

Don't Get Hooked By Phishing!

Did you know that emails appearing to come from companies you trust may actually be from criminals trying to steal your money or identity? So-called "phishing" emails have quickly become one of the most devastating scams on the Internet.

What is Phishing?

Phishing scams use hoax emails and phony Web sites to trick you into providing your personal and financial information. By using the trusted brands of online retailers, banks, or credit card companies, phishing scammers are able to convince about 5% of recipients to give them credit card numbers, bank account numbers, and passwords that can be used to defraud them or even steal their identity.

How Do Phishing Scams Work?


The most common scam is an email that looks like it's from a company with whom you may have an account. The email directs you to a phony Web site to update your account with financial or personal information. If you provide the information, the scammers use your data to steal your identity, purchase goods and services, or open a credit card in your name.

How Can I Avoid Being Tricked by Phishing Scams?

1. Don't click on links in an email to get to a Web page. If a company appears to ask for your personal information by email, close the email and type in the company website name in your web browser. Examples: www.aol.com or www.bankone.com If you don't know the website name, go to www.Google.com and get it.
2. Don't fill out forms in email messages, especially when the forms request personal information. Watch out for emails with urgent requests that require you to act quickly.
3. Make sure you use a secure browser when submitting personal or financial information. A secure browser will have a URL address that begins with [httpS://](https://) and ends with a padlock icon rather than the standard <http://>
4. Use an anti-phishing protective solution, such as the one offered in [ZoneAlarm Security Suite](#). A separate Fraudulent Folder is integrated with your email (Outlook or Outlook Express) so that phishing and other fraudulent emails won't reach your Inbox.

Here are five typical E-mail Phishing Scam pages:

1 Fake Email and Web Forms



Dear Wells Fargo Customer,

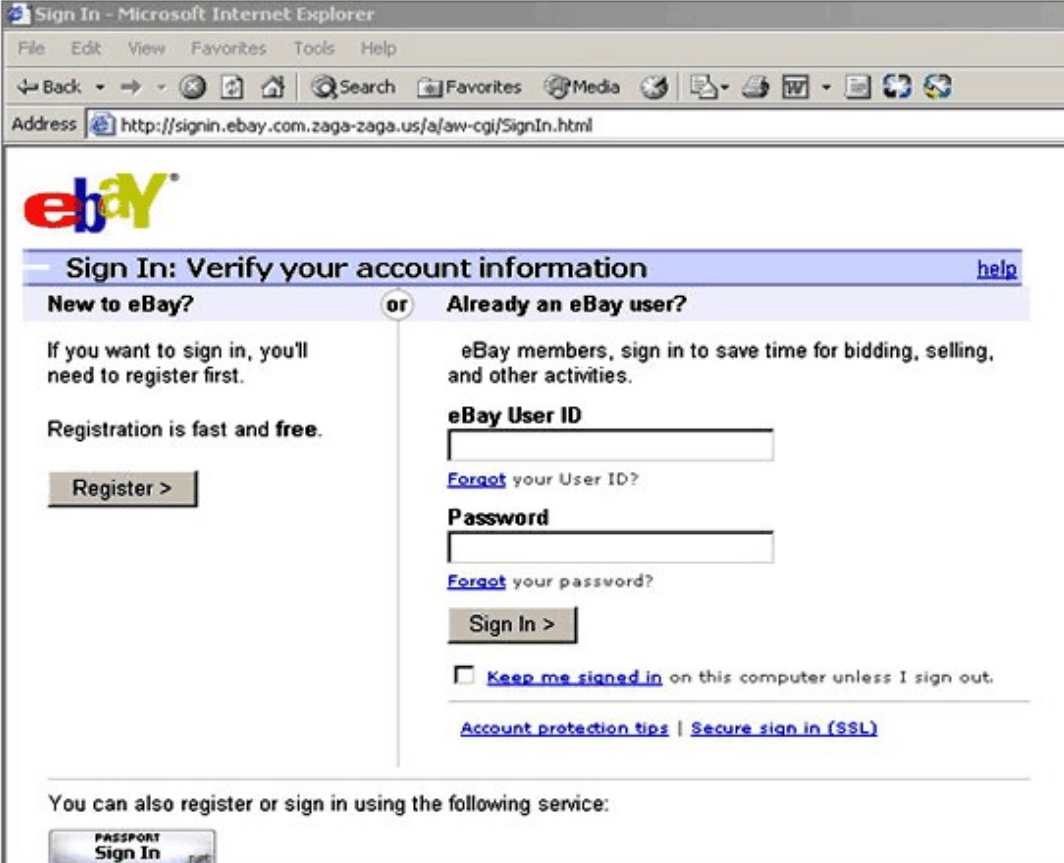
We are glad to inform you, that our bank is switching to new transactions security standards. The new updated technologies will ensure the security of your payments through our bank. Both software and hardware will be updated.

