

# >PHISHING FOR VICTIMS

## TRUTH, MYTH & CYBER-CRIME

>AUTHOR MATHEW NISBET, MALWARE DATA ANALYST,  
MESSAGELABS

MessageLabs



## >CONTENTS

>EXECUTIVE SUMMARY	>1
>INTRODUCTION: EVOLUTION IN ACTION	>2
>PHISHING FACTS, PHISHING MYTHS	>3
>LIFE BELOW THE SURFACE	>4
>THE ORIGIN OF THIS SPECIES	>5
>CLASSIC PHISHING	>5
>MORPHING INTO MALWARE	>6
>SPEAR PHISHING: HITTING THE TARGET	>7
>BLUNT THE THREAT	>9

## >EXECUTIVE SUMMARY

First emerging in the mid-1990s, the term 'phishing' describes a range of criminal activities designed to steal confidential data via computer systems and then use this data or sell it for a profit.

Whether the stolen information consists of valuable intellectual property, customer data, bank account or credit card details, usernames or passwords, the bottom-line damage suffered by businesses falling victim to phishing attacks can be enormous.

Traditional, 'deceptive' phishing involves sending fake emails that pretend to come from trustworthy organisations. These emails entice the victim to click on a link to a fake webpage where they are instructed to enter sensitive information.

A significant proportion of phishing, though, is now malware-based, with the malware surreptitiously installed onto the victim's machine using a variety of methods and secretly feeding data back to the phishers via the internet.

'Spear' phishing is a relatively new sub-species of phishing in which targeted attacks are launched against specific organisations or even individual employees selected by the phisher. Data used to craft such an attack and maximise its chances of success is primarily gathered from the internet itself (company websites, social networking sites etc).

MessageLabs hosted services equip businesses to defend themselves effectively from the full range of phishing threats. Operating across all protocols, they offer benchmark anti-phishing protection, whatever vector cyber-criminals use and whatever method of deception they try to harness.

## >INTRODUCTION: EVOLUTION IN ACTION

In the mid-1990s, a new word entered the language. This quirky, harmless-looking term simply replaced the 'f' in 'fishing' with a 'ph'. Yet the activity it described was blatantly criminal – the distribution of electronic communications ostensibly from a trustworthy source, but actually designed to dupe recipients into giving away their bank account or credit card details, usernames and passwords to computer hackers.

## PHISHERS ARE IMMERSED IN THE WORLD OF INDUSTRIAL ESPIONAGE.

Phishing, then, was really just another byword for trickery, deception and the determination to make money at someone else's expense. Initially, it was a more or less homogenous species of cyber-crime. Fool your victim (whether a business, a public sector body or a private individual) into giving you sensitive information. Use the data to gain access to their funds. Take the funds.

Since those early days, though, phishing has remorselessly evolved, diversifying and steadily transforming into an umbrella term with a multiplicity of evolutionary offshoots – each of which represents a subtly different weapon wielded by today's highly professional cyber-criminal fraternity.

The age-old objectives of fraud and theft are still in evidence, with stolen data widely used in identity scams and the creation of false bank accounts for money-laundering, for instance. But now phishers are also immersed in the world of industrial espionage, harnessing increasingly ingenious ways of gaining access to computer networks, stealing intellectual property and other confidential data (the life blood of the cyber-criminal) and turning it into profit.

Whatever the phisher's precise purpose, every time they succeed, one thing is absolutely certain. An organisation somewhere in the world stands to suffer a brutal blow to its balance-sheet, market share, investor confidence and/or corporate reputation. Phishing is far from being a victimless crime.

This White Paper examines the phenomenon of phishing. It explains the potentially catastrophic threat it presents to all kinds of organisation. Exploding some widespread myths, it lights up the murky waters where phishing first emerged and where it continues to evolve. But it also highlights what your business can do to blunt the threat.

