



Chaser: A Year of JPMorgan Chase Phish
infectionvectors.com
March 2007

Overview

With the practice of phishing now at least ten years old¹, the crime has received attention from all types of media – from newsletters targeting the Internet security community to articles designed for average bank customers. This report aims at both groups, exploring the technical mechanisms used by email criminals and the non-technical affects of phishing attacks. Phishing itself may not be understood to be an “attack” by the casual observer. However, the practice is best described as phishing attacks for two reasons: the onslaught of fraudulent messages is certainly a mass-theft attempt, and second, it is a targeted assault on the brand and/or trademarks of the company being impersonated. This paper uses a full year of phishing attacks (received by a single mailbox) against JP Morgan Chase (referred to as just “Chase”) as its context. The number attacks for the year totaled 71 pieces of email. Infectionvectors.com selected Chase in March of 2006, after receiving a number of fraudulent emails referencing their products and institutions.² Since that time, until March of 2007, the incoming phishing attempts were saved, analyzed, and finally, collected into this report.

The Scam

In late December 2003 security professionals warned users of a new criminal scheme that took aim at Visa card holders.³ In 2003, it was still necessary to explain how the scam actually worked, going into details about the “decoy web sites” and “phony email messages.” Email security company Tumbleweed estimated that 5% of those targeted with this iteration of the scam responded, a population of approximately three million people. Everyday of the three years that followed, Chase Visa (JPMorgan Chase & Co.)⁴ found itself the target of “brand hijacking.” Sadly, the 71 email-based attempts to defraud Chase customers documented in this report are just a fraction of the phishing scams directed at consumers from March 2006 through March 2007.

Although also the subject of numerous marketing papers, brand hijacking has been adopted by phishing researchers as the criminal act of taking the trade name and/or logo of an established business and utilizing it for illicit ends. In the case of phishing, that quite simply means taking a company trademark (in the form of actual web graphics) and presenting a message to a target as though the message is an official communication of the company. The brand is also used to give legitimacy to the complementary web sites used by phishers. As a consequence, the actual brand and brand holder are damaged. JPMorgan Chase & Co. knows this very well, they have a number of resources available to their customers – from education sites to monitoring and investigation resources.⁵

When There's Money Involved

The first scam received during the monitoring period is now all too familiar to phishing researchers: the “receive \$20 for taking our survey” scheme copied by many criminals in the last year. As is seen in the graphic below, the phisher is very reassuring to the target that information collected is “non-sensitive and anonymous” and would certainly not be passed to a third party. Of course, in order to receive the reward for their time, the subject must provide their account data.

Dear Chase Bank Customer,

CONGRATULATIONS!

You have been chosen by the Chase Manhattan Bank online department to take part in our quick and easy 5 question survey. In return we will credit \$20 to your account - Just for your time! Helping us better understand how our customers feel benefits everyone.

With the information collected we can decide to direct a number of changes to improve and expand our online service.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

SERVICE: **Chase Online® \$20 Reward Survey**
EXPIRATION: **March - 16 - 2006**

[Confirm Now](#) your **\$20 Reward Survey** with **Chase Online® Reward** services.

The information you provide us is all non-sensitive and anonymous. No part of it is handed down to any third party groups. It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey.

Please do not reply to this message. For any inquiries, contact Customer Service.

Document Reference: (87051203)

Copyright 1996 - 2006 Chase Bank, N.A. Member FDIC Copyright © 2006

For the most part, the spelling and grammar in the “Chase” scams are both good – much improved over the average phishing attempt from years back. Consider this example, a minor variation on the one above, from one of the collected schemes:

Dear Valued Customer,

CONGRATULATIONS !!!

You have been chosen by the Chase Manhattan Bank online department to take part in our quick and easy 5 question survey. In return we will credit \$100 to your account - Just for your time! Every question answered will add \$20 to your account.

Helping us better understand how our customers feel benefits everyone. With the information collected we can decide to direct a number of changes to improve and expand our online service.

The information you provide us is all non-sensitive and anonymous - No part of it is handed down to any third party groups.

