Phishing and the threat to corporate networks

A Sophos white paper

August 2005

SUMMARY

This paper explains the online fraud known as phishing, examining how it threatens businesses and looking at the dramatic rise in the number of attacks over recent years. Phishing methods and tricks are described and ways of protecting computers and networks from phishing attacks are discussed.

What is phishing?

Phishing, an increasingly common form of online theft, is the act of tricking computer users into handing over control of their online accounts using, typically, a combination of a forged email and website. "Phishing" is a hackers' term that comes from the scam's parallels with fishing, with the fake emails and website acting as the "bait", and the victims' accounts as the netted "phish".* Phishing is done by spamming out authentic-looking emails that claim to come from a well-known financial or e-commerce institution such as Citibank™, PayPal™, eBay™ or America Online™. These emails contain different messages, but usually follow the same formula: the recipient is asked to click on a link contained within the message, taking them to what appears to be a legitimate website. In fact, the website is a clever forgery, often virtually indistinguishable from the real thing.

The majority of phishing emails will be ignored. However, only a few victims are needed to make the scam turn a profit.

The senders of these phishing attacks know that the vast majority of recipients will have no dealings with the organization named in the email and disregard it. However, for the phishers, the probability that a small percentage will be account holders at the targeted organization makes it worthwhile. Even if only a tiny percentage fall prey to the trick, the phishers can make a significant amount of money while the site is up and running – most phishing sites last only a few days before being shut down. Considering the low cost of setting up a website and sending out thousands of emails, only a few victims are needed to turn the trick into a profitable scheme. Phishers are able to convince up to 5% of recipients to respond according to the Anti-Phishing Working Group (APWG). The APWG is an industry association, of which Sophos is a member, focused on eliminating the identity theft and fraud that result from the growing problem of phishing. For more information visit www.antiphishing.org.

An international crime

Once the victim has entered their data onto the fake website, the phishers can use it as they please. The usual goal is to clean out the account, but there are many other uses for the scam. Depending on the type of account which has been compromised, it can be used to help phishers commit further fraud or gain unauthorized access to networks. International phishers may 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. Sophos has reported on a scam in which innocent people were being asked to help phishers move their funds, under the guise of a money-making opportunity.[1]

Why businesses are vulnerable

Phishing represents one aspect of the increasingly complex and converging security threats facing businesses today. The methods used by spammers have become more sophisticated, and spam is now increasingly combined with malware and used as a tool for online fraud or theft, or to propagate malicious code.

Phishing is just one of a number of email-borne threats that can compromise network security.

This convergence is well illustrated by the use of malicious code by phishers. Sophos has reported on one example in Brazil, where 53 people were arrested on suspicion of remotely installing Trojan horses on users' computers without their knowledge. The Trojans ran in the background,

*The "ph" spelling is something of a tradition in hacking terminology. It dates back to the 1970s when the first hackers began breaking into the US telephone system to make free calls, an activity they named "Phone Phreaking".

monitoring the users' login details when they visited certain online banking sites, and secretly passed the information on to thieves.[2] This is an example of phishing without using a forged website – all that is needed is a spam email which attempts to install the malicious code secretly. Another phishing technique, also reported in Brazil, involved using a secretly installed Trojan to redirect an affected user's internet browser to a phishing site, even when the legitimate URL of the online bank was typed into the address bar.[3]

So phishing can be considered a combined threat, part of a fast-changing and increasingly complex threat environment facing networks, which can encompass spam and various kinds of malware.

Although consumers are the main targets of phishers, a phishing attack can damage the reputation and credibility of the affected business, putting brand equity at risk and leading to significant costs. Smaller businesses, meanwhile, may be more directly at risk of falling victim to email fraud, particularly where the corporate accounts are controlled by one or two people who may not have a great deal of technical knowledge. While this is less likely with larger organizations, it is clearly preferable for employees to be protected from fraud attempts arriving in their inboxes via the corporate network.

It is therefore important that businesses use an integrated, robust solution to defend their email gateway from spam such as phishing attacks and the many other varieties of email-borne security threat.

A growing threat

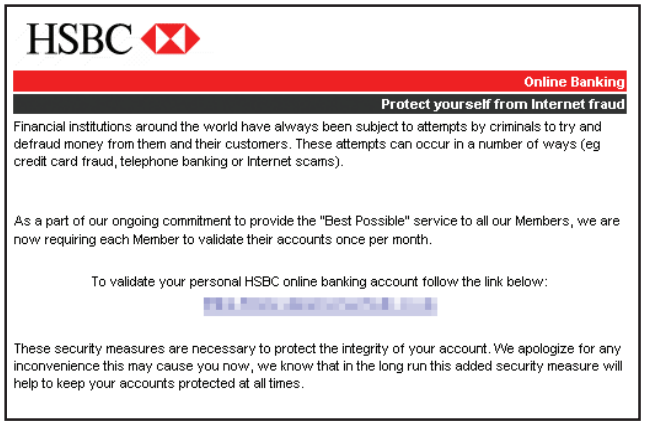
There has been a surge in the number of reported phishing attacks. The Anti-Phishing Working Group tracked over 3,326 unique phishing sites in May 2005, with that number rising by an average of 28% per month since July 2004. According to a survey released by research group Gartner in June 2005, over 2.42 million US adults reported losing money in phishing attacks, amounting to nearly $929 million in the past year.[4] Another report in October 2004 by research group IDC cited phishing as one of the fastest growing non-violent crimes.[5]