The information presented here is based on MessageLabs hosted services' experience of providing messaging and web security management services for over 19,000 clients and 8 million end-users worldwide, with approximately 3 billion attempted SMTP email connections and 1 billion web requests processed each day on their behalf.

## >PHISHING FACTS, PHISHING MYTHS

During its decade and a half of existence, some widely-held myths have inevitably grown up about phishing and the threat it poses. In some cases, the myths reflect a one-time but now outdated truth. In others, the underpinning belief has always been irrational. But the myths have one characteristic in common: their presence within your organisation can weaken your defences in the face of a phishing attack – with disastrous consequences.

**FALLING PREY  
TO PHISHING  
JUST ONCE  
CAN LEAD  
TO ENORMOUS  
DAMAGE .**

### ***Myth 1: “It won’t happen to me”***

Complacency is the sworn enemy of internet security. And while it’s true that, statistically, you’re less likely to receive a phishing email than spam, the scale of the problem shouldn’t be underestimated.

Analysis of internet traffic processed by MessageLabs hosted services shows that malware-based phishing accounts for around 600 million emails worldwide every day – in addition to the huge volume of traditional, non-malware-based phishing emails circulating the globe.

Two further facts should also be borne in mind. First, phishing is a classic ‘relatively low percentage, very high impact’ threat – falling prey to just one such email can result in big, big damage. Second, the very fact that phishing emails are not as numerous as spam, and are sometimes highly targeted, can mean they find it easier to slip through conventional internet security defences.

### ***Myth 2: “As long as I’m vigilant, I’ll be OK”***

Not so. In today’s cyber-crime environment, sceptical handling of every item in an email or instant messaging inbox is no longer enough to guarantee security. Such is the sophistication of many of the tools phishers now deploy, even the most computer-savvy individual can fall prey to phishing.

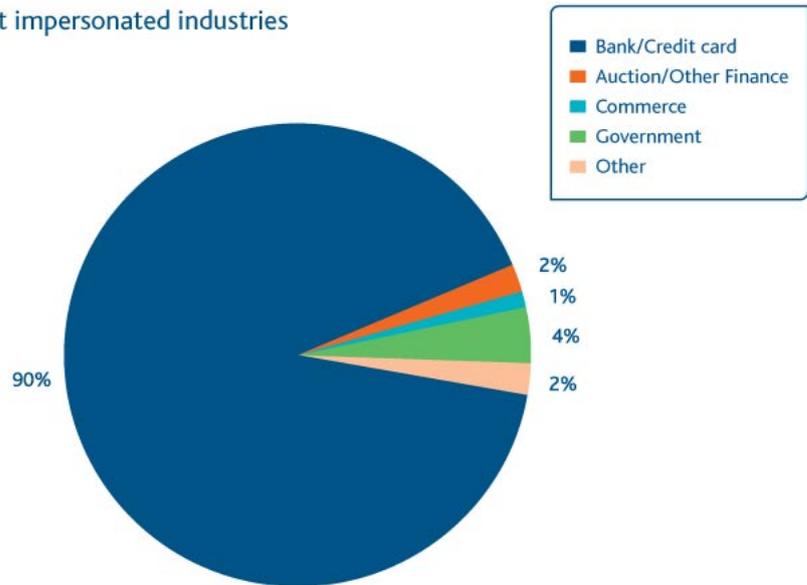
For instance, completely legitimate websites can be deliberately infected with phishing malware as a result of an SQL (Structured Query Language) injection attack. Simply visiting such a site could result in the malware automatically and secretly downloading itself onto your computer in a so-called ‘drive-by download’. Even the presence of a padlock icon in the browser window may not be a guarantee that a website is clean from infection – or indeed genuine.

### ***Myth 3: “Phishing consists of fake emails from banks”***

False. It’s certainly the case that, ever since phishing first appeared, phishers’ stock-in-trade has been emails masquerading as communications from banks asking for sensitive information. But phishing sub-species also now include emails purportedly sent by a range of other organisations such as government agencies and online retailers:

A LOT OF PHISHING IS NOW MALWARE-BASED.

