

**Paypal - 'Your PayPal account will be suspended'**  
**Circulant depuis le 1er avril 2005**

**En résumé**

Titre de l'email	'WARNING!!! Your PayPal account will be suspended!!!'
La cible	Les utilisateurs de PayPal
L'objectif	Obtenir les informations du compte PayPal (dont le mot de passe)
La méthode	Un lien 'Click Here' invitant à se connecter
Lien effectif	<a href="http://www.paypal-cgi.us/webscr.php?cmd=LogIn">http://www.paypal-cgi.us/webscr.php?cmd=LogIn</a>
L'adresse du site	68.142.234.44

Les contributeurs à remercier pour cette analyse:

Tumbleweed Communications - Message Protection Lab (reporté par APWG ".org")

**L'email transmis**

Un email sobre donc assez dangereux!



**Security Measures**

Dear Paypal Customer,

In accordance with our major database relocation, we are currently having major adjustments and updates of user accounts to verify that the informations you have provided with us during the sign-up process are true and correct. However, we have noticed some discrepancies regarding your account at Paypal. Possible causes are inaccurate contact information and invalid logout process.

We require you to complete an account verification procedure as part of our security measure.

You must click the link to complete the process.

[Click here to confirm your account](#)

**Please Note**

Unable to do so may result to abnormal account behavior during transactions. We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,  
PayPal Account Review Department  
PayPal Email ID PP560

En première lecture seule l'expression anonyme "Dear Paypay Customer" attire l'attention.  
Pourquoi PayPal n'utilise pas le nom du destinataire? Cet anonymat est révélateur!

### Le Site Web proposé via le lien "Click here"

L'astuce du fraudeur est basée sur un nom de domaine proche d'un domaine PayPal.

The screenshot shows a phishing website designed to look like the PayPal login page. The browser window is titled "Log In - Microsoft Internet Explorer" and the address bar contains the URL "http://www.paypal-cgi.us/webscr.php?cmd=LogIn". The page layout includes the PayPal logo at the top left, with "Sign Up | Log In | Help" links to the right. Below this is a dark blue navigation bar with buttons for "Welcome", "Send Money", "Request Money", "Merchant Tools", and "Auction Tools". The main content area is titled "Member Log In" and includes a "Secure Log In" icon. The text reads: "Registered users log in here. Be sure to [protect your password](#)." Below this are two input fields: "Email Address:" and "Password:", each with a "Forget your [email/password]?" link. A message for new users says "New users [sign up here!](#) It only takes a minute." A "Log In" button is positioned at the bottom right of the login section. The footer contains a list of links: "About | Account Types | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buyer Credit | Referrals | Shops | Mass Pay", followed by "PayPal, an eBay company" and a copyright notice: "Copyright © 1999-2004 PayPal. All rights reserved. [Information about FDIC pass-through insurance](#)".

L'absence de toute session HTTPS trahit définitivement la tentative de phishing!