How to avoid being phished

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. Careful checks and the exercise of caution when dealing with online accounts is vital. Avoid responding to emails requesting confidential information. Reputable companies do not ask their customers for passwords or account details in an email. Even if you think the email may be legitimate, never respond – contact the company by phone or by visiting their website. Be cautious about opening attachments and downloading files, no matter who appears to have sent them. 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. These tricks are designed to lull the recipient into a false sense of security, but it can be difficult for even the most wary user to spot a forged email. In a test of 200,000 email users, fewer than 10% were able to distinguish phishing messages from legitimate email all of the time.[6]

Tricks used to fool recipients range from warnings about their account security to invitations to collect prizes.

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 even pose as a warning against phishing. **Figure 1** shows an example of this which targets online account holders at HSBC bank.


HSBC

Online Banking

Protect yourself from Internet fraud

Financial institutions around the world have always been subject to attempts by criminals to try and defraud money from them and their customers. These attempts can occur in a number of ways (eg credit card fraud, telephone banking or Internet scams).

As a part of our ongoing commitment to provide the "Best Possible" service to all our Members, we are now requiring each Member to validate their accounts once per month.

To validate your personal HSBC online banking account follow the link below:

These security measures are necessary to protect the integrity of your account. We apologize for any inconvenience this may cause you now, we know that in the long run this added security measure will help to keep your accounts protected at all times.

Figure 1: Part of a phishing email aimed at HSBC account holders.

Visit banking and e-commerce websites by typing the URL into the address bar

Many reputable companies, including Sophos, provide links in customer emails, for example with links to news stories. The important factor to look out for in phishing attempts is the request for personal confidential data. However, if you suspect an email from your bank or online company may be false, do not follow any links embedded within it – type the address instead. Various tricks are used to dupe recipients into clicking on a phisher's URL.

One of the simplest is to make the phishing URL closely resemble the legitimate one, for example by adding a hyphen,

a dot or using a different domain name. Another technique involves making the bogus link exactly resemble the real one. In an HTML email 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.

One way to check that a link is not misleading is to look at the URL displayed in the bottom of the browser frame (status bar). However, only a certain number of characters can be displayed. This means that if a long enough URL is used, it can be disguised by starting it off with what appears to be a legitimate address and placing the "active" part – which actually directs the browser to the fake site – at the end of the string and hidden from view. An example might be www.anybank.comabcdef123456789etc@phishingsite.com. In this example, all that would be visible in the status bar would be www.anybank.com followed by some of the extra characters.

These issues were addressed in a Microsoft Critical Update in February 2004, but unpatched browsers are still vulnerable. A vulnerability also exists in some Internet Explorer and Mozilla browsers which (if unpatched) allows the legitimate website's URL to be displayed in the address bar even when the phishing site is being viewed.[7] So it is important to keep software updated with security patches. However, even patched browsers may still have as-yet undiscovered vulnerabilities or flaws that phishers could exploit.

Check the website you are visiting is secure and legitimate

Before submitting your bank details or other sensitive information there are some visual checks that you can do. For example, to help ensure the site uses encryption to protect sensitive data:

- Check the web address in the address bar. If the website you are visiting is on a secure server it should start with "https://" ("s" for security) rather than the usual "http://".
- Look for a lock icon on the browser's status bar. You can check the level of encryption, expressed in bits, by hovering over the icon with the cursor.

However, it should be noted 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. You can also check that the URL you see in the address bar corresponds with the actual URL of the website you are visiting by checking in the properties. To do this in Internet Explorer, right click with the mouse on the website, select "properties" and compare the URL displayed in the pop-up box with the one shown in the address bar. By making sure that the two URLs correspond, you can also help protect against another favorite trick used in phishing sites. It makes the forged site look like a pop-up window and opens it up with the real website in the background. When the requested data has been entered, the victim is transferred over to the real website, completing the illusion that nothing illegal has happened.

Keep a regular check on your accounts

Regularly log into online accounts, and check statements. If you see any suspicious transactions, report them to your bank or relevant company.

There are a number of visual checks that can help determine whether the website you are visiting is legitimate.

Be cautious with emails and confidential data

Most banks have a security page on their website with information on carrying out safe transactions, along with the usual advice relating to confidential data: never let anyone know your PINs or passwords, do not write them down, and do not use the same password for all your online accounts. Avoid opening or replying to spam emails as this may give the sender confirmation that they have reached a live address. Use common sense when reading emails. If something seems implausible or too good to be true, then it probably is.