We kindly ask you to confirm your ATM card details here:
<http://online.wellsfargo.com/?customersupport=CONFIRMATION>

We offer you a new convenient and safe high-quality level of service to handle your ATM card.

© Wells Fargo Customer Support.

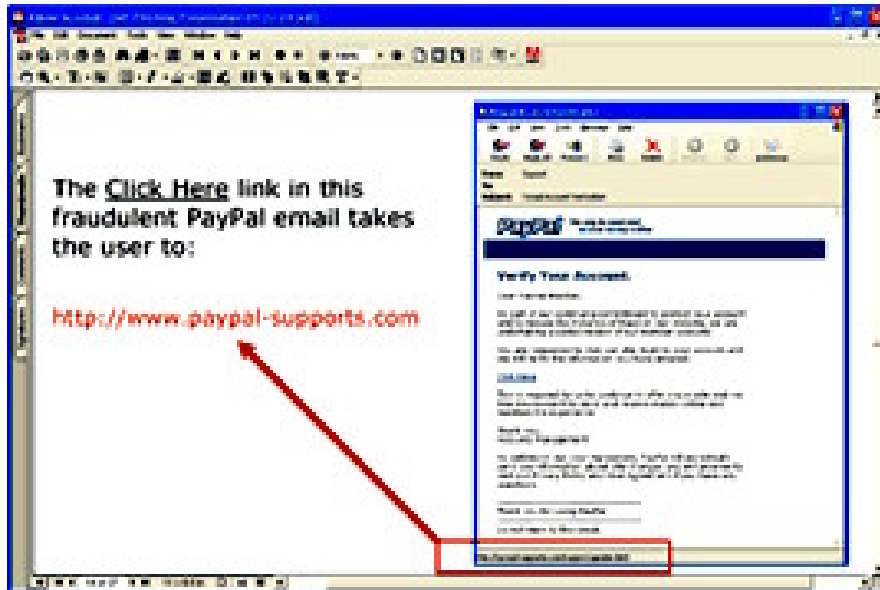
2 Credible-looking URLs are Really Fakes



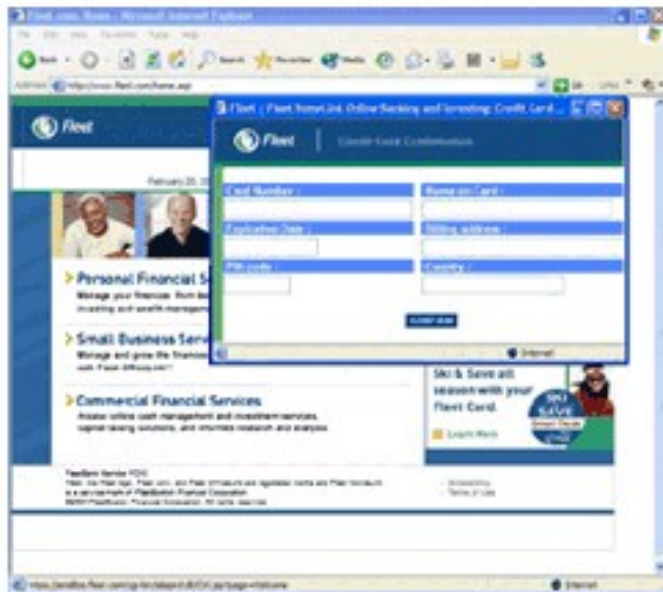
The screenshot shows a Microsoft Internet Explorer browser window. The title bar reads "Sign In - Microsoft Internet Explorer". The address bar contains the URL "http://signin.ebay.com.zaga-zaga.us/afaw-cgi/SignIn.html". The page content features the eBay logo and a sign-in form titled "Sign In: Verify your account information". The form has two columns: "New to eBay?" with a "Register >" button, and "Already an eBay user?" with fields for "eBay User ID" and "Password", a "Sign In >" button, and a checkbox for "Keep me signed in". A "help" link is visible in the top right of the form area. At the bottom, there is a section for "You can also register or sign in using the following service:" with a "PASSPORT Sign In" button.

Scammers will often use a credible sounding, but fraudulent, domain name.

3 False URLs displayed in Status Bar



4 Fraudulent Pop-Up Windows (over Legitimate Sites)



5 False URLs displayed in Status Bar