It will be stored in our secure database for maximum of 3 days while we process the results of this nationwide survey.

We kindly ask you to spare two minutes of your time in taking part with this unique offer!

To Continue click on the link below:

Many Thanks and Kind Regards - Chase Manhattan Bank Customer Department

Using financial rewards (specifically, “earn \$20 or \$100”) was a component of 14 of the 71 attacks. This “carrot” approach was opposed by the “stick” of limiting credit account access, among other inconveniences (as well over half of the messages involved fear, it is easy to see what the phishers have found to be successful). The “motivation” provided to the reader as a reason to click the link in the email was categorized as an Update (broken down into both Software updates and Information updates), the need to logon to the Chase servers to retrieve a personal message, the promise of a financial reward (for answering survey questions), or via fear (almost always as “your account has been targeted by numerous computers/attackers”). The motivations used are decidedly slanted in favor of fear:

Motivation	# Received	Percent
Update Information	11	15.15%
Update Software	3	4.55%
Message	2	3.03%
Financial Incentive	14	18.18%
Fear/Warning	41	59.09%
TOTAL	71	100.00%

As the tags are used numerous times, it is relevant to provide examples of each category. These are not scientific organizations, and there is room to argue placement of some messages, but it does provide us with a loose sorting capability with which to begin the dialogue. The majority of the “fear” tactics appeared as:

Your online credit card account has high-risk activity status. We are contacting you to remind that on March 27 2006 our Account Review Team identified some unusual activity in your account. In accordance with Chase Bank User Agreement and to ensure that your account has not been compromised, access your account was limited. Your account access will remain limited until this issue has been resolved.

There were very plain notices, indicating only that a message awaited the recipient at the official message center.

Dear Chase Online SM Customer:

A message regarding "Re: Credit Card - Update Profile User" has been sent to our Secure Message Center. To see your message:

Log on to Chase Online.

There were requests for software updates:

Technical services of the Chase Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation on customers data.

Requests for simply validating information that is on-file:

This email was sent by the Chase Bank server to verify your account . You must complete this process by clicking on the link below and entering your account information .

This is done for your protection , because some of our members no longer have access to their online access and we must verify it.

The table above, when expanded to show a monthly breakdown, gives a better

Motivation	Mar-06	Apr-06	May-06	Jul-06	Aug-06	Sep-06	Jan-07	Mar-07	TOTAL
Update Information	6	2	0	1	0	1	1	0	11
Update Software	1	0	0	0	2	0	0	0	3
Message	2	0	0	0	0	0	0	0	2
Financial Incentive	5	5	0	1	0	1	1	1	14
Fear/Warning	20	12	1	1	3	3	1	0	41
TOTAL	34	19	1	3	5	5	3	1	71

World Wide Verified

Where are the servers that host Chase-related phishing activities? More accurately, where were the servers, as most are taken down by Internet watchdog groups within days of publication. Location of the host that sent the message was not investigated as in most cases these are compromised machines and/or temporary spam servers. The following table summarizes what was found for the 71 messages:

Country	# Hosted	Percent
United States	21	29.58%
Korea	6	8.45%
UNK	5	7.04%
Germany	5	7.04%

China	4	5.63%
Japan	4	5.63%
Canada	3	4.23%
Slovakia	3	4.23%
Austria	2	2.82%
Brazil	2	2.82%
France	2	2.82%
India	2	2.82%
Luxembourg	2	2.82%
United Kingdom	2	2.82%
Argentina	1	1.41%
Australia	1	1.41%
Malaysia	1	1.41%
Poland	1	1.41%
Spain	1	1.41%
Taiwan	1	1.41%
Thailand	1	1.41%
Ukraine	1	1.41%
TOTAL	71	100.00%

These numbers are consistent with what has been offered from Phishtank (<http://www.phishtank.com>):

United States 24%
South Korea 14%
India 8%
China 6%
Japan 3%
Great Britain 4%
Germany 4%
Brazil 4%
Columbia 3%
Costa Rica 3%
Russia 3%

Table statistics from Phishtank.⁶

The scope of the problem is only partially revealed by examining the country of origin statistics. At its heart, Internet-based fraud is difficult to stop with traditional law enforcement practices because it exists in a different world altogether; a different dimension, in fact. Using statistics such as these helps to illuminate how resource intensive finding and prosecuting phishers is for a commercial organization, but it does not fully identify the challenge faced by corporations such as Chase.

