

Mail-SeCure Anti Phishing White Paper

December, 2006

Powered by



PineApp Mail-SeCure – Complete Anti-Phishing Solution

Introduction

The recent years have brought high-speed broadband and wireless interconnectivity to a growing number of users and corporations. This trend gave users an easy and un-interrupted access to information exchange, to the development of electronic commerce and online banking.

Phishing (also known as carding and spoofing) is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information (such as passwords and credit card details), by masquerading as a trustworthy person or business in an apparently official electronic communication (such as an email or instant message).

With many banks and businesses offering their customers access to their accounts over the web, email fraud has infiltrated into the Internet, using e-mail and fake web sites to pull off the scam.

Phishing has recently become very common; with many users drawn to almost any kind of on-line fraud, including “The Nigerian Fraud” letters, stock “Pump-and-Dump” spam and actually more or less any spam.

The Phisher can either randomly select a recipient or directly target a domain. The recipients receives a message pretending to be from an organization which the recipient has a relationship with (it could be a bank or an online commerce such as e-bay or an ISP), asking for "account confirmation", or directly requesting the recipient to reveal sensitive personal information, such as a password or credit card number.

Did You Know...
*The term **Phishing** is a combination of the words "fishing" and "phreaking" (studying and experimenting with equipment of public networks). Phishing alludes to the use of increasingly sophisticated lures to "fish" for financial information and passwords from the **sea** of Internet users. The term was coined in 1996 by hackers, who were stealing from AOL Internet accounts by scamming passwords from unsuspecting AOL users.*

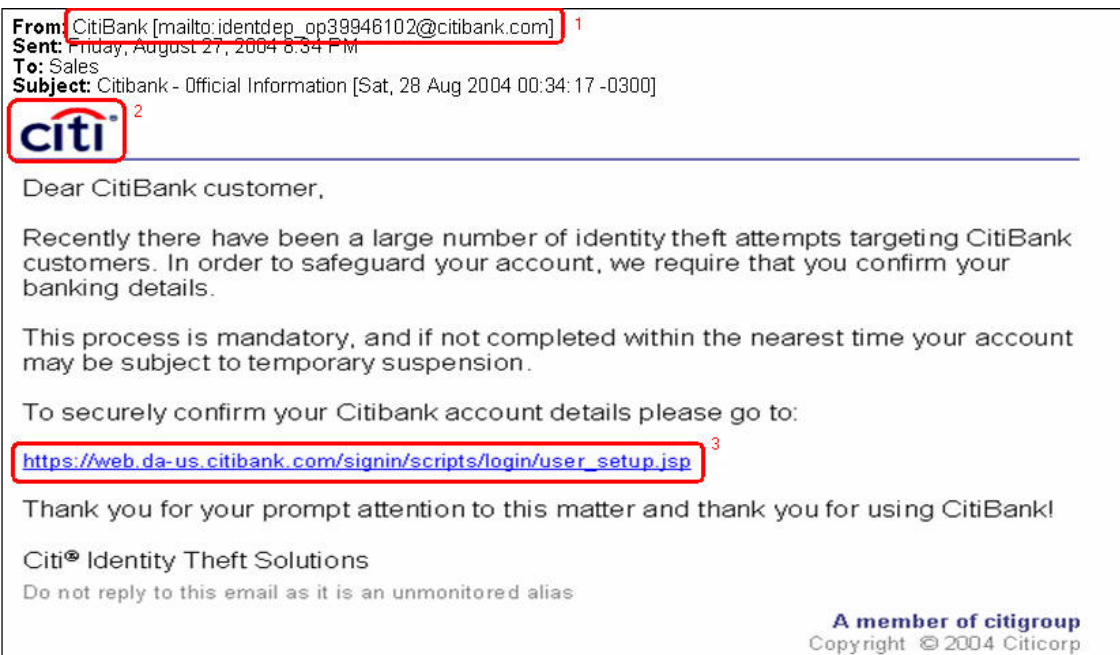
How to spot a Phishing scam



At first glance, it may not be obvious to the recipients that the message in their inbox is not a legitimate one from a company with whom they do business. The "From" field of the e-mail may have the .com address of the company mentioned in the e-mail, and the clickable link may also appear to be taking you to the company's Web site, but will in fact take you to a spoofed Web site.

