

# Branch Communications Ltd

## PHISHING FOR THE UNAWARE

### **SYNOPSIS**

The good news for all legitimate businesses is that the amount of SPAM being sent out is decreasing, thanks to improved software and increased awareness. Sources indicate that the ratio of SPAM to legitimate email decreased to 67% in June last year.

The bad news is that the number of phishing scams is rapidly rising, because of the ease in which unsuspecting email users can be persuaded to divulge personal information. Phishing is much more than frustrating and worthless – it can lead to the theft of sensitive personal data such as account numbers, card numbers and passwords.

Phishing scams use fraudulent e-mails and phoney websites to trick email users into disclosing personal data. Phishers send emails that are, to all appearances, from legitimate companies with whom the recipient has a relationship, such as their bank. The email will include a reasonable request to authenticate personal data (which the legitimate company will already have) - with a veiled threat of consequences for not providing the requested information. Many recipients feel intimidated into following the links to fake websites, where they unwittingly providing scam artists with information to steal their identity.

It is believed that there have been 57 million phishing attempts in the past twelve months. Those at most risk of losing revenue and customers are banks and companies trading on-line. In this internet age, it's vital for all banks and businesses trading on-line to understand phishing and how to protect their customers and business from it.

### **INDEX**

#### **Phishing Explained**

- Social Engineering
- Technical Subterfuge

#### **Phishing in Practice**

- Technical Tools

# Branch Communications Ltd

- Spear phishing

## **The Reality of Phishing**

### **Spot the Phish**

- Phishing content
- Phish camouflage

### **Battle against Phishing**

- Corporate responsibility
- Preventative Technical Measures

## **Branch Communications**

### **PHISHING EXPLAINED**

Phishing is the use of increasingly sophisticated means to “fish” for people’s identities. Once upon a time, this was done over the phone or in person. Now, with the internet playing a major role in every day life, phishing takes place on-line. Anyone entering an email address into a legitimate website form is vulnerable to attack. Email addresses can be cheaply and easily captured from various internet sources and contact lists using spiders.

### **SOCIAL ENGINEERING**

A social engineering phishing scam is based on deceit, with often millions of scam emails being sent to unwary email users. With large numbers of potential victims being targeted, the attacker can rely on a proportion of recipients (often up to 20%) being persuaded to surrender personal and financial information.

Phishing email messages will appear to come from any bank, credit card company or on-line store - basically from any trustworthy brand or reputable organisation with whom a person may have a registered account, and to whom they would have supplied financial information when registering or purchasing on-line. In fact, phishers often use a genuine email from the legitimate company as a template for the phishing email, to increase its credibility.

As the attachments, pop ups or website links in these emails appear to be authentic and legitimate, many recipients are tricked into disclosing the sensitive personal

## **Branch Communications Ltd**

information they think is being justifiably requested by a company they know. Threats such as closure or suspension of accounts provide an added incentive. Phishers can then use the passwords, dates of birth, credit card numbers or on-line banking details supplied to make on-line purchases, apply for credit cards, transfer money into other accounts and ultimately steal consumers' identities.

### **TECHNICAL SUBTERFUGE**

Of increasing concern is technical subterfuge. This form of phishing involves even more than phoney emails and websites, by intercepting legitimate communications between the business and the email user. Technical subterfuge makes use of spyware, surreptitiously planted onto PC's, to steal cookies entered by unwary internet users whilst on-line, such as websites visited and keystrokes used. Phishers are then able to logon to customer accounts using stolen cookies.

### **PHISHING IN PRACTICE**

Worryingly, social engineering scams commandeer legitimate websites to appear credible to the recipients of fraudulent emails. Using various means of technical deception, phishers make emails and linked websites appear to belong to the scammed company.

### **TECHNICAL TOOLS**

#### **1) Unauthorised links to image files on the company server**

Phishers often establish fake websites that feature a collection of official logos and graphics. These are not copied, but are hyperlinked directly to the image files hosted on the legitimate company website. These copycat sites are also called "spoofed" Web sites.

#### **2) Links to unofficial websites**

To make phishing e-mail messages look even more credible, the phisher may include a link that appears to take the recipient to a legitimate web site, but in actual fact directs the recipient to a bogus website or pop-up window. This will look exactly like the legitimate site, but will have been established solely to steal the user's information.

## Branch Communications Ltd

### 3) Links to official websites

Often, phishing emails and websites feature unauthorised referrals to real pages on the legitimate company's website. Website content appropriated in this way, particularly privacy policies or terms and conditions, provides victims with a false sense of security and deceives them into believing that they are indeed on a legitimate website.

