

## **Phishing, phaxing, vishing and other identity threats: The evolution of online fraud**

Fraudsters and scammers are finding increasingly devious ways of stealing financial and other confidential information. Anything they can learn about online credentials can seriously undermine an organization's profile, bring considerable risk to its reputation, and incur legal liability. This paper describes the online fraud of phishing, looks at other methods it has spawned, and gives advice on how organizations can prevent the theft of their identity.

# Phishing, phaxing, vishing and other identity threats: The evolution of online fraud

## Introduction

The growth in online shopping and banking has been matched by increasingly widespread risk. Financial motivation has led to an explosion of tactics designed to trick users into divulging their usernames, passwords and other confidential information which can then be used to commit a wide range of crimes based on identity fraud. A typical goal is to clean out the victim's bank account, but the information is also often used to help phishers commit further fraud or gain unauthorized access to networks.

The most well-known scam is "phishing", a hackers' term that comes from the scam's parallels with fishing, with fake emails and websites acting as "bait", and the victims' confidential information being the netted "phish". In phishing attacks,

*In January 2007, 135 brands were hijacked by phishing campaigns.<sup>1</sup>*

scammers spam out authentic-looking emails that claim to come from well-known legitimate institutions. The recipient is encouraged to click on a website link in the email. On doing so they are taken to a bogus (or "spoofed") site that is virtually indistinguishable from the real thing.

Even though only a small percentage fall prey to the trick, the phishers can make a significant

amount of money while the site is up and running – the average length of time for a phishing site to remain online is just four days, according to industry association the Anti-Phishing Workgroup (APWG)<sup>1</sup> Considering the low cost of setting up a website and sending out thousands of emails, only a relatively few victims are needed to turn the trick into a profitable scheme.

The success of phishing campaigns can be seen in just a couple of examples. A gang of phishers in Brazil was said to have stolen \$4.6 million from approximately 200 online bank accounts,<sup>2</sup> while in February 2007, 17 members of a gang were arrested in Turkey accused of breaking into online bank accounts and stealing \$300,000 from internet users.<sup>3</sup>

Initially, targeted institutions were restricted to a handful of financial and e-commerce organizations such as Citibank™, America Online™, PayPal™, or eBay™. In July 2006, 75 percent of phishing emails were targeting the last two organizations alone.<sup>4</sup> Now, however, the fraudsters' net has spread much wider taking in social networking and gambling sites among others. In January 2007, the APWG identified 135 brands that had been hijacked by phishing campaigns that month.<sup>1</sup>

## An international crime

A report by IBM reveals that US-based businesses are the most targeted organizations of phishing emails, accounting for 71.37 percent of all phishing email. It also shows that more than half

(55.78 percent) of the world's phishing attacks have fake websites that are hosted in the US.<sup>5</sup>

Nevertheless, as the examples cited earlier show, phishing is an international problem. Often the phishers find it hard to move stolen money out of a country without leaving a trail, so further spam emails may be sent to help them recruit “mules” – computer users who are promised a fee in return for allowing money to pass through their account. In April 2007 authorities in Singapore were reported to be investigating a group of “money mules” suspected of laundering money for an international crime syndicate to accounts in Russia and Latvia.<sup>6</sup>

### A growing threat

There has been a surge in the number of reported phishing attacks. The APWG's January 2007 report revealed an increase of 67.4 percent in phishing attacks over the same month in 2006. There were 29,930 reports pointing to 27,221 unique phishing URLs. October 2006 had an even higher number of unique URLs – 37,444.<sup>1</sup>

### Phishers' tricks

Most methods of phishing use some form of technical deception designed to make a link in an email (and the website to which the link leads) appear to belong to the spoofed organization.

*95 percent of phishing emails rely on HTML delivery.<sup>5</sup>*

Many tricks are used to fool computer users into thinking they are reading a genuine email – using the graphics, fonts and logos found in genuine emails from the targeted organization is common.