Looks can be deceiving, as with Phishing scams the e-mail is never from who it appears to be!

Here is an example:



Phishing e-mails will contain some of these common elements: (view screen capture above from Eudora)

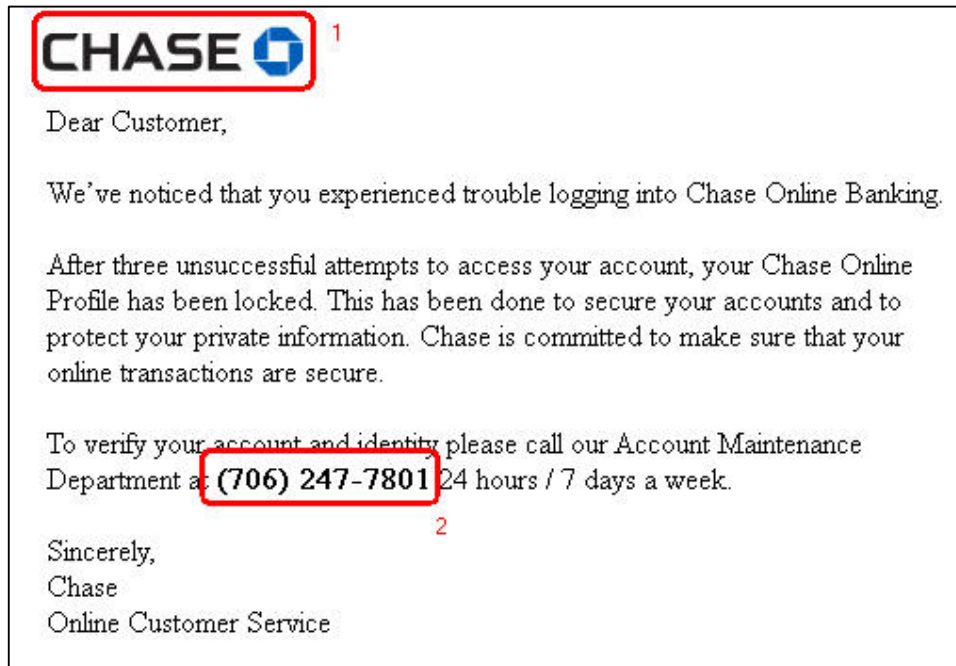
1. The "From Field" appears to be from the legitimate company mentioned in the e-mail. It is important to note, however, that it is very simple to change the "from" information for any e-mail client.
2. The e-mail will usually contain logos or images that have been taken from the Web site of the company mentioned in the scam e-mail.
3. The e-mail will contain a link or hyperlink to a website with a similar URL name as the "real" sender. *Note that the hyperlink does NOT point to the legitimate Citibank Web site URL.*

Vhishing (Voice-Phishing):

Vhishing (Also called "VoIP Phishing"), is a new type of Phishing scam. The term Vhishing is a combination of the words "voice" and "Phishing", and is the voice counterpart to Phishing.

In this scam, instead of being directed by e-mail to a Web site, the recipient is asked to call an 800 number to an organization which he has a relationship with, requesting him to verify his account and identity. Because people are used to entering credit card numbers over the phone, this technique can be effective; the fraudsters hope to fool people who know better than to click a link in an unsolicited email that asks for personal information. For these people, making the call might seem like the safe thing to do. What they don't realize is that their call is to be answered by a crook. When the user calls the number, a message is played stating "This is account verification. Please enter your 16 digit account number". Only the number isn't to a bank or credit card company, it's to a VoIP phone that can recognize telephone keystrokes.