### 4) Cross site scripting attacks

Phishers may also create emails and websites that feature a mix of content from the legitimate website and phishing. In this popular method of phishing, a phisher uses a company's own scripts against the victim. These types of attacks are of particular concern, as the user signs into their account at their bank or service's real web pages, where everything from the web address to the security requirements appear correct. Users may receive a message saying that they have to "verify" their account, by following a link to what appears to be an authentic website; in reality, the link takes them to a false data capture form. This is very difficult to spot without specialist knowledge.

## SPEAR PHISHING

The first examples of phishing emails were dispersed indiscriminately, in the hope that they would reach at least some customers of the bank or company being scammed. For example, eBay were targeted in 2003 by a scam in which customers received emails supposedly from eBay, stating that the user's account would be suspended unless he clicked on the included link and updated the credit card information that eBay already held. The phishers targeted a large number of people, in the hope that a percentage actually had accounts with eBay and would be tricked into verifying their credit card information on what was actually a fake site.

Now, phishers can establish which companies a potential victim has dealings with, and thus send targeted emails which are more likely to be acted upon. This is known as spear phishing.

# **Branch Communications Ltd**

## **THE REALITY OF PHISHING**

The Anti-Phishing Working Group suggests that phishing scams grew by 25% per month in 2004. Particularly vulnerable to this growing threat are customers of banks and companies that trade on-line – who regularly input sensitive personal data. The internet may have transformed the financial services sector more radically than any other. However, the internet has also exposed it to the greatest risk of criminal attack, such as phishing.

Phishing not only puts consumers at risk of identity theft and financial loss, but puts businesses at commercial risk through fraudulent transactions, lost custom and fewer (more cost effective) on-line transactions. Phishing leads to irreparable damage to a company's brand and reputation, as customer confidence in on-line security and the legitimate company crumbles.

Phishing is increasingly sophisticated, and yet easier than ever – phishing tools can even be downloaded from the internet. Therefore, it's vital for businesses, particularly those at greatest risk in the financial services sector, take action to protect their customers and themselves.

AOL is just one major organisation fighting back against the growing problem of identity theft, by launching a campaign to educate their customers, and request their feedback. It's also working with an on-line security company to identify and monitor suspected phishing sites, and to protect customers by blocking access to website that attempt to spoof legitimate companies.

## **SPOT THE PHISH**

At first glance, recipients of phishing emails will think that they have received a legitimate email from a company with whom they do business. However, although phishing is becoming increasingly sophisticated in line with technology and experience, it's easy to spot phishing traits with practice.

## **PHISHING CONTENT**

## Branch Communications Ltd

Firstly, phishers use phrases which any reputable company would and must avoid. These may include “verify your account”, “update your personal information”, or “change your password for increased security” – which no bank or ecommerce business would ask their customer to do through email.

Phishers will always be courteous, yet intimidating. They will insist email recipients follow a hyperlink to provide their personal information, with threats that accounts will be blocked or closed if they don't take action. Many unwary recipients respond to this without realising that any reputable business with which they have a relationship would not approach them in such a manner.

Most companies address their customers by their name or user name in emails. However, phishing emails are sent out in large numbers and are rarely personalised (even though phishers no doubt have this information). An email addressed in a generic fashion such as “Dear valued customer” and asking for personal details is not to be trusted.

### PHISH CAMOUFLAGE

Most phishing emails contain links to forms on websites or pop ups, where personal data is collected, as with many legitimate websites and emails. However, JavaScript commands may have been used to conceal real URL of the fake website in the address bar. Therefore, the link in a phishing email may appear to be that of a legitimate company's name, but will actually take the user to a fake website or pop up.

Another common trick used by phishers is to misspell or disguise URL's. Many phishers mask URL's to their fake websites by using addresses that, at first glance, appear to be that of a well known company. On closer inspection it's clear that they have actually been altered slightly by the addition, omission or transposing of letters. For example, [www.branchommunications](http://www.branchommunications) could easily be mistaken for the correct URL of [www.branchcommunications.co.uk](http://www.branchcommunications.co.uk) at a glance. Another disguise uses web addresses containing the @ symbol. For example, [www.branch@communications.com](http://www.branch@communications.com) could easily deceive the recipient of a phishing email into believing that the link will take them to the legitimate website of Branch Communications.

## **Branch Communications Ltd**

A further flaw which may lead to phishing lies with internationalised domain names. This could allow the use of visually identical web addresses to lead to fake websites, due to the fact that different characters in different coding languages can look the same, depending on the font used. So, although a computer may display visually identical or very similar characters to the user, these differences are still significant to the computer when locating web sites or validating certificates.