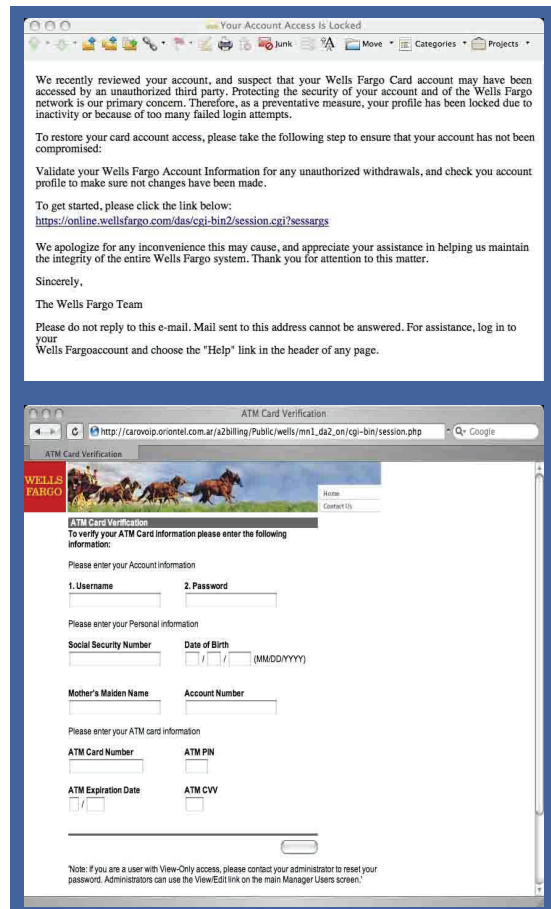


Figure 1: Spammed email linking to bogus website

Aside from the appearance of the email, phishers use sophisticated social engineering techniques to lower the recipient's guard. Messages often include an urgent call to action, perhaps claiming that “your account may have been accessed by unauthorized persons”, or claiming that the recipient has won a prize. Some, like those linking to bogus websites related to the Hurricane Katrina relief efforts,<sup>7</sup> rely on emotional persuasion, and some even pose as a warning against phishing.

## Subverting URLs

Some previously successful types of URL, for example those that used the @ symbol to allow for the inclusion of a username (e.g. <http://www.sophos.com@www.phisher.com>) have been disabled in Microsoft's Internet Explorer, while the Mozilla and Opera web browsers present a warning message. Nevertheless, there are numerous methods still in operation and still highly successful.

Common tricks include misspelt URLs and/or use of subdomains, such as <http://www.sophas.com> or <http://www.sophos.example.com>, rather than <http://www.sophos.com>. Another common trick is to make the anchor text for a link appear to be a valid URL when the link actually goes to the phisher's site. In an HTML email (and 95 percent of phishing emails rely on HTML delivery<sup>5</sup>) this is relatively simple to do – standard HTML code can be used to make the text of the link say anything, regardless of where it actually leads to.

Further problems with URLs come from users believing that the website they are visiting is genuine. Internationalized domain names (IDN) that can contain non-ASCII characters allow visually identical web addresses to lead to different, possibly malicious, websites. For example, the character "l" can be an upper case I, a lower case L or the number 1. Another way phishers mislead even careful web users, is to subvert open URL redirectors on the websites of trusted organizations to disguise malicious URLs within a trusted domain. So what appears to be a legitimate redirect actually takes the user to the wrong website.

## Using scripts

Once a victim visits a deceptive website the deception is not over. Some phishing scams use JavaScript commands in order to alter a browser

address bar. Alteration may be done by placing a picture of a legitimate entity's URL over the address bar or by closing the original address bar and opening a new one containing the legitimate URL.

A particularly difficult method of phishing to spot is where a phisher uses a trusted website's own scripts against the victim. Cross-site scripting attacks direct a user to sign in at a bank or other organization's own web page, where everything from the web address to the security certificates appears correct but is bogus. There are also tools available that help phishers convincingly reproduce a website and capture any log-in details entered at the fake site.

