

# 9

## **Paypal's Phishing Dilemma**

Ben Weinbaum and Brett Mencin

In today's world of ecommerce, efficiency seems to come at a price. This price is most prevalent in the online payment and credit industries, where thousands of people in both third world countries as well as more developed nations seek out the financial information of others. While many financial companies are at risk of being hijacked by scammers, the vulnerability of Paypal is widely seen as the biggest risk of all.

### **What is Paypal?**

Paypal is an online ecommerce payment company that was acquired by eBay in 2002. With over 133 million accounts in 103 countries, it is the largest e-payment company in the world. Paypal is unique in that it allows buyers to purchase items using only their email address. Once a consumer registers on Paypal, they can fund their account by transferring money from a personal bank account. Bank information is stored on Paypal and the account can also be directly linked to a credit or debit card. Paypal's simplicity is what makes it so popular and creates an appeal for online shopping. Members do not have to enter their credit card information numerous times at merchant sites, making them able to buy something in a matter of seconds. There are over 42,000 merchant websites that currently accept Paypal as a form of payment, and the company's site's popularity is soaring as major brand names such as Apple, Dell, Walgreen's and many more, join the ranks of those who use Paypal as their form of online payment.

The majority of Paypal's business comes from eBay, where nearly every seller accepts Paypal when purchasing an item. Paypal's global reach and vast customer base makes it a prime target for fraudulent activity, especially phishing.

### **What is Phishing?**

According to the FTC, Phishing is a form of fraud in which Internet users are sent instant-messages, or more commonly emails, claiming to be from a company or organization that a user may deal with on a regular basis. Phishers attempt to fraudulently acquire sensitive information such as passwords, login names, credit card numbers, bank account numbers and other personal information. Paypal and Citibank are currently the most targeted companies in phishing attacks, especially in terms of fraudulent emails. Fraudulent emails from companies such as Paypal request the recipient to “confirm” or “validate” account information. If the recipient does not comply, the email suggests that consequences may arise. The emails then have a link to a bogus website that looks just as legitimate as the original website. The sole purpose of this is to lure email recipients into divulging personal and financial information to the operator in order to gain access to bank account and credit card information. Phishing has become increasingly more prevalent on Paypal than anywhere else on the web.

## **Advanced Techniques**

Phishers need to accomplish three objectives in order to successfully retrieve the personal information they are after. First, the target must read the email. Second, the target must click the link to the fake website embedded in the email. Third, the linked website must be a mirror image of the website they are trying to fraudulently represent.

Phishers use specific techniques to achieve their objective to gain your personal information. The most common technique used is called “link manipulation.” A link is disguised as a legitimate website by using misspelled letters in the URL or using a sub domain such as [www.paypal.com.security](http://www.paypal.com.security) instead of [www.paypal.com](http://www.paypal.com). If someone were to click on the fraudulent link, they would be directed to a forged website that appears to be legitimate. Websites can be forged by using JavaScript commands to alter the address bar. When someone clicks on the link in the email, the website they are taken to detects what browser they are using; then it suppresses the real address bar and generates a fake one to take its place. The fraudulent browser bar shows the real web address of the website being impersonated rather than the address of the scam site the user is actually visiting.

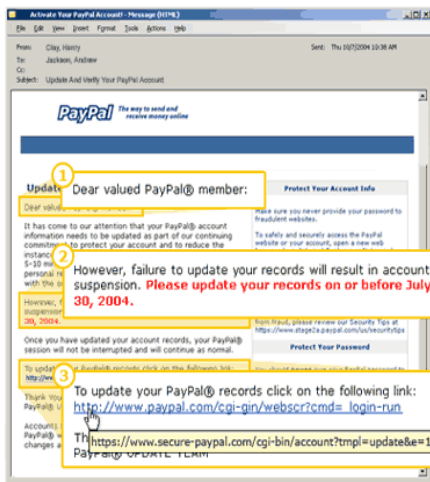
Another method that phishers use is called “URL Redirection.” Anyone who owns a website can re-direct their site to someplace else. This allows phishers to take advantage of website misspellings and re-direct users to a forged website. For example, users type in [www.paypal.com](http://www.paypal.com) hundreds of thousands of times a day. If someone were to type in [www.paypol.com](http://www.paypol.com) or [www.paupal.com](http://www.paupal.com), they could potentially be re-directed to a forged “Paypal.com” without knowing they misspelled the intended domain name and could be subjected to a phishing attack.