Customers should be advised to always check the real IP address of a website, which will always be displayed in the bottom corner of the email/website. Just as importantly, they should always access a company's website by entering the URL they are familiar with directly into the address bar of their browser.

### **BATTLE AGAINST PHISHING**

To combat the rise in phishing, various educational, legislative and technical techniques are now available to protect both businesses and consumers. Thankfully, the Anti-Phishing Working Group, an industry and law enforcement association, believes that conventional social engineering techniques could become obsolete in due course as email users become increasingly familiar with the techniques used by phishers (in the same way that they have become confident in spotting and dealing with spam). Unfortunately, they suggest that technical subterfuge will become more common – a tool which is not so easy to spot. In the meantime, whilst there is no complete remedy to phishing, the following measures can minimise the number of phishing emails and consequent risk.

### **CORPORATE RESPONSIBILITY**

Having played a major role in educating consumers to spot and deal with spam, reputable businesses now need to educate their customers to spot and deal with phishing attacks.

Firstly, a company should establish a policy for email content and communicate that to customers. The objective is for customers to confidently recognise legitimate emails from the company. As part of that policy, customers should be reassured regularly and at every opportunity via email, the email content policy and websites that they will

## **Branch Communications Ltd**

never be asked to provide sensitive information by email. Hyperlinks and forms should never be included in emails as a matter of course.

Organizations should also introduce much stronger authentication processes for on-line transactions. "Challenge questions", for example, ask the user for information that should only be known to the user and the company with whom they are transacting. Some websites have also added two way verification and two way authentication tools. This may allow, for example, users to see a secret image that the user selected in advance; if the image does not appear, then the site is not legitimate. At the very least, companies should include personal authentication information into every email it sends, so the customers can validate the email. Digital signatures, email sequence numbering and visual and audio personalisation of emails should also be considered.

Customers should be educated to spot a phishing email, and to never click on links in any email. The golden rule for any internet user, in order to avoid being phished, is to access the legitimate company's website by typing the URL directly into the address bar of their browser.

If a customer does receive an email asking for personal data, then they should be asked to inform the legitimate company straight away – a reputable company would always be glad to hear of potential security threats so immediate action can be taken to protect themselves and their customers. Above all, if a customer has any doubt at all about the authenticity of an email, then they should trust their instincts and ignore it. If they think there is the remotest possibility of the email being legitimate, then once again they should contact the legitimate company directly or visit its website by typing the URL into the address bar and login as usual. This will provide the customer with accurate information about their account and allow them to avoid the possibility of landing on a spoof Web site and giving their information to someone they shouldn't.

Any business concerned about a phishing scam should send details to the Anti-Phishing Working Group, who is building a database of common scams to help inform people of the risks.

# **Branch Communications Ltd**

## **PREVENTATIVE TECHNICAL MEASURES**

As phishing websites are often launched before the email attack takes place, companies should monitor and analyse the internet for potential phishing attacks. Those susceptible to phishing scams can use commercial monitoring and analyzing services, offered by companies that will also take legal action against phishing websites on their behalf.

Every company should introduce high standards of anti spam, anti virus and content filtering software at the internet gateway, as an added layer of protection.

Customers should be advised to protect themselves with anti spam and anti virus filters, which will reduce the number of phishing-related emails that get into their inbox. Several anti-phishing firewalls and software programs can now be recommended for personal use, which customers can integrate with their email software and web browsers. These identify the real domain names of companies from whom they have had communication.

Customers can also use commercial software to spot and remove any spyware or malicious programmes on their PC, and use privacy protection software to warn them when they are about to submit personal data to questionable sources. Software is also available that will identify the real website that will receive personal data a person is about to submit.

## **WHAT BRANCH COMMUNICATIONS CAN DO FOR YOU**

Phishing presents an ever increasing risk to businesses and their customers as technology improves and as we place greater reliance on the internet than ever before. The financial loss to businesses can be considerable, not just through fraudulent transactions but also through loss of revenue as customers lose faith in the company and on-line security.

Whilst no simple solution to phishing exists, the risks can be managed and minimised with the right knowledge, procedures and communication programmes in place.

## **Branch Communications Ltd**

Branch Communications can help you understand phishing and establish an appropriate email policy for your business. Together, we can implement that policy as you build closer relationships with your customers through regular digital communication. We can also devise a programme of education to make sure your customers are not caught unawares by phishing.

Contact the Branch marketing team on 0870 443 5778 for more information and support or visit our website [www.branchcommunications.co.uk](http://www.branchcommunications.co.uk).