

## Paypal - 'Update Account.' Le 29-Avril-2005

## Summary

Email title:	'Update Account.'
Scam target:	Paypal users
Sender:	service@paypal.com
Sender spoofed/hidden?	Spoofed
Scam goal:	Getting victim's credit card information, other personal information
Phish link method:	a 'Click Here' type link
Link 'masked'?	Yes
Visible link:	'Please click here to update your billing records.'
Actual link to:	<a href="http://review-data.org/go.html">http://review-data.org/go.html</a>
Resolved URL:	<a href="http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd_login_access_account_uptead_curreny(truncated)">http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd_login_access_account_uptead_curreny(truncated)</a>
Phish site IP:	83.16.123.18

Analysis contributed by: Tumbleweed Communications - Message Protection Lab

## Overview

## E-mail

The email is very convincingly shaped up, but the threatening aspect does not look much like a legitimate company's communication with its customers:



Dear bpmoe@hotmail.com

It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.

Failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

[Please click here to update your billing records.](#)

---

Thank you for using PayPal!  
The PayPal Team

Your monthly account statement is available anytime; just log in to your account at <https://www.paypal.com/us/HISTORY>. To correct any errors, please contact us through our Help Center at <https://www.paypal.com/us/HELP>.

---

FOR INTERNATIONAL PAYMENTS ONLY

Commissions and Fees incurred by sender: \$0.00

Rate of Exchange: If and when the Recipient chooses to withdraw these funds from the PayPal System, and if the withdrawal involves a currency conversion, the Recipient will convert the funds at the applicable currency exchange rate at the time of the withdrawal, and the Recipient may incur a transaction fee.

RIGHT TO REFUND

You, the customer, are entitled to a refund of the money to be transmitted as a result of this agreement if PayPal does not forward the money received from you within 10 days of the date of its receipt, or does not give instructions committing an equivalent amount of money to the person designated by you within 10 days of the date of the receipt of the funds from you unless otherwise instructed by you.

If your instructions as to when the moneys shall be forwarded or transmitted are not complied with and the money has not yet been forwarded or transmitted, you have a right to a refund of your money.

If you want a refund, you must mail or deliver your written request to PayPal at P.O. Box 45950, Omaha, NE 68145-0950. If you do not receive your refund, you may be entitled to your money back plus a penalty of up to \$1,000 USD and attorney's fees pursuant to Section 1810.5 of the California Financial Code.

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, [log in](#) to your PayPal account and choose the Help link located in the top right corner of any PayPal page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID PP120

## Web Site

Visible link:	<a href="http://www.citizensbankonline.com/logon/secaresurvey.asp">http://www.citizensbankonline.com/logon/secaresurvey.asp</a>
Actual link to:	<a href="http://review-data.org/go.html">http://review-data.org/go.html</a>
Resolved URL:	<a href="http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd_login_access_account_uptead_currency(truncated)">http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd_login_access_account_uptead_currency(truncated)</a>
Phish site IP:	83.16.123.18

The site first opened is just a redirect. The second site is where the phish resides.

There is no login screen imitation. The site demands information immediately:

**PayPal** [Help](#)

**My Account** **Send Money** **Request Money** **Merchant Tools** **Auction Tools**

**Overview** **Add Funds** **Withdraw** **History** **Profile**

### Update your Credit Card or Debit Card


Debit Cards (also called check cards, ATM cards or banking cards) are accepted if they have a Visa or MasterCard logo.

**Email Address:**






**Password:**

**First Name:**


**Last Name:**

**PayPal VISA CARD**  
**Get Clear Choices!**  
  
**Apply Now!**  
30-second Response  
Your Choice of

**Card Type:**

**Card Number:**      

**Expiration Date:**  /

**Card Verification Number:**   (On the back of your card, find the last 3 digits) [Help finding your Card Verification Number](#)

**Name On Card:**

**Mothers Maiden Name:**

**Social Security Number:**

**Date Of Birth:**  /  /

**Card Pin**  4 Digit code used in ATMs. (For verification with bank)

Billing Address

Enter the address where you receive monthly billing statements for this card:

**Enter billing address**

**Address 1:**

**Address 2:**   
(optional)

**City:**

**Phone Number**

**State:**

**Zip Code:**  (5 or 9 digits)

**Country:**

**For your protection, we verify credit card and debit card billing addresses.**

The process normally takes about 30 seconds, but it may take longer during certain times of the day. Please click **Continue** to update your information. When your card has been successfully added, you will see a confirmation page.