## Poisoning Domain Name Servers

Organizations can protect themselves against all the above scams by using up-to-date security solutions. However, there is one form of attack (sometimes called "pharming") which cannot be detected in this way. Albeit extremely difficult to achieve and therefore rare, pharming attacks redirect a legitimate website's traffic to another (bogus) website. This is done by hijacking (or "poisoning") the victim's Domain Name Server (DNS) and changing the address of the target website from its real IP address to the IP address of the fake website. So the victim can enter the web address properly and still be unknowingly directed to the fake website.

## Trojans, spyware and downloaders

In the cases above, the victim is taken to a bogus website and then keys in a range of details which allow the phisher to use their identity. There is also a growing threat from the use of Trojans, which are downloaded from the infected website on to visitors' computers. These Trojan downloaders pull down the spyware code from the website,

which then unbeknownst to the victims captures their confidential information as they key it in and surreptitiously shares it with the criminals. The malicious code is changed frequently – sometimes several times a day – in an attempt to evade detection.

### Phishing's evolution – vishing and phaxing

As computer users become wise to these web-based scams, we are now seeing the emergence of other ways of stealing details. In voice phishing, or “vishing”, scammers use VoIP (Voice over IP) to build bogus switchboard systems, mimicking those of genuine online banks and other organizations. Emails are spammed out, claiming to come from an online company but rather than including a link to a bogus website as in a “traditional” phishing attack, the email instead gives a phone number that the recipient should call (see Figure 2). The phishers can then steal information from the innocent victim.

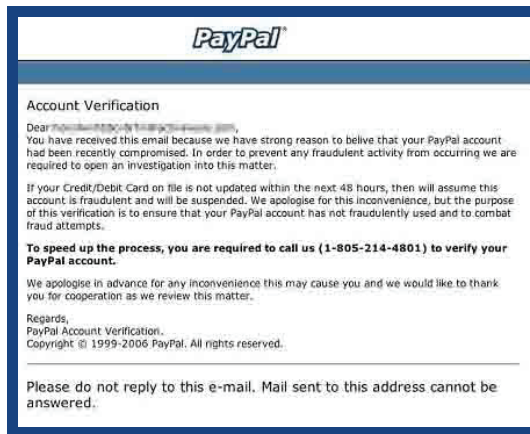


Figure 2: Example of vishing email

Phaxing (fax phishing) works in an identical way except that the victim faxes back a form with their

Figure 3: Example of phaxing – part of the faxback form

data instead of calling a phone line, as can be seen in Figure 3.

What is particularly devious about these methods is that they do not ring any alarm bells. First, most people do not know the phone or fax numbers of their favorite companies or banks. In addition, people generally trust phones and faxes and even if they were to question whether the email was a scam, they would assume that no fraudster would go to the lengths of setting up a phone number and switchboard or fax number to perpetrate crimes.

### What organizations can do now

There are several ways in which the chances of a successful phishing attack on an organization's IT infrastructure or a personal computer can be minimized. The top rule is – if something seems implausible or too good to be true, then it probably is. There are some general best practice rules that

IT and other departments can follow:

- Keep your systems patched and up to date with security software at the email and web gateways, and install a personal firewall against backdoor Trojans.
- Use sender-authentication technologies, such as Sender Policy Framework (SPF) to make phishing far more difficult since – in theory at least – phishers will only be able to send their spams from “unapproved” domains.
- Enforce a password policy so that passwords cannot be easily guessed and are changed at regular intervals. If a phisher manages to steal one password and the same password is used for all websites, then all your online activity is at risk. 41 percent of respondents to a Sophos poll reported using the same password for all websites.<sup>8</sup>
- Pay attention to advice from organizations like getsafeonline<sup>9</sup> and from providers like eBay and PayPal, both of which, for example, have issued advice.<sup>10,11</sup>
- Always report suspicious activity.