Any Other Name

Branding, building a product and company reputation in the hearts and minds of consumers, is of vital concern to every organization. It is the association customers have

with one brand of goods and services over another that dictates purchasing habits over the long-term. Dennis Hahn, executive vice president of ID Branding, noted that,

"Most companies have recognized for some time that branding is of paramount importance to the success of their business. Building a strong brand, it is believed, will make it easier for over-stimulated consumers to make buying decisions. More importantly, it will increase the likelihood that one company's product or service will be chosen over another's." 7

Numerous pieces complete the brand puzzle: a logo, advertising, press coverage, and most importantly, customer interaction with the respective company and products. This interaction takes place whether or not the individual is actually buying or using the product in question – public relations are constantly being formed.

Given the importance of a brand, and every component that goes into it, it is no wonder that the repeated fraudulent use of such brands is the heart of the millions of phishing attacks that cross the globe. In an April 2004 Bank Technology News article, Karen Krebsbach, quoting (David Jevans from APWG) posits:

"Brand is everything," observes Jevans, who estimates phishing costs financial institutions about \$100,000 to \$150,000 per attack. "There's a lot of brand risk. Fraud is easier to sweep under the rug. It's very different when one million people are getting e-mails from you. Are they likely to continue to do business with you? What's a bank's whole thing? Security. Safety. Trust. Anything that undermines those issues can't be good." 8

The article goes on to mention the variable fronts that are under siege when a phishing scheme is launched. Beyond the email-based help desks, customers are likely to flood call centers when they receive a suspicious message. This is in addition to the inevitable fraud that takes place after an unsuspecting consumer answers the fake requests. The damage to the intangible brand of a bank may not be realized for years to come, but it is sure to be steep.

Many banks, including JP Morgan Chase, have already had to pay a great deal for fraudulent charges and withdrawals as a result of phishing. This has been accepted as a service that is required to keep customers protected. The erosion of their brands and customer trust will be a steeper price to pay.

Reaction

While far from impossible, catching phishing suspects is a resource intensive effort. As hinted to above, simply culling through email, server, and payment tracking details can take even skilled researcher a great deal of time, and may possibly lead nowhere. However, over the last few years, there have been a number of notable arrests.⁹ As arrests increase and returns decrease (meaning that recipients become aware of the phishing

threat and guard personal data more closely), it is possible that phishing itself will diminish.

However, given the apparent fortune to be made in email fraud, complete eradication of phishing seems unlikely. It would seem more likely that creative means to make phishing less lucrative, beyond traditional law enforcement tactics, will become increasingly prevalent. When the Sasser worm claimed countless PCs in 2004, an enterprising malware coder wrote Dabber, a worm that exploited a bug in the Sasser FTP server.¹⁰ The result was to give the Dabber author control over many of the resources that the Sasser coder worked to seize. The same type of attack is certainly conceivable with phishing, where a criminal needs to establish a remote web server to collect customer data.

Finding the criminals may be difficult, but finding their “fronts” is simple: the web servers are open to the public as a necessary component of the crime. Phishing sites are notoriously temporary; they appear and then disappear quickly as needed. Nonetheless, it is possible to catch many of the sites with little difficulty, especially for the skilled and quick-acting anti-phishing vendors/organizations today. In fact, it may be that due to the need to build and destroy sites so quickly, the designer is less inclined to be concerned about securing the site. Once found, reaction to the discovery could be in the form of SQL injection or cross-site scripting (XSS) attacks.