Here is an example:

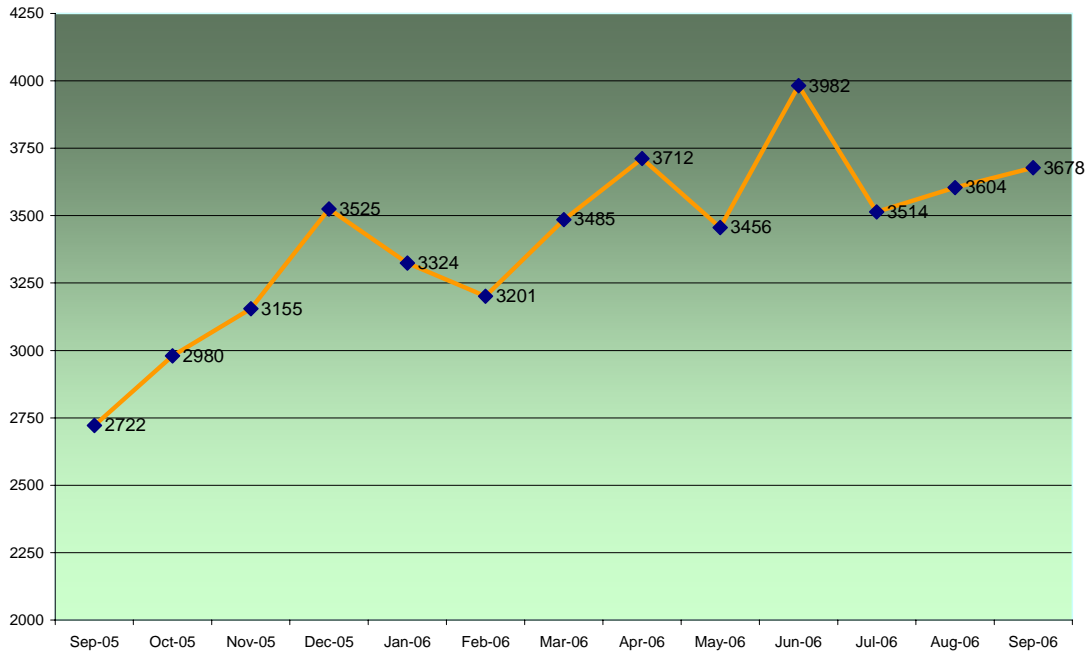


1. The e-mail will usually contain logos or images that have been taken from the original company's Web-site.
2. The phone number does NOT belong to the company mentioned (in this case: Chase) .The number, in most cases, will lead you to an automated voice box in which you will be required to dial in your account information.

Phishing Growth

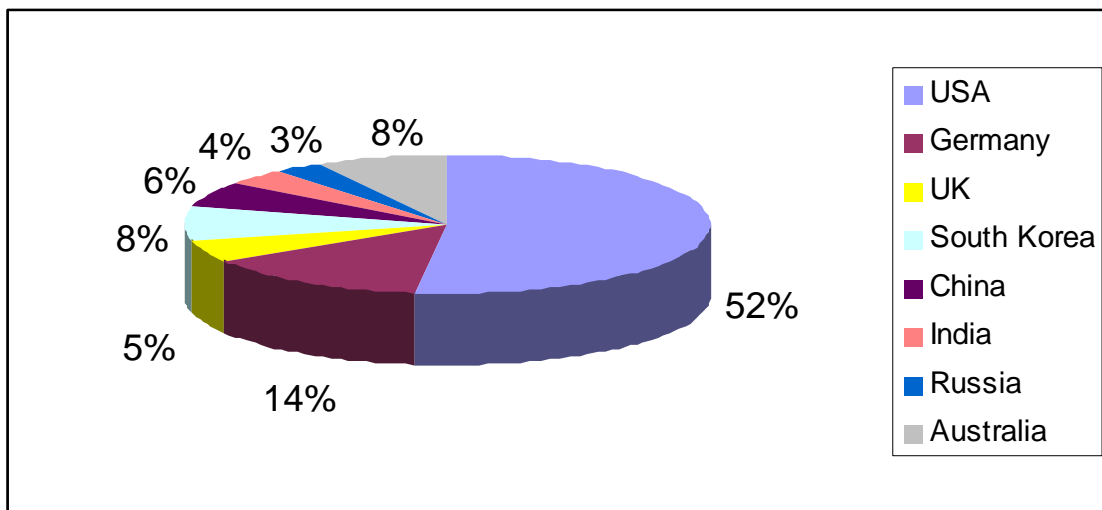
Phishing is growing rapidly; In the past 12 months only, the number of untargeted attacks has grown by 41%, whilst the number of targeted attacks against distinct brands has grown by 135% (according to RSA).

