

Phishing: The act of sending an e-mail to a user **falsely claiming to be an established legitimate enterprise** in an attempt to **scam** the user into surrendering private information that will be used for **identity theft**. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is **bogus** and set up only to **steal the user's information**. (Source: www.webopedia.com)

Legitimate WellsFargo.com

The screenshot shows the legitimate Wells Fargo website homepage. The browser address bar displays the URL <https://www.wellsfargo.com/>. The page features the Wells Fargo logo, navigation tabs for Personal, Small Business, Commercial, and About Us, and a search bar. The main content area includes a "View Your Accounts" section with login fields for Username and Password, and a "One Team, Twice As Strong" banner for Wachovia. Below the banner are sections for Banking, Loans, and Investing, each with links to various services. There are also sections for "Open an Account", "Check Today's Rates", and "Home Equity Financing".

Phishing Site: (Read the URL Address Line) Is it different than the legit site?

The screenshot shows a phishing site that impersonates the Wells Fargo website. The browser address bar displays the URL http://www.puertaoskura.info/www.wellsfargo.com/online_banking/update.html. The page layout is identical to the legitimate site, but the URL is suspicious. The main content area features a banner for "TODAY | Visit Our Home Resource Center" with a list of benefits: "Get a FREE mortgage prequalification", "Discover our NEW Home Improvement Program", and "Find out about special offers & discounts". Below the banner are sections for Banking, Loans, and Investing, and a "Get Started Now" button. The URL address line is the key indicator of a phishing site.