The attack upon a phisher would effectively reduce the reward of the fraud (presumably, the more people sharing the stolen data would thin out each share and may alert the rightful owner of the data before the original thief was to exploit it). If phishing efforts were less profitable for the person taking the risk of being caught it is reasonable to assume there would be fewer people involved in the activity. This is in no way an endorsement of offensive tactics to deal with the threat of phishing, law enforcement bodies are best left to combating crime. However, criminals may engage in such activities with increasing regularity in the future. In fact, such efforts may also mean that compromised data will be much more difficult to contain, as it will spread among more criminals with even greater speed.

Attacks against Internet assets have been considered as a means of fighting cyber crime in the past. In 2005, the United States considered the, "Peer-to-Peer Piracy Prevention" act, which would have authorized offensive action against machines suspected to be housing pirated software, music, etc.¹¹ It was theorized that film and music producers may have need for such attacks in order to fight piracy. This would not be a likely choice for financial institutions such as Chase. Invariably, such attacks are used against innocent people and for ends that are far from noble. Just as in the case of “beneficial malware,” benevolent intentions are not enough to justify consequences of legalizing and/or endorsing the use of criminal acts for “good” ends. SQL injection attacks against poorly guarded databases could certainly divulge the stolen data to any number of people: from other criminals looking to exploit passwords, credit card numbers, etc. to vigilantes hoping to alert victims before stolen data is used. Many phishing sites are loaded onto compromised web servers, meaning attacks that reveal phishing databases may open the

records of legitimate businesses as well. Stored XSS attacks against data collection pages could be used to warn phishing victims that “unauthorized” collectors run the site. Allowing such practices, however, would likely develop into reflected XSS attacks that end up stealing even more data from victims.

Education is the best method to combat phishing attacks, something that Chase appears to take seriously. This takes the form of both awareness training for customers as well as moderate technical countermeasures, such as periodically changing image links (replacing logos with “Expired” tags to prevent phisher recycling) and requiring tokens for authentication.

The Chase

Chase, as mentioned, has established awareness pages on the web and extols customers never to provide account information based on email requests. In addition, during the research for this report, it was noted that the company kept up with new phishing efforts on its “examples” page.¹² Protecting its customers is clearly good business, as they are responsible for the majority of fraudulent charges to stolen accounts. In addition, JP Morgan Chase became part of an anti-phishing consortium in 2004; this group aims at both the technical requirements to stop phishing and legal ramifications of going after phishers.¹³

The continued increase in online banking and commerce may be seen as evidence that the financial organizations are winning the battle against phishing. However, if the cost of reimbursing consumers and vendors does not swamp these gains, they certainly erode the profits of each bank that finds itself in the way of these scams. These are attacks very different from the traditional bank robber. Thieves from all corners of the globe, leveraging the trust and brand loyalty that the bank itself has built, have replaced the masked gunman with a sack who actually had to show up at a bank.

Although it is clearly not a simple technological problem, phishing is often addressed as a crime requiring technical solutions. From site detecting to dismantling, many security advisors, even those advocating brand protection as their primary goal, focus on factors such as detection speed, forensic data collection, and ways to stay ahead of criminals using logos directly off of the legitimate web site. Although technical tricks are helpful when controlling the impact of phishing, they do not offer a long-term solution to such confidence crimes. Technical solutions help researchers, law enforcement, and security professionals. To combat fraud effectively, the target/victim of such activities should be attended to as well. JP Morgan Chase’s attention to educating consumers, which includes posting fresh examples of fraudulent emails, presenting simple instructions to those faced with requests for personal data (“...never respond or reply to e-mail that...”) ¹⁴, and response efforts ¹⁵ offers tangible support to customers while still supporting technical needs of researchers.

Notes

1. Although not referred to as “phishing,” this 1996 article from a Jacksonville, Florida newspaper is the earliest description of email being used to lift credit card numbers found during the research for this report . The original source is not available at the publisher’s website, however, two sources are noted below for those seeking the initial article:

“The Internet is a Source of Wonder, as Well as Fraud”

By John Dunbar, The Florida Times-Union, Jacksonville, July 7, 1996.