In September 2006, PineApp’s Phishing Tracking Center™ received reports of approximately 22,560 unique Phishing scams.



Phishing Attacks per month – worldwide

(According to data received from PineApp’s Phishing Tracking Center™)



Top Hosting Countries

(According to data received from PineApp’s Phishing Tracking Center™)

Anti-Phishing

Mail-SeCure's Anti-Phishing module combines several layers and technologies to detect and block Phishing attempts. The main technologies used are:

- **Anti-Phishing Database** - Mail-Secure maintains a data base which is updates on a daily basis. This database features millions of known Phishing URLs and domain names. If one of the listed URLs appears in a mail, it is blocked.
- **SURBL** - an RBL which is designed to block or tag Phishing attempts based on URI's (usually their domain names) scattered in the body of the message. In this case, the RBL is not intended to block the source of the spam message. Instead, SURBL is used to block spam based on its message content.

Even if a spammer uses new domains, they may point to the old, blocked IPs and will therefore be blocked, right from the first spam message received.

- **CommTouch RPD™** - CommTouch's Recurrent Pattern Detection (RPD™) is based on the fundamental characteristic of Phishing, spam and email-born Malware - its mass distribution over the Internet. Sniffers located worldwide, lookout for real traffic in over 60 million operational mailboxes. They then extract patterns to detect recurring patterns and examine the number of sources to determine if they are Trojan-based outbreaks. CommTouch RPD™ differentiates between bulk mail (which can be a mailing list), and confirmed spam.

CommTouch RPD™ advantages:

- Generates patterns from more than 300 million daily messages, from over 15 locations worldwide.
 - Real-time – blocks spam from the first minute of the outbreak.
 - Near-zero false positives – as the pattern of legitimate mail sent from one to another will probably appear only once.
 - Content-agnostic – effective against Phishing, fraud and innocent-looking spam.
 - Language independent.
 - Detects spam of any file type.
 - Adaptive technology – As spam is economically motivated, spammers constantly change tactics to achieve mass distribution.
- **Heuristic Fraud detection sets of rules** - Mail-Secure uses Heuristic rules in order to detect possible new Phishing attempts. Mail-SeCure has over 2,500 sets of rules to detect characteristics of Phishing. The heuristic engine uses a score-based system to identify Phishing.
 - **Zombie detection** - Most Phishers use zombie computers to distribute their mail. Zombie computers are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and used for mail distribution.

Mail-SeCure has a unique Zombie Detection System – ZDS. It identifies zombies and automatically blocks them at the session level (similar to RBL). PineApp has a central ZDS, RBL-like server, which dynamically blocks identified IPs. Since a zombie computer owner can change his IP, ZDS automatically adds or removes IP addresses from blacklists.

- **IP Reputation** - a powerful additional layer used to block Zombies at the SMTP session level. IP Reputation saves bandwidth and lowers the load on your Mail-SeCure system.

The IP Reputation mechanism is based on sniffers located at various points of the world, monitoring traffic of hundreds of millions of email messages daily. IP Reputation center dynamically classifies IPs, according to a profile built from parameters such as: volume, percentage of spam & viruses and elevations. When an SMTP session is established, Mail-SeCure queries the IP Reputation system (or uses local cache) and performs various actions according to the IP classification, such as: permanently reject the mail, respond with a temporary error to be able to re-evaluate the IP on the retry time, activate grey-listing, activate Rate limit, etc.

- **Rate limit** - provides an advanced layer against mail bombing, by limiting the amount of messages or SMTP sessions allowed from a certain IP on a pre-defined time. Rate limit uses a complex algorithm using a sliding-window method. Limitations can be defined for timeframes of: minutes, hours and days.

Conclusion

Mail-SeCure is not just another Anti-Spam product but one of the most robust Anti-Phishing solution in the market, which is able to detect and block all known Phishing attacks and protect organizations' sensitive information.