Always report suspicious activity

If you receive an email you suspect is not genuine, forward it to the organization it fraudulently claims to have come from. Many companies have a dedicated email address for reporting such phishing attempts.

Legislation against online criminals is having an effect – there have been arrests of suspected phishers in several countries, including the UK and Brazil, while in Australia an email scammer who stole millions of dollars in an email fraud was sentenced to five years in prison.[8]

Keeping computers secure

The threat of Trojans being used in phishing attacks raises the possibility of a "backdoor" being opened to allow attackers access to the affected computer or network. To combat this, installing a personal firewall will provide some measure of protection. As we have seen, keeping operating systems up to date with the latest security patches is also important in countering some of the phishing tricks already described, such as disguising headers and URLs. However, firewalls and patches will not stop users entering their details onto a forged

site if they have been duped, and will not protect against the discovery by phishers of any further vulnerabilities in the future.

Using sender-authentication technologies may also help reduce the effect of phishing attacks. One such method is Sender Policy Framework (SPF). Under SPF, organizations publish lists of servers which are allowed to send emails on their behalf. Any email which claims to come from an organization but does not originate from a server on its "approved" list can therefore be rejected. While SPF and other sender authentication technologies are fairly new, they have the potential to make phishing far more difficult since – in theory at least – phishers will only be able to send their spams from "unapproved" domains. The challenge with authentication alone is that while a recipient may be able to verify that a sender's address is not spoofed, the recipient also needs to know if they actually trust messages from that domain, and that it is not, for example, used by a known spammer.

Organizations who choose a security solution which is backed by 24-hour global anti-virus and anti-spam labs are in the best position to protect themselves reliably from rapidly evolving combined threats such as phishing and other attacks. The most important step a business can take is to use an integrated gateway security solution to protect its IT infrastructure. Sophos PureMessage™ guards the email gateway, giving award-winning protection from viruses, spam and the Trojans used in phishing attacks. PureMessage also provides policy enforcement, giving organizations protection against malware attacks, and also gives them liability protection, allowing them to meet regulatory compliance and increase productivity. PureMessage employs Genotype™ spam detection technology, which provides pre-emptive protection against variants of spam campaigns even before specific detection is made available.

A suite of management tools enables Sophos PureMessage to be easily installed and updated, and 24-hour technical support is available with every license. In addition SophosLabs™, a global network of threat analysis centers, ensures a rapid response to threats anywhere in the world, irrespective of time zone.

Subscribe to Sophos PhishAlert Service

Even the most security-conscious organizations can become the target of a phishing attack – phishers don't require access to a network to launch a successful campaign. So, while security solutions such as anti-virus and anti-spam software are the first line of defense, they may not offer total protection.

Based on SophosLabs' extensive network of spam traps and expert analysis, Sophos PhishAlert™ Service provides rapid notification of phishing attacks detected by Sophos that target an organization's customer base. Message samples and additional information on the website owners are provided in the alerts to help customers quickly respond to the attack by shutting down the fraudulent website and communicating with their customers. This service most obviously benefits financial institutions and online retailers, but other organizations with an online presence should also subscribe to the service, especially those who conduct a significant portion of their customer transactions online. Phishing attacks are also broadening out to target other customer bases such as charity donors. Sophos PhishAlert Service can also assist government and law enforcement efforts against identity theft by providing information on the hosts of phishing sites.

For more information on how Sophos can protect your business, visit www.sophos.com.

Sources

1 www.sophos.com/spaminfo/articles/phishrecruit.html ["Phishers recruit UK computer users into stealing money, 'Don't be a mule' says Sophos," 3 November 2004].

2 www.sophos.com/virusinfo/articles/brazilarrest.html ["53 arrests as Brazil cracks down on phishing Trojan authors, Sophos comments on online bank fraud," 21 October 2004].

3 msnbc.msn.com/id/6416723 ["A new, more sneaky phishing attack". By Bob Sullivan, 5 November 2004].

4 "Increased Phishing and Online Attacks Cause Dip in Consumer Confidence". By Avivah Litan, Gartner, 22 June 2005.

5 www.idc.com/getdoc.jsp?containerId=AP223108L ["Security Threats in Asia/Pacific (Excluding Japan) 2004"].

6 www.informationweek.com/showArticle.jhtml?articleID=48800408 [Deceptive E-Mail Could Cost Consumers $500 Million, Study Finds". By Thomas Claburn, 30 September 2004].

7 www.millersmiles.co.uk/identitytheft/phishing.html ["Spoof Email Phishing Scams and Fake Web Pages or Sites". By Mat Bright, 23 February 2004].

8 www.sophos.com/spaminfo/articles/marinellis.html ["Email scammer who stole over £2 million sent to jail, Sophos reports," 8 November 2004].

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

SOPHOS
WWW.SOPHOS.COM