Continue

**Card Designs**



[an eBay Company](#)

Copyright © 1999-2004 PayPal. All rights reserved.  
[Information about FDIC pass-through insurance](#)

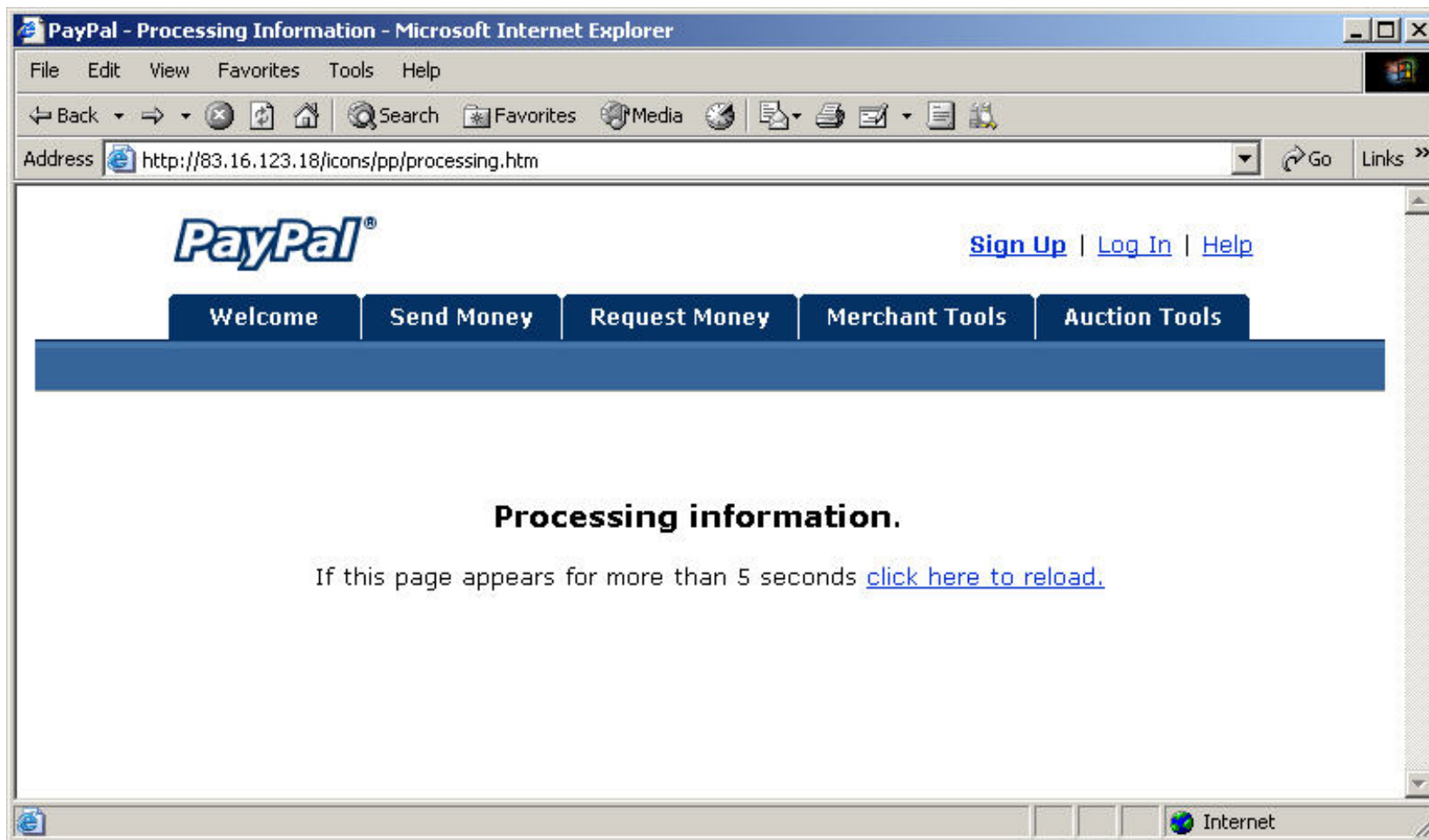
The main phishing clue is the URL in the address bar:

Address  http://83.16.123.18/icons/pp/update.htm?=https://www.paypal.com/=cmd\_login\_access\_account\_uptead\_curreny%%%di

Though it has 'https://paypal.com' in it, this is in the path part, not the domain name. This site is NOT Paypal.

The lack of a security certificate also points to a scam going on (the presence of a security certificate is indicated by a lock icon in the status bar of IE).

The site would accept any information passed - no checks will be made. Then, a fake 'processing delay' page pops up:



Followed by a fake logout screen:

Your information submitted - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Print Preview Stop

Address <http://83.16.123.18/icons/pp/processed.htm> Go Links >>

**PayPal** [Sign Up](#) | [Log In](#) | [Help](#)

Welcome Send Money Request Money Merchant Tools Auction Tools

## Your information submitted successfully

Your submitted information will be verified by PayPal Accounts Management Department in 24 hours.

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [User Agreement](#) | [Developers](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

[an eBay Company](#)

Copyright © 1999-2004 PayPal. All rights reserved.  
[Information about FDIC pass-through insurance](#)

reviewed by **TRUST.e** site privacy statement **PRIVACY** BBBONLINE