Most impersonated industries



Furthermore, a significant proportion of phishing is now malware-based, with the malware installing itself onto victims' computers in a variety of ways and with a variety of objectives, as we will see. MessageLabs hosted services block around 1.5 million malware-based phishing attempts in a typical week.

The key point is that phishers are constantly devising and implementing new ways to deceive. And these co-exist with tried and tested methods, as well as older techniques given a modern twist – for example, the abuse of VOIP (Voice Over Internet Protocol) technology discussed later in this paper.

#### **Myth 4: "Phishing's a blunt instrument"**

Again, not so. Certainly, many phishing runs are indiscriminate and use mass-mailing techniques (i.e. emails fired out rapidly by botnets). But the key to maximising success, from the phishers' point of view, lies in their ability to impersonate someone (a) you trust and (b) who could have a plausible reason to ask you to disclose sensitive information.

And as this paper highlights, phishers can go to considerable lengths to achieve this, mining key data about potential victims from the internet and elsewhere, and using this to craft highly convincing attacks closely targeted at a specific company, department or individual. It really can be all too easy to become yet another victim of these carefully camouflaged predators.

#### **>LIFE BELOW THE SURFACE**

The murky depths inhabited by cyber-criminals are a largely hidden world where all kinds of internet threats are created and incubated before being unleashed. In this sense, phishing is no different from other breeds of internet-borne danger. Like them, it has developed into what is now an extensive and diverse array of closely related but nevertheless distinct tools and techniques.

**'PHISHING'  
NOW INCLUDES  
AN EXTENSIVE  
ARRAY OF  
DIFFERENT  
TECHNIQUES.**

**>THE ORIGIN OF THIS SPECIES**

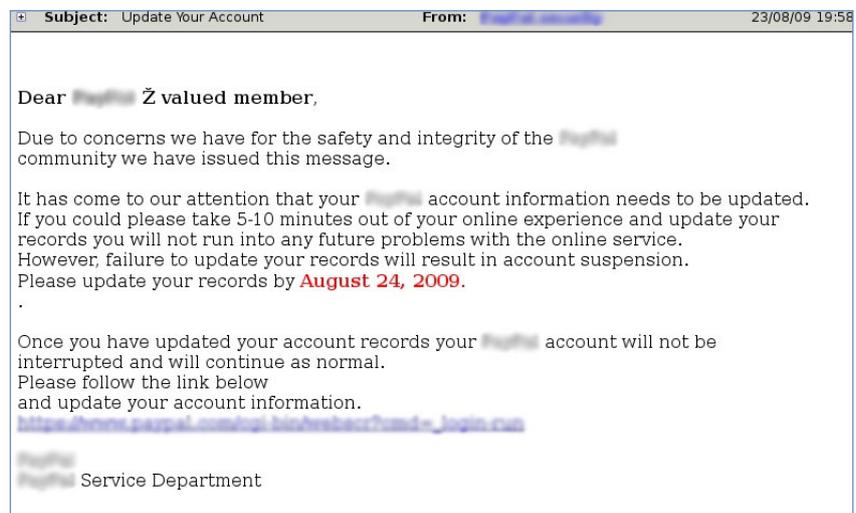
Phishing first crept into the light around 1996. Its initial form involved attempts to obtain login credentials for AOL accounts. The attack vector was usually the AOL instant messenger service, with phishers impersonating AOL employees in a bid to convince account owners to divulge login details or billing information. These first-wave phishers then used the compromised accounts to sell and disseminate 'warez' – software illegally copied and/or 'cracked' (i.e. modified to remove means of copy protection, serial numbers etc).

Soon phishers began to embrace email as their preferred attack vector. Moreover they recognised the huge potential profits that could be gained from online payment systems and bank accounts – indeed, anywhere offering a means of access to somebody else's money.

