

visit or use trusted services like CityBank or Paypal when their address are shown as something like 211.158.34.250/citifi/ (

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [October](#) >

Never visit or use trusted services like CityBank or Paypal when their address are shown as something like 211.158.34.250/citifi/

LinuxReviews.org

The above URL point to criminals who, at the moment of writing, have set up a website that looks identical to Citybanks pages. The site is announced in a mail that warns customers that their security is compromised and advices customers to visit Citybank in order to verify their personal details. The link looks like it is pointing to their official sites, while it actually refers user to a fishing scam site.

Fishing scams is a ever-increasing problem on the Internet. It is very easy to setup a website that looks, feels and behaves just like any real and authentic site. These fishing sites are used to fool people into giving away their credit card details and frequently announced by sending millions of e-mail spam messages.

It is very important that you verify that the URL, universal resource locator, that is shown in your browsers address field is the domain that actually belongs to the service you are using. Also make sure the address starts with `https://`, showing you are connected using a secure socket. Known services do not use IP addresses (numbers) to communicate securely with their users.

It is quite possible to make a link that looks like it is pointing one place while it is actually pointing somewhere else using simple hypertext tricks. Good mail clients do not fall for this trick, but most Windows based mail clients do. It is generally preferable to use a mail client that displays only the text version of mail, and only the source of hypertext messages when no alternative is provided. Only spam senders and idiots send hypertext-only messages anyway. Know that you should verify that the link you think you are visiting when clicking a e-mail message is the same link that appears in your browsers location bar.

Criminals are currently operating a fishing site at <http://211.158.34.250/citifi/>. The site looks a login form for CityBank Online Internet Banking and is meant to fool people into giving away their account information:

Never visit or use trusted services like CityBank or Paypal when their address are shown as something like

Never visit or use trusted services like CityBank or Paypal when their address are shown as something like 211.158.34.250/citifi/ (

CityBank and PayPal are the most popular targets for these scams, but other services are also targeted.

Things you can do to prevent being scammed:

- Make sure the connection is secure, using the https protocol, when giving sensitive details on the net
- Make sure you verify that the address displayed in the browser refers to the site you think you are using.
- Make sure you are using the latest available version of your browser. Opera verisons > 7.52 and most versions of Internet Explorer can be fooled into displaying anything in the location bar, make sure your browser is safe and not capable of being tricked into displaying fake locations.

This is not news, such scams have been going on for years. However, the site mentioned here is not yet closed, and the criminals involved are not yet arrested and shot to death (if that is allowed at their current location) as they should be: They are guilty in serious bank fraud and worse, guilty of sending millions of spam messages.

More:

- [Check what URL is actually used when using banks or submitting credit card information! The number of Phishing scams is increasing.](#)

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [October](#) >

Never visit or use trusted services like CityBank or Paypal when their address are shown as something like 211.158.34.250/citifi/

Never visit or use trusted services like CityBank or Paypal when their address are shown as something like