

## Internationalized Domain Names and Homograph Attacks

Author:  
**Resale Rights**

Created On: 07 Oct 2009 10:03 PM

---

With normal spoofing a scammer tries to get personal information by sending fraudulent emails masquerading as an official website an individual might be working with. While some fall for the deception, many know better since the domain name in the email doesn't resemble the domain name they usually use to access whatever site. However, what happens if a domain name looks exactly like an official website?

This, in combination with a more 'professional' email, could trick someone into giving away all of their personal data. And when this happens they will eventually become victims of identity theft. But, how can a scammer acquire a domain name that looks official? It's through the unfortunate practice of the homograph attack.

What is a homograph attack? A homograph attack is when a person makes an internationalized domain name, (also known as an IDN), look like a traditional domain name associated with a popular website. They are able to do this because of the way internationalized domain names work. Basically, internationalized domain systems use a different type of coding system than the ASCII-based domain names Americans are used to.

However, even with a different coding system, some languages have characters that look similar to characters used in American English. Scammers exploit this by taking these letters and creating domain names that look 'new' to browsers and servers, at least in terms of coding. To the human eye, these fraudulent domain names appear to already be taken, which is exactly what a scammer wants. They cause further confusion by creating sites that look pretty much like the sites associated with the original domain name that the scammers are spoofing.

Before and even after internationalized domain names became popular, homograph attacks were expressed through spoofing just English characters. Scammers exploited the visual similarities between 'O' and '0' or 'l' and 'I'. Examples include 'G00Gle.com' or 'PayPal.com'. If a person is not paying attention, they could still become victims, but at least these types of domain names still look unusual. With internationalized domain name homograph attacks, the above-mentioned websites could look just as they are supposed to, fooling even the most vigilant Internet user.

So, how can a person prevent becoming a victim of an internationalized domain name homograph attack? First, they should never click on any domain name that is given through an email. Instead, they should enter the domain name manually into their browser. In situations where one is working with a third-level domain that could be harder to remember, Internet users need to copy and paste the domain name into Notepad. This program will help them determine what character set and coding is being used for the domain name. If it's not English and ASCII, a person should be weary.

In conclusion, internationalized domain name homograph attacks can cause a lot of havoc for Internet users. However, Internet users should find comfort in the fact that while they do need to be aware of the presence of the homograph attack, the traditional method of spoofing which is much easier to spot tends to be more common. This is because a person must be both clever and lucky

to land an internationalized domain name that looks that much like a domain name that is already in use.Â It's much easier for scammers to try and fool people through email hyperlinks.