**>CLASSIC PHISHING**

The first known phishing attack on an online payment system took place in 2001. By this time, the phishers' preferred and most commonly used modus operandi – dubbed 'deceptive phishing' – was becoming firmly established.

Deceptive phishing generally involves sending out a bulk email or instant message fraudulently claiming to come from a reputable organisation. The message encourages the recipient to click on a weblink leading to an equally fake webpage set up by the phisher. Once there, the victim is asked to provide confidential data which the phisher can then record, keep and use – perhaps to siphon funds from the victim's bank account or buy goods on their credit card.



The email above is a typical specimen. Impersonating a well-known online payment service, it's not a very sophisticated example. It doesn't, for instance, incorporate any logos or other authentic touches to strengthen the illusion that it originates from its purported source.

But the key to such an email's effectiveness is the fact that the address in the weblink (which is a genuine address) is not the same as the address that the victim will actually be taken to if they click on the link. The latter address, however, will usually closely spoof the genuine address (e.g. by adding an extra character somewhere) in the hope that it won't raise any suspicions in the victim's mind.

## THE VICTIM IS TAKEN TO A WEBSITE DESIGNED TO STEAL ANY DATA THEY ENTER.

### >MORPHING INTO MALWARE

Inevitably, the very success of deceptive phishing as a data theft tool sowed the seeds of its own (relative) demise. Computer users grew more alert to the danger and its hit rate began to decline. In response, phishers introduced even more potent, malware-based techniques to achieve their objectives.

Rather than trying to dupe the victim into handing data over directly, malware can be used to pinpoint valuable information on the victim's machine and send it to the phishers via the internet. There are many ways in which such malware can infiltrate a computer. The victim may be enticed into clicking on an infected email attachment or visiting a malicious website. Or they may be infected when visiting a legitimate but compromised site. Once on the victim's machine, the malware can set about its work. At first, the victim will almost certainly be totally unaware of its presence and the damage it's doing.

The most common forms of malware-based phishing involve:

- **Activity loggers:** these monitor what the victim is doing on their computer. They can record keyboard/mouse input, or even what's on the computer screen. Usually, they simply track internet activity and only become active when a particular website is visited, recording login details etc.
- **Session hijacking:** again, internet activity is monitored. When the malware detects that the victim is logged-in to an online banking site, for example, it 'hijacks' the authenticated session and performs transactions as if it were the user.
- **Host file poisoning:** whenever a URL (Uniform Resource Locator) such as www.company.com is entered into a computer, it's translated into an IP (Internet Protocol) address using the Domain Name System (DNS). Many operating systems have a shortcut or 'host' file that the computer checks before contacting a DNS server. Malware has been devised that alters host files, causing them to give wrong IP addresses. Instead of the site they requested, the user is taken to a legitimate-looking website which has the correct URL in the browser window, but is in fact a malicious site designed to steal any data they enter.

### >LATEST VARIATIONS

Ever-imaginative and opportunistic, cyber-criminals are constantly looking for new ways of bolstering their already extensive repertoire – especially as computer users get wise to their existing battery of tricks and traps.

The advent of free VOIP services, for example, has enabled phishers to extend their classic 'deceptive phishing' technique into the realm of the spoken word. First, they set up an automated telephone system imitating those used by many banks and financial institutions. An invitation to call the system is then contained in a fake email. On making the call, the potential victim is asked to divulge account numbers, PIN codes, passwords etc in response to a recorded list of questions. In some cases, though, the systems call the victims – and sometimes the phishers even dispense with an automated system and make the calls themselves.

Underpinning this brazen technique is the assumption that people aren't yet aware that telephone systems can be abused by phishers. So they aren't likely to check a phone call's authenticity before divulging confidential information. The fallout from the global financial crisis has also helped make the phishers' task easier. The plethora of bank mergers and takeovers during the last year or so means unsolicited phone calls from sometimes unfamiliar financial institutions are less likely to ring warning bells than in the past.