## **How the Paypal Email Scam Works**

The operators of this particular phishing scam involving Paypal have, without a doubt, created one of the most malicious and deceiving scams the Internet community has seen. There are many variations of the Paypal scam, but they usually involve a spoofed email address such as security@paypal.com. The branding and logo of the email look nearly exact when compared to any other email members may receive from Paypal. This is a problem in itself, because Paypal tends to send its members regular emails. The email message may vary from a simple "Please update your account" message to "Please Confirm Your Purchase" to "Notice: Buyer has filed a Claim on Your Recent Transaction." Messages such as these are very threatening because of their specificity. It is not uncommon for a high volume seller to have buyer complaints about wrong merchandise sent or failure to deliver. When a buyer files a claim, Paypal freezes the seller's funds in the amount of the transaction until an investigation is complete or the buyer and seller resolve the issue. Nonetheless, Paypal notifies both parties via email when a claim has been filed and will continue to send emails as deadlines approach for submitting evidence and feedback. Because of the need for Paypal to communicate with members through email, these fraudulent emails can potentially deceive a seller into believing a legitimate claim has been filed and consequently, the member will log in to their account from the sham link in the email.

## Recognizing the Threat

Paypal phishers are highly sophisticated in computer language programming. They are always whipping up new methods to attack the oblivious consumer who either lacks attention to detail or is unaware of warning signs that would help to identify a fraudulent email. Fortunately, it is possible to recognize the anatomy of a fake email from Paypal. Here are some of the most common elements that a Paypal user should know in determining the authenticity of the email:

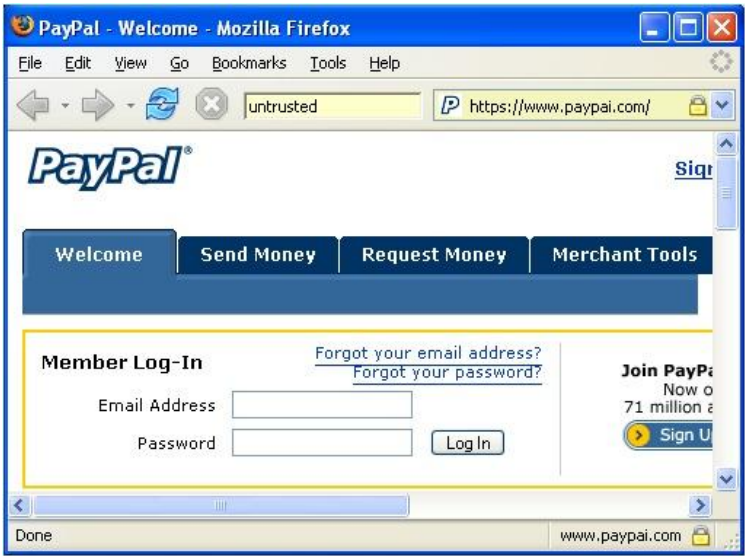


- ① **Generic greetings.**  
Many spoof emails begin with a general greeting, such as: "Dear PayPal member."
- ② **A false sense of urgency.**  
Most spoof emails try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP.
- ③ **Fake links.**  
The text in a link may attempt to look valid, then send you to a spoof address. Always check the source of a link before you click. Mouse over it and look at the URL in your browser or email status bar. If the link looks suspicious, don't click on it. Be aware that a fake link may even have the word "PayPal" in it.

- Paypal will never send an email asking for personal information

- The email has forged headers. This requires looking at the email addresses source by right clicking on it.
- The greeting begins with “Dear Paypal Member” instead of “Dear (user’s first name)”
- The email is a threat in the form that if not completed the required action there will be a suspension of account.
- The link will not direct the user to a secure page. Secure pages have a “padlock” symbol in the url bar.

Since phishing is based on impersonation, preventing it depends on users having some reliable way to identify the fraudulent sites. For example, some anti-phishing toolbars display the real domain name for the visited website. The petname extension for Firefox lets users type in their own labels for websites, so they can later recognize when they are back at the correct site. If the site is a suspect, the software may note that the website is not trusted or block the site outright.

