

# All Linux Browsers are vulnerable to web site address spoofing

*LinuxReviews.org*

The International Domain Name system (IDN) which allows local characters to be used as part of domain names can be used to fool browser into showing the wrong URL displayed in the address bar, status bar and even on SSL certificates.

Browsers based on both khtml (Konqueror, Safari) and gecko (Mozilla, Galeon, Firefox) are open to so called Homograph attacks. Opera 7.54 is also vulnerable. The technique allows evil people to spoof the URL (domain address) of known businesses. By linking to a spoofed page that looks very much like the attacked business the evil ones can fool people into thinking they are on a trusted site.

Homograph attacks were described as early as December 2001, before any browsers had actually implemented the new IDN domain name standard that allows Unicode and UTF-8 characters to be used as part of domain names.

Internet Explorer, Dillo and Links are just about the only browser on the planet that is not exploitable, but this is simple because they do not support IDN at all. There is a plug-in available for Internet Explorer and people who use that are also exploitable.

Eric Johanson has made a proof of concept page available (actually links to [www.p&#1072;ypal.com](http://www.p&#1072;ypal.com)):

[www.paypal.com](http://www.paypal.com)

All Linux Browsers are vulnerable to web site address spoofing (Linux Reviews)

This will take you to `www.xn--pypal-4ve.com`, not `www.paypal.com` as it may appear.

**Mozilla** and **Firefox** users can protect themselves by going to the URL `about:config` where you will be able to set the value `network.enableIDN` to `false`.

Phishing, meaning using false sites to fool visitors into giving you their credit cards and other valuable information by claiming to be a known business, is a huge problem on the Internet today. Phishing sites are frequently advertised using SPAM mail, often with spoofed headers and content that looks like a regular mail from a known service. Mail clients such as kmail use khtml to render html messages and can be fooled using the same technique (note that kmail by default has html mail and other features with security problems disabled, so this would only be a problem if you have manually asked to allow insecure features).

**There is really no way** a business can protect itself against IDN spoofing. It is obviously possible to register all possible IDN variants of your domain, but that would be an extremely expensive solution.

More information:

- <http://www.shmoo.com/idn/>
- [http://secunia.com/multiple\\_browsers\\_idn\\_spoofing\\_test](http://secunia.com/multiple_browsers_idn_spoofing_test)

---

> [Linux Reviews](#) > [News and headlines](#) > [2005 News archive](#) > [February](#) >  
All Linux Browsers are vulnerable to web site address spoofing