Mail-SeCure™ - Anti Phishing Whitepaper

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 online fraud, including "The Nigerian Fraud" letters, stock "Pump-and-Dump" spam and actually more or less any spam type.
The Phisher can either randomly select a recipient or directly target a domain.
The recipients receives a message pretending to be from an organization with which the recipient has any kind of business engagement (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.

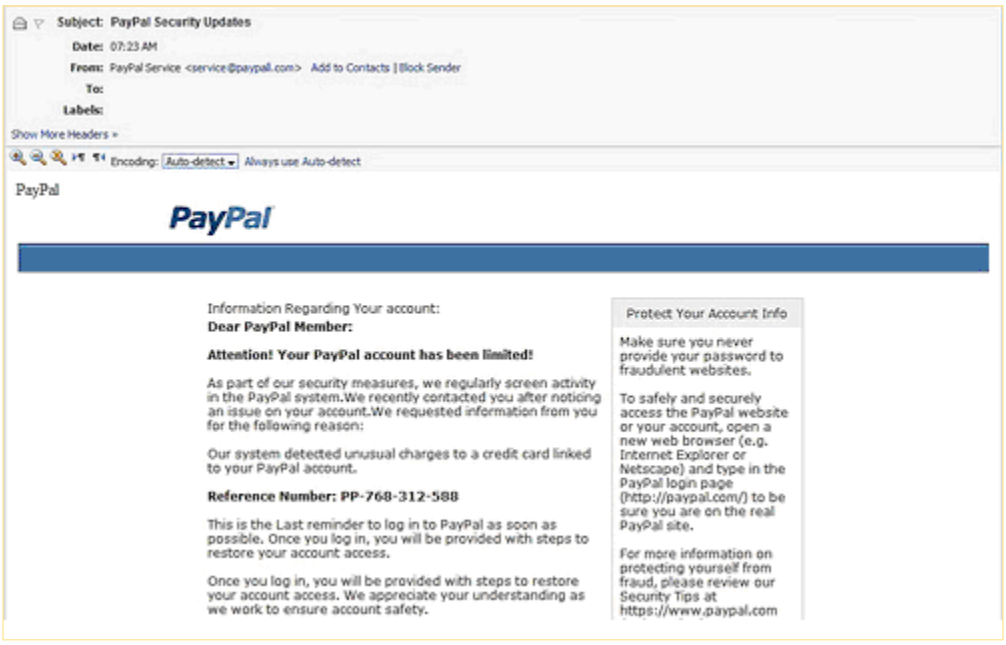
Did You Know...

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 website, but will in fact redirect you to a spoofed website.
Looks can be deceiving, as with Phishing scams e-mail is never from who it appears to be!

Here is an example:

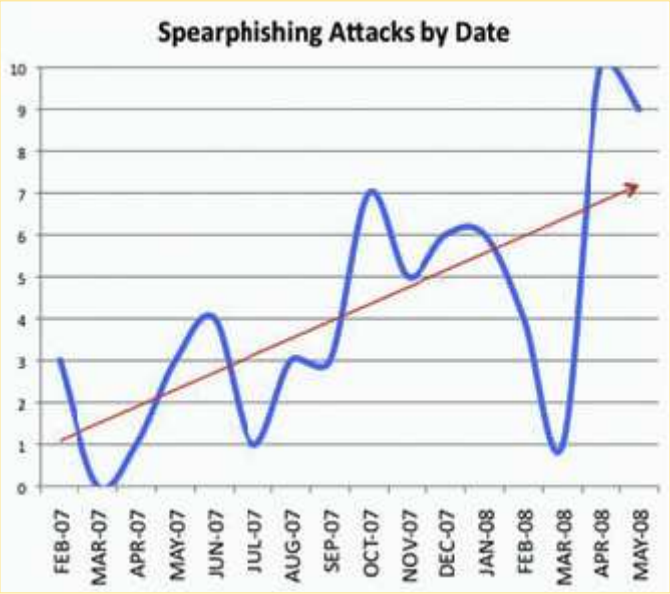


Phishing e-mails will contain some of the following common elements:

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 in any e-mail client.
2. The e-mail will usually contain logos or images that have been taken from the website 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.

Phishing Growth

Phishing is a serious threat for both consumers and businesses. In the last decade, ever since phishing arrived on the scene, this fraud method has been growing rapidly, with one estimation citing approximately 8 million daily phishing attempts worldwide[1].

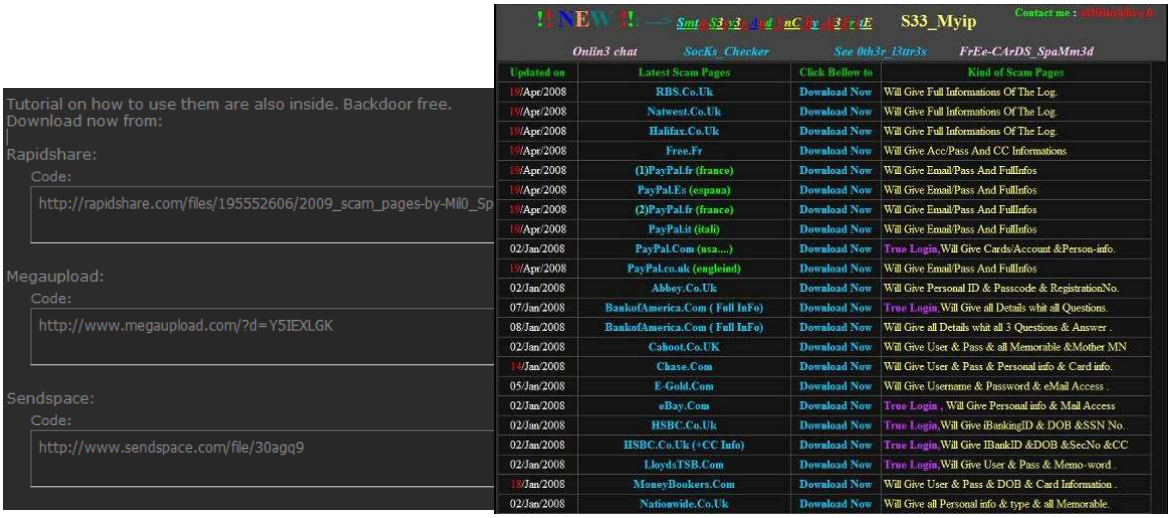


"Counterfeiting & Spear Phishing — Growth Scams of 2009," Trade Me, Infonews.co.nz, March 2, 2009

Phishing is easy!

Phishing user guide and tools can be found over the internet , you are just a click away from a home made scam.

Websites with toolkits to download



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 (Reatlime Blackhole List) which is designed to block or tag Phishing attempts based on URI's (usually their domain names) scattered in the message's body. 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 IP's 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 messages daily, from over 15 locations worldwide.
- ✓ Real-time – blocks spam from the first minute of the outbreak.
- ✓ Near-zero false positives – as the pattern of a legitimate email, sent from one to another, will probably appear only once.
- ✓ Content-agnostic – effective against Phishing, fraud and innocent-looking spam.
- ✓ Language independent.
- ✓ Detects embedded Spam in 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 e-mails. Zombie computers are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and are being 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 IP's. 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.