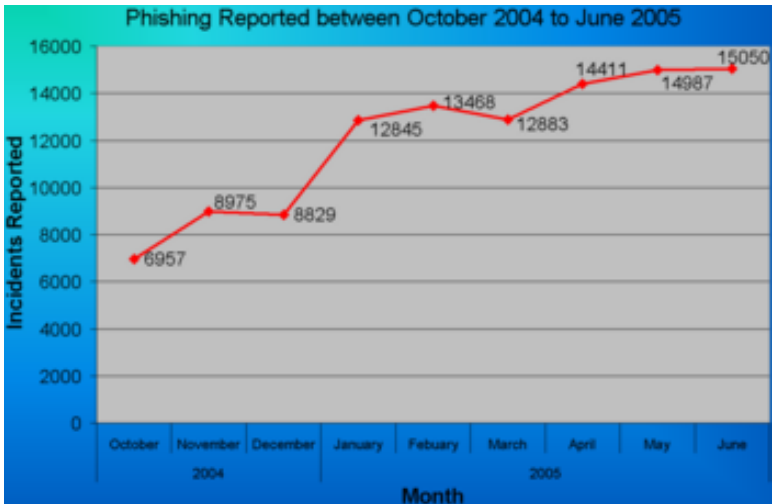


## How Victims are Targeted

It remains unclear as to how people are targeted for phishing attacks. During research with a Paypal security representative, it was determined that Paypal has no knowledge whatsoever as to how people are targeted. This leaves one to speculate that phishers have different ways of acquiring email addresses in mass quantity. The most likely scenario is the purchase of email lists from marketing firms. Companies such as Constantcontact.com allow customers to narrow their prospects by many different demographics, such as income, online spending activity, geographic location, age, and other criteria. Phishers can then purchase a list of 1000 or so email addresses that match the criteria “high online purchase rate,” under the assumption a Paypal user worth scamming would make frequent purchases.

## Damages Incurred By Phishing

Identity theft has affected over 9.3 million Americans since 2005. Damages are estimated at \$52.6 billion with 11.6% of instances occurring online. Phishing damages alone have cost consumers and businesses over 2 billion dollars since 2005.



## Financial and Legal Recourse

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher. The defendant, a Californian teen, allegedly created and used a webpage designed to look like the America Online website, so that he could steal credit card information. Other countries have followed by tracing and arresting phishers. One phishing kingpin, Valdir Paulo de Almeida, was arrested in Brazil for leading one of the largest phishing crime rings, which in two years stole between \$18 and \$37 million USD. In 2006, eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo! Japan websites, netting themselves 100 million yen (\$870 thousand USD). The arrests continued in 2006 when the FBI Operation Cardkeeper detained a gang of sixteen in the U.S. and Europe. On March 1, 2005, United States Senator Patrick Leahy introduced the *Anti-Phishing Act of 2005*. The federal anti-phishing bill proposes that criminals who create fake web sites and spam emails in order to defraud consumers could receive a fine up to \$250,000 and receive jail terms of up to five years. The UK strengthened the legal arsenal against phishing with the Fraud Act 2006, which introduces a general offense of fraud that can carry up to a ten year sentence and prohibits writing or possessing phishing kits with intent to commit fraud.

Companies have also joined the effort to crack down on phishing. On March 31, 2005, Microsoft filed 117 federal lawsuits in the U.S. District Court for the Western District of Washington. The lawsuits

accuse "John Doe" defendants of using various methods to obtain passwords and confidential information. March 2005 also saw Microsoft partner with the Australian government to teach law enforcement officials how to combat various cyber crimes, including phishing. AOL also reinforced its efforts against phishing in early 2006 with 3 lawsuits seeking a total of \$18 million USD under the 2005 amendments to the Virginia Computer Crimes Act, and EarthLink joined in by helping to identify six men subsequently charged with phishing fraud in Connecticut.

In January 2007, Jeffrey Brett Goodin of California became the first defendant convicted by a jury under the provisions of the CAN-SPAM Act of 2003. The CAN-SPAM act was the first piece of legislation that prosecuted illegal spam within the United States. He was found guilty of sending thousands of e-mails to America Online users while posing as AOL's billing department, which prompted customers to send personal credit card information. He faces 101 years in prison for the CAN-SPAM violation and ten other counts including wire fraud, unauthorized use of credit cards, and misusing AOL's trademark.

## Improving Security Measures

In February of this year, Paypal released its latest fraud protection technology. Paypal users now have the option of purchasing a five dollar security token that fits inside a pocket that randomly generates a six-digit code every 30 seconds. Every time a Paypal member logs into their account, they will have to enter the most recently generated number in order to gain access to their financial information. While this is the most proactive step Paypal has ever made, the five dollar cost may deter members from taking advantage of it. Currently, only Paypal Business Members are waived the five dollar charge for the token. The security device also signals how passwords, which were originally devised for user convenience, might one day be obsolete and replaced by the online equivalent to a combination lock. It will be very interesting to see in the next five years how many Paypal members will embrace this new device.



Another recent security measure Paypal has taken is its partnership with Equifax Credit Reporting Agency. This free service allows Paypal members to sign up and receive early warning emails from Paypal when new accounts are opened that may affect their credit file. In the event that identity theft actually occurs, users may call a 1-800 hotline offered through Equifax to report fraudulent activity and receive dedicated phone support from security specialists who will help track down the source of the theft.