### >SPEAR PHISHING: HITTING THE TARGET

## METHODICAL PLANNING AND TARGETING CHARACTERISE SPEAR PHISHING.

Arguably the most potent breed of phishing to have emerged recently is so-called 'spear phishing'. This phenomenon involves attacks directed at specific organisations or even, in some cases, particular people within them. Spear phishing's potency derives from two key characteristics: first, the attacks are extremely difficult to spot; second, they can wreak significant – and frequently business-compromising – damage.

The aim is usually to infiltrate an organisation's computer system by bypassing its security systems. Once achieved, the options for the phisher are almost limitless: misappropriate confidential data, disrupt the organisation's operations, recruit its computers to a botnet – the list goes on.

But it's the methodical planning and targeting that really distinguish this breed from other types of phishing. From the phisher's perspective, the key is to maximise the chances of a 'bite' by sending highly plausible communications. This means making sure they appear to originate from someone the victim would expect to receive communications from – and that the topic it feigns to address is one the victim would expect that person to contact them about.

So where does the vital data needed to set up a spear phishing attack come from? Quite simply, most comes from the internet itself. It's easy to underestimate the sheer volume of publicly available and phish-friendly data – about company structure, areas of expertise, board members etc – now circulating in the online world.

It's not just company websites that are a data goldmine. Social networking sites also host an incredible array of information about people, their jobs and their lives that can lend credibility to phishing attacks.

In view of their value for social engineering purposes, then, it's not surprising that these sites are themselves a regular target for phishers, enticed by the ocean of data available, plus of course potential access to social networkers' 'friends' lists.

So let's put a typical spear phishing attack under the microscope:

#### **1) Identify Target**

The first step is to pinpoint a potential victim and define the purpose of targeting them. A company with a unique product that is doing particularly well, for example, might make a tempting target, with the phisher's strategy being to steal confidential data about the product and sell this to competitors.

**THE TARGETS ARE MOST LIKELY TO HAVE ACCESS TO THE MOST VALUABLE DATA.**

The phisher will visit the company's website, read its publications and perhaps phone the company masquerading as a general enquirer – the real aim being to find out the names of employees who can be targeted. The individuals selected are generally executives and senior managers as they are most likely to have access to the most valuable data.

### **2) Select Method of Attack**

Next the phisher decides exactly how to gain access to the company's computer system and the data they want to steal. For example, they might:

- Impersonate someone (e.g. an employee of an outsourced IT department) who might plausibly ask the target for their user details, which can then be used to infiltrate the system.
- Impersonate someone who might plausibly send a certain type of file to the target. For instance, they could pose as a print company representative sending a pdf containing examples of the company's work, but actually infected with phishing malware.
- Build a relationship of trust with the target. While difficult to do, this tactic can pay big dividends. Again, the key is to pose as someone with good reason to contact the target – perhaps someone in a similar role at a different (possibly fictitious) company. Once initial emails have been exchanged, the phisher will calculate the right moment to send a file with a malicious payload which the target will open without suspicion.

### **3) Craft Attack**

Crafting the attack will require knowledge both of the company and of the individual being targeted. As noted above, this type of information is freely available. The means of communication with the target will typically be a carefully tailored email using the target's name and title, and discussing a topic relevant to their role in some way.

### **4) Unleash Attack**

The email is sent. This may be a simple request for user details, after having gained the target's trust, but it could also carry a payload – usually a word processing document, spreadsheet, or other common type of file. Many of these formats can easily be infected with malicious code. Once the file is opened, the code activates and installs itself on the target's machine.

### **5) Reap Rewards**

Now with access to all kinds of confidential data, the phisher will work quickly before the security breach is noticed and corrective action is taken. They will waste no time looking for something of potential value (product designs, customer lists etc), copying it and selling it to the highest bidder in the cyber-crime community. The phisher wins. The victim – and their company – loses. Game over.