There is also a range of advice that organizations can give to their end users:

- Never respond to emails requesting confidential information.
- Be cautious about opening attachments and downloading files, no matter who appears to have sent them.

- Visit banking and e-commerce websites by typing the URL into the address bar (although, as described above, this will still allow you to be infected if the DNS has been poisoned).
- Check the website you are visiting is secure and legitimate. If it is on a secure server it should start with “https://” (“s” for security) rather than the usual “http://”, and a lock icon on the browser’s status bar will show that the information being sent is encrypted. However, it is important to realize that both these indicators show only that the data is being encrypted before transmission; they are not a guarantee that the website itself is legitimate – phishing sites can be set up on secure servers too.

## Conclusion

In a very short space of time, online identity theft has become a real threat to organizations’ reputation and to business continuity. Part of the fast-changing and increasingly complex threat environment, phishing has been worked and honed by cybercriminals who have found, and continue to find, increasingly devious ways to exploit network vulnerabilities and human foibles. Only by combining end-user awareness with robust best practices and consolidated security solutions can organizations expect to stay one step ahead of the fraudsters.

---

## The Sophos solution

Sophos protects organizations from phishing attacks at the email gateway through highly flexible, scalable software solutions and managed email appliances, all of which block malicious spam before it can get onto the network and individual computers. Sophos web appliances enabling safe and productive web browsing, blocking malicious sites, stopping spyware from being downloaded and protecting against other malware. Sophos Client Firewall, part of Sophos Endpoint Security and Control, prevents hackers stealing information at the desktop. Sophos products incorporate Behavioral Genotype® Protection, which blocks malicious code before it executes, proactively protecting against new threats. Sophos ZombieAlert Service lets organizations know if any of their computers have been hijacked to send out spam. In addition, Sophos PhishAlert lets organizations know in near real-time if their brand has been used in a phishing campaign. All products are backed up by 24/7 support.

## Sources

- 1 Phishing activity trends, Anti-Phishing Working Group, January 2007, [www.antiphishing.org](http://www.antiphishing.org)
- 2 [www.sophos.com/pressoffice/news/articles/2006/02/brphishgang.html](http://www.sophos.com/pressoffice/news/articles/2006/02/brphishgang.html)
- 3 [www.sophos.com/pressoffice/news/articles/2007/02/hackergang.html](http://www.sophos.com/pressoffice/news/articles/2007/02/hackergang.html)
- 4 [www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html](http://www.sophos.com/pressoffice/news/articles/2006/07/top-phishing-targets.html)
- 5 IBM Internet Security Systems X-Force® 2006 Trend Statistics, IBM Corporation, January 2007, [www.iss.net/x-force\\_report\\_images/index.html](http://www.iss.net/x-force_report_images/index.html)
- 6 [www.sophos.com/pressoffice/news/articles/2007/04/sing-phish.html](http://www.sophos.com/pressoffice/news/articles/2007/04/sing-phish.html)
- 7 [www.sophos.com/pressoffice/articles/2006/08/hurricane-phisher.html](http://www.sophos.com/pressoffice/articles/2006/08/hurricane-phisher.html)
- 8 [www.sophos.com/pressoffice/news/articles/2006/04/passpoll06.html](http://www.sophos.com/pressoffice/news/articles/2006/04/passpoll06.html)
- 9 [www.getsafeonline.org](http://www.getsafeonline.org)
- 10 [pages.ebay.com/education/spooftutorial](http://pages.ebay.com/education/spooftutorial)
- 11 [https://www.paypal.com/cgi-bin/webscr?cmd=\\_vdc-security-spoof-outside](https://www.paypal.com/cgi-bin/webscr?cmd=_vdc-security-spoof-outside)

## About Sophos

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
WWW.SOPHOS.COM