## **What Actions Need to Be Taken**

Paypal is aware of this situation and strives to take every measure currently available to protect the security of its members. Even though Paypal provides guidelines that it recommends its users follow to ensure identity protection, the threat is real, and millions of not so savvy Internet users are at risk. In the event of an account hijacking, recourse is minimal, especially due to conflicting international laws with phishers in third world countries where Internet crimes are hardly punished without the intervention of US Federal agencies pressing foreign governments.

## **Our Research**

Out of the 125 people surveyed, 90% were familiar with Paypal's service. Only 40% were registered members, and 16% had an understanding of online phishing. 100% responded saying they have received an email, yet only 25% had some degree of skepticism before opening the mail. No one responded positive to having been a victim of identity theft or knowing anyone who did. Nearly half responded positively to sending personal financial information to confirm an online transaction. Only 30% would actually carry the security token if it meant their identity would not be compromised (See Appendix A).

These results were not surprising, because no one surveyed actually lost their identity or knew someone who had. That could indicate why only 30% would consider purchasing the token. It would be expected that the percentage would increase in the event of a survey respondent having a friend who had his identity stolen or the respondent himself having had his identity stolen. This would raise the awareness level and cause a proactive approach in the future in terms of protecting identities. The most interesting result of the survey was that 25% had some degree of skepticism before opening an email, yet only 16% had an understanding of what phishing was. This result was puzzling because it was expected that the 16% pool would have been greater than the 25% pool of skeptic respondents. Perhaps the 25% could indicate that a majority were skeptic for reasons other than phishing. Possibly, they were skeptic of obtaining spy-ware or ad-ware. This theory makes sense, because 40% had Paypal accounts and 100% received emails from Paypal. So this means that 100% of respondents who did not have a Paypal account received an email from Paypal which could only be fake because Paypal does not send emails to non-members.

## **Conclusion**

Phishers are always one step ahead of the game. Paypal along with Internet security companies have to be diligent in preventing new attacks, dedicating financial resources, and protecting their members. Phishers only have to be right once. One stolen identity can do immeasurable damage to a person. In the future, expect there to be a breaking point in the amount of online attacks and they will then be reduced to a minimal number. Steps such as issuing the new Paypal token provide the assurance of safety. But the double edged sword still

remains; if people want more protection, they may have to sacrifice leisure and convenience.

## Work Cited

Dinev, Tamara. "Why spoofing is Serious Internet Fraud." Communications of the ACM, 49 Oct. (2006): No. 10  
"Phishing is Catching on." Communication News, 44 Jan. (2007): No.1  
"Phishing Trip: A Majic Bullet Becomes the Crooks' New Weapon." Bank Technology News, 20 Jan (2007): No. 1.  
"The Latest in Phishing schemes uses dual authentication sign-ups to scam Bank. Customers." Bank Technology News, 20 Jan (2007): No. 1.  
Jakobsson, Markus. "Privacy & Security of Customers Information '07." The Human Factor of Phishing. Retrieved on February 2, 2007.  
Tan, Koon. Phishing and Spamming via IM (SPIM). *Internet Storm Center*. Retrieved on Dec 5, 2006. Skoudis, Ed. "Phone phishing: The role of VOIP in phishing attacks", searchSecurity, June 13, 2006

## Appendix A

A recent survey was administered to 125 people to find out their knowledge and behavior in online security theft pertaining to Paypal. Please answer the following question to the best of your knowledge. This research is completely confidential and will be used to comprise an academic paper.

1. Are you familiar with the Paypal payment service?
  - a. yes
  - b. no
  
2. Do you currently or have you ever had a Paypal membership?
  - a. yes
  - b. no
  
3. If you answered yes to #2, how much do you value Paypal for your online shopping capability? (Please circle your response)  

NOT IMPORTANT	1	2	3	4	5	6	7	8	9	10	VERY IMPORTANT
---------------	---	---	---	---	---	---	---	---	---	----	----------------
  
4. Do you know what the term Phishing means?
  - a. yes
  - b. no
  
5. Whether or not you are a Paypal member have you ever received an email (notification) from them?
  - a. yes
  - b. no
  
6. If Yes to #5, were you skeptical before opening the mail?
  - a. yes
  - b. no

7. Have you ever experienced any level of credit card theft?
  - a. yes
  - b. no
  
8. Are you comfortable giving your banking information via e-mail, to secure or confirm an online transaction?
  - a. yes
  - b. no
  - c. no, but do it anyway to avoid any hassle with my purchase
  
9. Would you pay \$5 for a palm-sized token that generated you a new password every 30 seconds if it guaranteed your account would be safe?
  - a. yes
  - b. no
  
10. Do you know someone who had their identity stolen?
  - a. yes
  - b. no