

Gone Phishin'

Phishing Email Received by Mrs. B:

The screenshot shows an email client window titled "Notice of Account Review Necessity : Greenwich Pub. Schools". The email header includes the date "Friday, May 4, 2007 12:55:44 PM", the sender "PayPal" (service@paypal.com), and the recipient "Karen Ball". The main body of the email contains a "Notice of Account Review Necessity" with instructions to read the notice thoroughly. It asks "Why did I get the notice?" and "What should I do now?". A yellow button with the text "Click here to confirm your account" is highlighted, with an arrow pointing to it from a callout box that says "Link to a 'spoofer' server". The email also includes a "Protect Your Account Info" sidebar with security tips and a "Protect Your Password" section.

Notice of Account Review Necessity

Read this notice thoroughly and follow the instructions.

Why did I get the notice?

You have been sent this notice because the records of PayPal database indicate you are a current or former PayPal account holder. PayPal is conducting a periodic update of the database record. To ensure your account's security, it is important that you provide us accurate information. Please take a moment to verify the information we have on file. This notice provides instructions on how to confirm your PayPal account.

What should I do now?

We sincerely ask you, as a PayPal account holder, to login to your account and give us the necessary information. Complete the necessary verification tasks within 5 days, or your account might get temporarily suspended. Proceed with the link below.

[Click here to confirm your account](#)

We apologize for your inconvenience.

Thank you for your support,
PayPal Accounts Department

Please do not reply to this email. Anything you send to this address cannot be answered. For assistance, [login](#) to your PayPal account and choose the "Help" link in the footer of any page.

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

PayPal Email ID PPS71

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser and type in the PayPal URL to be sure you are on the real PayPal site.

For more information on protecting yourself from fraud, please review our [Security Tips](#)

Protect Your Password

You should **never** give your PayPal password to anyone, including PayPal employees.

Link to a "spoofer" server

How do I know this is a fake?

1. They sent it to my work email. I never use this email for Paypal or eBay.
2. Paypal never asks users for account information via email. They leave messages in your account on their secure server, which you can only see if you have logged onto your account. Banks and other corporations or institutions who handle money (or sell things online) also will not ask you for personal information through an email.

Where does the “confirm your account” link in this phishing email go to?

The screenshot shows a browser window titled "PayPal - Login" with the address bar containing "http://200.86.131.236/~paypal/secure/index.php". The page features the PayPal logo, navigation links for "Sign Up", "Log In", and "Help", and a menu with "Welcome", "Send Money", "Request Money", "Merchant Tools", and "Auction Tools". The main heading is "Member Log In" with a "Secure Log in" icon. Below this, it says "Registered users log in here. Be sure to [protect your password](#)." There are input fields for "Email Address:" and "Password:" with a "Forget your password?" link. A "New users [sign up here!](#) It only takes a minute." message is present. A "Log In" button is at the bottom right. Footer links include "About", "Accounts", "Fees", "Privacy", "Security Center", "Contact Us", "User Agreement", "Developers", "Buyer Credit", "Referrals", "Shops", "Mass Pay", and "PayPal, an eBay company". Copyright information for 1999-2007 PayPal is also visible.

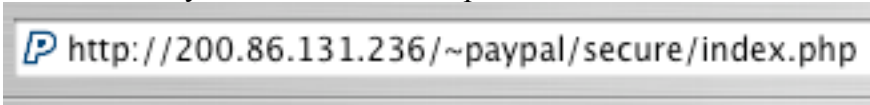
It goes to a server – NOT a Paypal server. This looks *almost* identical to the Paypal login page (they missed the “forgot your email” link).

Here’s the REAL login page:

The screenshot shows the real PayPal login page in a browser window with the address bar containing "https://www.paypal.com/cgi-bin/webscr?cmd=_login-run". The page features the PayPal logo, navigation links for "Sign Up", "Log In", "Help", and "Security Center", and a menu with "Welcome", "Send Money", "Request Money", "Merchant Services", and "Auction Tools". The main heading is "Member Log-In" with a "Secure Log In" icon. Below this, it says "Registered users log in here. Be sure to [protect your password](#)." There are input fields for "Email Address:" and "Password:" with links for "Forgot your email address?" and "Forgot your password?". A "New users [sign up here!](#) It only takes a minute." message is present. A "Log In" button is at the bottom right. Footer links include "About", "Accounts", "Fees", "Privacy", "Security Center", "Contact Us", "Legal Agreements", "Developers", "Jobs", "Mobile", "Plus Card", "Referrals", "Shops", "Mass Pay", and "PayPal, an eBay company". Copyright information for 1999-2007 PayPal is also visible.

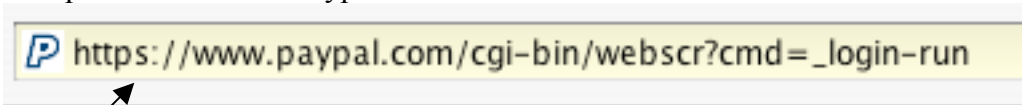
The spoof server could be anywhere in the world. When you fill in the boxes with your email address and your password, you have just given the crooks all the information they need to empty your Paypal account and any bank accounts or credit cards that are linked to your Paypal account.

Look carefully at the URL in the top window:



<http://200.86.131.236/~paypal/secure/index.php>

Compare to the REALPaypal URL:



https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

The “s” in “https” is for “secure” – this is an encrypted server that is using high security protocols. Banks and many internet companies that deal with buying and selling use this to protect credit card and bank account information. Greenwich Public Schools uses secure servers also.

Notice that the rest of the real URL starts with “paypal.com” and the spoof one starts with a string of numbers. Those numbers are the IP (Internet Protocol) address of the server. It is NOT secure. It may well be sitting in Joe Schmo’s momma’s basement in Idaho, or someplace in China, Asia or Africa. You have no way to know!

The FBI and Interpol are working furiously to battle online fraud like this. It is difficult if the criminals are outside the United States or Europe, as many third world countries do not have the law enforcement officers, equipment or training to handle this type of crime. Millions of people fall for this and lose substantial amounts of money to the crooks.

So what do I do about this?

1. BE SUSPICIOUS! Be extremely careful about emails that ask you for personal information. When in doubt, call your bank or contact the online group directly and ask about the email. DO NOT use the links within the email – log on separately as you normally would, or call.
2. Forward emails like this to the security or fraud detection team at the group that is being targeted. I sent this to the fraud team at Paypal.
3. Delete phishing emails from your email account.
4. Do not respond to the email. This may make you feel temporarily better but what you are actually doing is letting them know that you have an active email address, and that you read your emails. They will put your email on a list and sell the list to others who will send you more phishing and spam.