what are the effects?

Phishing [a conscious misspelling of the word 'fishing'] is a specific form of cyber crime. It involves tricking computer users into disclosing their personal details [username, password, PIN number or any other access information] and then using these details to obtain money under false pretences. It's fraud: Data theft, followed by theft of money.

Phishers relies heavily on 'social engineering' techniques. This is just a fancy way of describing non-technical breaches of security that rely on human interaction: Tricking users into breaking normal security measures.

Social engineering is commonly employed by writers of viruses and worms as a way of beguiling unsuspecting users into running malicious code. This might mean attaching a virus or worm to a seemingly innocent email message. The LoveLetter worm, for example, arrived as an email with the subject line 'I LOVE YOU' [and who doesn't like to receive a love letter?] and the body text 'Kindly check the attached LOVELETTER coming from me'. In an effort to put unsuspecting users further off their guard, the attachment had a double extension [LOVE-LETTER-FOR-YOU.TXT.vbs]: by default, Windows does not display the second [real] extension. This double extension trick has been used by lots of viruses and worms since, including SirCam, Tanatos and Netsky.

Another social engineering technique is to construct an email to look like something that's positively beneficial. The Swen worm, for example, masqueraded as a cumulative Microsoft patch, manipulating users' growing awareness of the need to secure their operating system from attack by Internet worms. Such 'sweet' emails are not the only form of social engineering. We've seen instant messaging [IM] items containing links to infected web pages, for example.

In the case of phishing scams, the criminal creates an almost 100% perfect replica of a chosen financial institution's web site. The criminal then goes 'phishing', using spam methods to distribute an e-mail that imitates a genuine piece of correspondence from the real financial institution. Phishers typically use legitimate logos, good business style and even make reference to real names from the financial institution's senior management. They also spoof the header of the email to make it look like it has come from the legitimate bank. In general, these letters inform customers that the bank has changed its IT structure and is asking all customers to re-confirm their user information. Occasionally, the letters cite network failures, or even hacker attacks, as reasons for requiring customers to re-confirm their personal data.

The fake email messages distributed by phishers have one thing in common: they're the bait used to try and lure the customer into clicking on a link provided in the letter. If the bait is taken, the luckless 'fish' stands in serious danger of divulging confidential information that will give the criminal access to his or her bank account. The link takes the user directly to an imitation site that mimics the real bank's web site very closely. This site contains a form that the user is told they must complete: and in doing so, they hand over all the information the criminal needs to access their online account and steal their money.

As you'd expect, phishers target organisations that handle significant numbers of customer financial transactions online. Naturally, this includes all the major banks, together with other organizations [such as Amazon, AOL, BestBuy, eBay, MSN, PayPal and Yahoo]. It's hardly surprising that providers of financial services continue to be the main target, given that the ultimate aim of phishers is to steal money.



Of course, in any single phishing scam, it's likely that only a small proportion of those who receive the fake email will be customers of the spoofed bank or other organization; and only a small proportion of them may 'take the bait'. However, as with spam email, the perpetrators send out such large volumes of fake messages that even a low response is likely to harvest enough data to make scam worthwhile. In this sense, the term 'trawling' might be more appropriate than phishing.

Personal financial data isn't always the phisher's target. So-called 'spear phishing' is designed to lure a corporate user into revealing confidential data that can be used to gain wider access to a corporate system. Typically, the phisher spoofs the email address to make it look like it has come from someone 'important' within the enterprise [the HR department, IT support, etc.] and personalizes the e-mail to make it look even less suspicious. When an off-guard user responds, the phisher is then able to use the information to gain access to corporate assets.

Since most phishing attacks make use of social engineering, the forms of attack are many and varied. For example, 'mophishing' offers a subtle alternative to the 'standard' email-based phishing attack. Here the phishers cash-in on users' fears about responding to emails and ask them to send confidential data by fax. The unsuspecting user is conned into believing that it's the method [i.e. the *online* transaction] that's insecure and is asked, as a 'safer' alternative to confirm their personal details by fax. Unfortunately, it's the data that is valuable to the cyber criminal, irrespective of the means they use to get it!

There are high stakes involved. Estimates of the losses resulting from phishing scams vary [search online and you can find figures ranging from \$400 million to \$2.4 billion]. However, it seems clear that the number of phishing attacks, and the associated costs, are increasing. In April 2006, the number of unique phishing web sites detected by the [Anti-Phishing Working Group](http://www.antiphishing.org/) (APWG) was 11,121, a significantly higher number than in previous months and the highest recorded by APWG. And while the number of unique phishing reports was down on the month before [to 17,290] it remains significantly higher than a year ago.<sup>1</sup>

As if this weren't enough, the problem doesn't necessarily end with direct costs. Some phishers also place exploits for Microsoft Internet Explorer [IE] vulnerabilities on their sites. When the victim follows the link to the fake web site, the exploit is used to upload a Trojan to their machine. As a result, not only is the user's banking information harvested, but their machines become unwilling 'soldiers' in a 'zombie' army that can be used for further malicious activities: as part of a DDoS [Distributed Denial of Service] attack designed to extort money from a victim organization, for use as a platform for spam distribution or for use in the distribution of a virus, worm, Trojan or 'spyware' program.

Not bad for a day's phishing!

It's hardly surprising that phishing has attracted considerable media attention during the last two years or so. At the same time, financial institutions now provide advice to their customers about the potential dangers. The result is that users are becoming increasingly wary. So phishers continue to look for ever more sophisticated ways of luring users into giving up their personal banking information.