## >BLUNT THE THREAT

Phishing, then, has evolved into a multiplicity of forms. Moreover, it will certainly continue to do so. The key to keeping your business safe from the threat is to invest in a solution that can block all messages containing phishing characteristics, infected attachments or links to infected websites, as well as all requests to visit websites contaminated with phishing malware, or that have been made to impersonate legitimate websites. Unfortunately, traditional internet security solutions struggle to deliver this level of capability.

## MESSAGELABS HOSTED SERVICES CAN HELP TURN PHISHING INTO AN ENDANGERED SPECIES.

MessageLabs hosted services are different. Operating across all protocols (email, web and IM), they offer cost-effective, benchmark protection preventing phishers from gaining access to your network and your confidential information, whatever vector they use and whatever deception techniques they try to harness.

Key to this capacity to instantly stop existing threats and block new ones at zero-hour is Skeptic™, MessageLabs proprietary predictive technology. Skeptic™, too, constantly evolves, relentlessly learning and growing in strength, maintaining leading-edge understanding of phishing characteristics and detecting even one-off phishing attacks, no matter how artfully devised.

So the predator becomes the prey. The hunter becomes the hunted. Opting for MessageLabs hosted services really can help turn phishing into an endangered species.

Find out more about MessageLabs fully managed internet security services – call us today or visit [www.messagelabs.co.uk](http://www.messagelabs.co.uk)

>WWW.MESSAGELABS.CO.UK  
>INFO@MESSAGELABS.COM  
>FREEPHONE UK: 0800 917 7733

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom  
Tel +44 (0) 1452 627 627  
Fax +44 (0) 1452 627 628  
Freephone 0800 917 7733  
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor  
40 Whitfield Street  
London, W1T 2RH  
United Kingdom  
Tel +44 (0) 203 009 6500  
Fax +44 (0) 203 009 6552  
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam  
Zuidplein 36/H-Tower  
NL-1077 XV  
Amsterdam  
Netherlands  
Tel +31 (0) 20 799 7929  
Fax +31 (0) 20 799 7801  
Support +44 (0) 870 850 3014

>BELGIUM/LUXEMBOURG

Symantec Belgium  
Astrid Business Center  
Is. Meyskensstraat 224  
1780 Wommel,  
Belgium  
Tel: +32 2 531 11 40  
Fax: +32 531 11 41  
Support +44 (0) 870 850 3014

>DACH

Feringastrasse 9a  
85774 Unterföhring  
Munich  
Germany  
Tel +49 (0) 89 203 010 300  
Support +44 (0) 870 850 3014

>AMERICAS

>HEADQUARTERS

512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA  
Tel +1 646 519 8100  
Fax +1 646 452 6570  
Toll-free +1 866 460 0000  
Support +1 866 807 6047

>CENTRAL REGION

7760 France Avenue South  
Suite 1100  
Bloomington, MN 55435  
USA  
Tel +1 952 886 7541  
Fax +1 952 886 7498  
Toll-free +1 877 324 4913  
Support +1 866 807 6047

>CANADA

170 University Avenue  
Toronto, ON M5H 3B3  
Canada  
Tel :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza  
18 Harbour Road  
Tower II  
Wanchai  
Hong Kong  
Main: +852 2528 6206  
Fax: +852 2526 2646  
Support: +800 901220

>AUSTRALIA

Level 13  
207 Kent Street,  
Sydney NSW 2000  
Main: +61 2 8200 7100  
Fax: +61 2 8220 7075  
Support: +1 800 088 099

>SINGAPORE

6 Temasek Boulevard  
#11-01 Suntec Tower 4  
Singapore 038986  
Main: +65 6333 6366  
Fax: +65 6235 8885  
Support: +800 1204415

>JAPAN

Akasaka Intercity  
1-11-44 Akasaka  
Minato-ku, Tokyo 107-0052  
Main: + 81 3 5114 4540  
Fax: + 81 3 5114 4020  
Support: + 531 121917

© MessageLabs 2009  
All rights reserved



Confidence in a connected world.