<http://www.textfiles.com/digest/TELECOMDIGEST/vol16.iss0301-0350.txt> & in the following newsgroup:

<http://groups.google.com/group/comp.dcom.telecom/msg/cccb7dafef17177f?dmode=sour ce&hl=en>

2. The idea to follow one “brand” of phish was based on a perceived flurry of attacks during March and the notion that the number would diminish over the course of a year – as customers became educated to the scam, either because they fell victim to it or because of awareness efforts. Chase itself was selected due to its size and notoriety in addition to it being one of the companies for which we had ready examples in March 2006 (i.e., there was no scientific, economic, or political reason for its selection, nor should one be inferred). Note that the examples used for this report are only those that came into the selected mailbox; although there are number of other good examples of Chase-based phishing attempts, only those received by infectionvectors.com were used.

3. “Latest ‘phishing’ scam targets Visa customers.” Paul Roberts, IDG News Service. December 26, 2003.

<http://www.computerworld.com/newsletter/0,4902,88583,00.html?nlid=SEC2>

4. <http://www.chase.com/> & <http://www.chase.com/PFSCreditCardHome.html>

5. Chase’s offerings include detailed guidance regarding phishing scams:

http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/Protect_Identity and their Identity Theft Protection Kit:

http://www.chase.com/ccpmweb/shared/document/Identity_Theft_Kit.pdf.

6. “Phishing Sites by Country of Host, October 2006”

<http://www.phishtank.com/stats/2006/10/>

Also of interest may be: “Sophos reveals “Dirty Dozen” spam producing countries” 6 November 2006.

<http://www.sophos.com/pressoffice/news/articles/2006/11/dirtydozq306.html>

7. Denna Hahn “Identity-Driven Branding: Branding from the Inside Out.” July 2006.

allaboutbranding.com. <http://www.allaboutbranding.com/index.lasso?article=428>

8. “Goin' Phishing: Growing e-mail attacks threaten banks' bottom lines.”

Karen Krebsbach Bank Technology News, April 2004.

<http://www.banktechnews.com/article.html?id=200405264EFZ0YLD>.

9. For information on a few high-profile arrests, see:

BBC News. “‘Phishing’ arrest is first for UK.” 29 April 2004.

http://news.bbc.co.uk/2/hi/uk_news/3668941.stm

Notable arrests include Brazil’s activity in 2005:

John Leyden. “Brazilian cops net ‘phishing kingpin’.” Channel Register. 21 March 2005.

http://www.channelregister.co.uk/2005/03/21/brazil_phishing_arrest/

and Bulgaria’s action in 2006:

Microsoft Corporation. “Microsoft Praises Bulgarian Authorities on Investigation and Arrest of Alleged Phishing and Organized Crime Group.” 20 January 2006.

<http://www.microsoft.com/presspass/press/2006/jan06/01-20BulgariaPhishingPR.mspx>.

10. Paul Roberts. “New worm exploits Sasser code flaw.” Computerworld 14 May 2004.

<http://www.computerworld.com/securitytopics/security/virus/story/0,10801,93154,00.html>.

11. Read the proposed change to Title 17 of the US Code (HR 5211) from July of 2005 at: <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.5211>.

12. The examples of phishing page at Chase.com:

http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/example_messages

13. In October of 2004, a number of financial institutions announced the creation of a group that would define requirements to combat phishing efforts:

Steven Marlin, Information Week. “Banks Join Group to Battle Phishing.” 4 October 2004. <http://www.informationweek.com/showArticle.jhtml?articleID=49400524>.

14. The steps are found at Chase’s “How to Protect Yourself” site:

http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/Protect_Yourself, and the “Phishing” site:

http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/Phishing.

15. The “ID Theft Kit” is available at:

http://www.chase.com/ccpmweb/shared/document/Identity_Theft_Kit.pdf.

Additional References

Dan Kaplan, "Security firm warns of 'toll-free' Chase phishing scam." SC Magazine, 12 April 2006.

<http://www.scmagazine.com/us/news/article/553652/security-firm-warns-toll-free-chase-phishing-scam/>

Dennis Fisher. "Phishing Is Big Business." eWeek. 7 March 2005.

<http://www.eweek.com/article2/0,1759,1772523,00.asp>.

For more information on email-based crime, please visit www.infectionvectors.com.