Some phishers now make use of vulnerabilities [or unwanted features] to make their scams less obvious. For example, an Internet Explorer [IE] vulnerability documented by Microsoft in late 2003 allowed a phisher to create a fake web site that not only has the right 'look-and-feel' of a legitimate financial institution, but displays the correct URL in the IE browser window. So when the user clicks on the link in the phisher's email, the web browser displays content from the fake web site, but the URL in the browser window is that of the legitimate bank. This vulnerability is explained fully on the [Microsoft](http://support.microsoft.com/?id=833786) (<http://support.microsoft.com/?id=833786>) web site, together with tips on how to identify spoofed web sites.

Alternatively, the phisher may actually load a legitimate web page, but then display a pop-up window over it that asks the user to key in their personal information. In this case, the dangerous pop-up looks like a legitimate request from the bank.

<sup>1</sup> Figures taken from the APWG [Phishing Trends Activity Report](http://www.antiphishing.org/reports/apwg_report_apr_06.pdf) ([http://www.antiphishing.org/reports/apwg\\_report\\_apr\\_06.pdf](http://www.antiphishing.org/reports/apwg_report_apr_06.pdf)), April 2006.



It's common for phishers to disguise the link they distribute in an email: the real destination is disguised beneath a link that looks legitimate [and you only see the real destination if you hover over the link with your mouse]. This provides a solid reason to use plain text e-mail, rather than HTML, and to disable scripting on your machine. Be careful though. It's possible to hide a dangerous link even in a plain text e-mail. Consider the following URLs:

<http://www.kaspersky.com/>  
<http://www.kaspersky.com/>  
<http://www.kaspersky-antivirus.com>  
<http://www.kasperksy.com>

They all look innocuous enough. But only one is legitimate. By transposing letters, missing out letters, replacing a letter with a number [an 'l' for a '1', for example] it's possible to catch the unsuspecting user unaware and lure them into clicking on a link.

More and more phishers seek to re-direct users to fake web sites without the need for the user to click on a link at all. In November 2004, phishers began to exploit the fact that it's possible to embed script instructions [including exploit instructions] within HTML that will execute automatically when an email message is read. The phishers send out HTML emails containing scripted instructions to edit the hosts file on the victim's machine. As a result, when the user next directs their browser to their bank's web site, it is automatically re-directed to the fraudulent web site, where any input can be captured. The user hasn't clicked on a link. And they have no reason to think that they aren't accessing their bank's web site as normal. Yet they still become a victim of the phishers.

Phishers also make use of Trojan programs to 'automate' this re-direction process. The Trojan may be spammed directly to a pre-defined PC population. Or it may be downloaded when the victim visits a web site. Or it may be installed by some other malicious program [a worm, for example]. Once installed on the victim's machine, the Trojan either edits the hosts file or modifies the DNS server settings to re-direct specific [or all] look-ups to a fraudulent web server. This server will typically deliver appropriate content most of the time, but is able to re-direct selective requests to a fake web site. The user doesn't click on a link and has no way of knowing that the requested data has been falsified.

Phishing is a specific cyber crime that relies heavily on 'social engineering', non-technical breaches of security that focuses on human interaction: in other words, tricking users into doing something they shouldn't. As such, phishing is a moving target. Cyber criminals are continually trying to find new ways to catch users off-guard. This may include new technological developments. Or it may simply mean using some topical 'hook' to beguile users.

For this reason, it's impossible to provide a definitive list of phishing characteristics. So the following is intended to highlight some of the main characteristic of phishing emails and to provide some general guidelines on how to minimize the risk of getting 'hooked' by the phishers:

- Be very wary of any email message asking for personal information. It's highly unlikely that your bank will request such information by email, or that a corporate IT department would ask you to confirm a system login or password. If in doubt, call them to check!
- Don't use links in an email message to load a web page. Instead, type the URL yourself into your web browser.
- Don't complete a form in an email message asking for personal information. Only enter such information using a secure web site. Check that the URL starts with 'https://', rather than just 'http://'. Look for the padlock symbol in the lower right-hand corner of the web browser and double-click it to check the validity of the digital certificate. Or, if you're in any doubt, use the telephone to transact your business.
- Check to see if your anti-virus program blocks phishing sites, or consider installing a web browser tool bar that alerts you to known phishing attacks.



- Check your bank accounts regularly [including debit and credit cards, bank statements, etc.], to make sure that listed transactions are legitimate.
- Make sure that you use the latest version of your web browser and that any security patches have been applied.
- Report anything suspicious to your bank immediately!
- Check any dates, mentioned in the body of the e-mail. Be wary of any email that contains a reference to a date that has already passed: for example, if the deadline specified for you to take action has already passed.
- Be suspicious if an email is not addressed to you personally: for example, if it begins 'Dear Valued Customer', or something similar.
- Be suspicious if you are just one of several recipients. If your bank does communicate with you about your personal bank account, it will not send the email to others also.
- Look for spelling mistakes in simple words, or for poor grammar, syntax and other clumsy use of language.

For more information on avoiding phishing scams, and what to do if you think you have wrongly disclosed personal information, check out the APWG's [Consumer Advice on Phishing](http://www.antiphishing.org/resources.html) (<http://www.antiphishing.org/resources.html>)

### **About Kaspersky Lab**

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers.