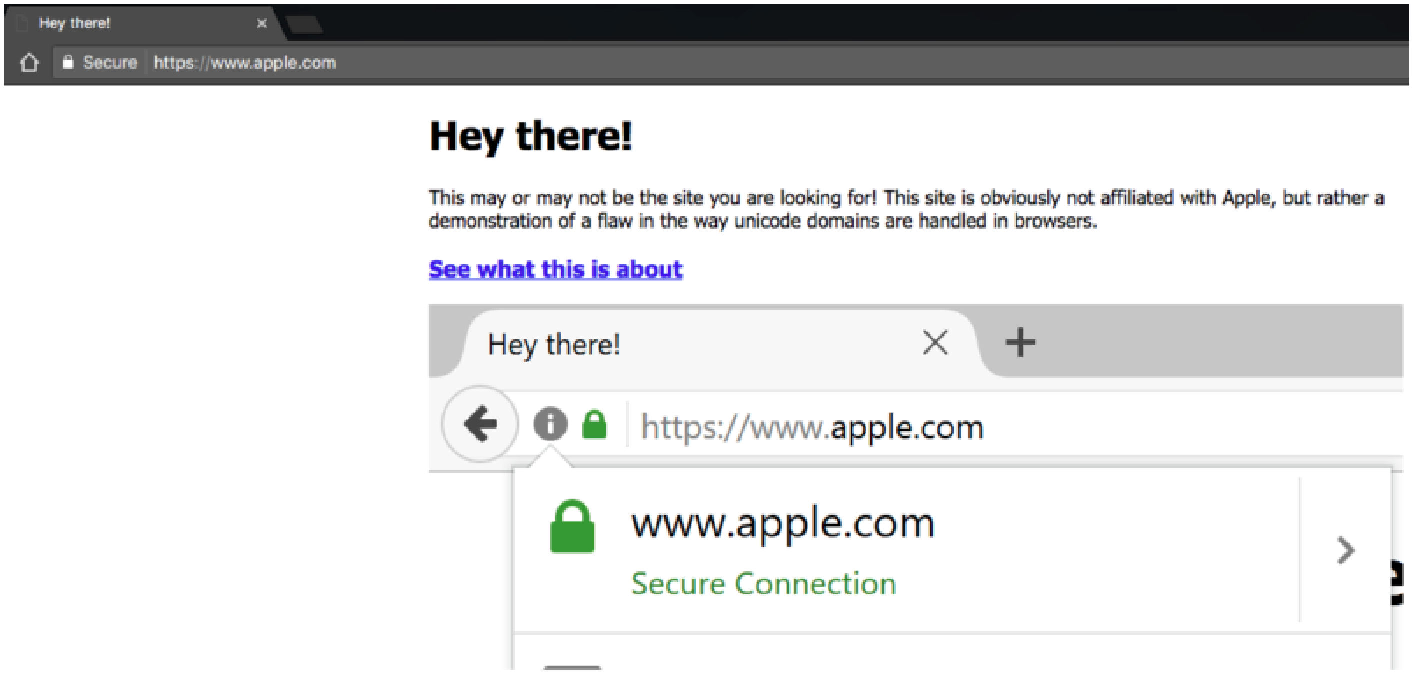
*RISK ASSESSMENT —*

# Chrome, Firefox, and Opera users beware: This isn't the apple.com you want

Unicode sleight of hand makes it hard for even savvy users to detect impostor sites.

DAN GOODIN - 4/20/2017, 11:34 AM



## Hey there!

This may or may not be the site you are looking for! This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers.

See what this is about

Enlarge / **This is how a Chrome 57 displays https://www.xn--80ak6aa92e.com/. Note the https://www.apple.com in the address bar.**

If you're using Chrome, Firefox, or Opera to view websites, you should be aware of a weakness that can trick even savvy people into trusting malicious impostor sites that want you to download software or enter your password or credit card data.

The weakness involves the way these browsers display certain characters in the address bar. Until Google released version 58 in the past 24 hours, for instance, Chrome displayed https://www.xn--80ak6aa92e.com/ as https://www.apple.com. The latest versions of Firefox and Opera by default continue to present the same misleading address. As the screenshot above demonstrates, the corresponding website has nothing to do with Apple. Had a malicious attacker registered the underlying xn--80ak6aa92e.com domain, she could have used it to push backdoored software or to trick visitors into divulging passwords or other sensitive information.

Xudong Zheng, a Web application developer who developed the apple.com look-alike site to demonstrate the threat, explained here how the attack works.

> Punycode makes it possible to register domains with foreign characters. It works by converting individual domain label to an alternative format using only ASCII characters. For example, the domain "xn--s7y.co" is equivalent to "短.co".
>
> From a security perspective, Unicode domains can be problematic because many Unicode characters are difficult to distinguish from common ASCII characters. It is possible to register domains such as "xn--pple-43d.com", which is equivalent to "apple.com". It may not be obvious at
> uses the Cyrillic "a" (U+0430) rather than the ASCII "a" (U+0061). This is known as a homograph attack.

SIGN IN

> Fortunately modern browsers have mechanisms in place to limit IDN homograph attacks. The page IDN in Google Chrome highlights the conditions under which an IDN is displayed in its native Unicode form. Generally speaking, the Unicode form will be hidden if a domain label contains characters from multiple different languages. The "аpple.com" domain as described above will appear in its Punycode form as "xn--pple-43d.com" to limit confusion with the real "apple.com".
>
> The homograph protection mechanism in Chrome, Firefox, and Opera unfortunately fails if every characters is replaced with a similar character from a single foreign language. The domain "аррӏе.com", registered as "xn--80ak6aa92e.com", bypasses the filter by only using Cyrillic characters. You can check this out yourself in the proof-of-concept using Chrome, Firefox, or Opera.
>
> Visually, the two domains are indistinguishable due to the font used by Chrome and Firefox. As a result, it becomes impossible to identify the site as fraudulent without carefully inspecting the site's URL or SSL certificate. This Go program nicely demonstrates the difference between the two sets of characters. Safari, along with several less mainstream browsers are fortunately not vulnerable.

The issue has generated an interesting discussion on the Mozilla developer forum. For now, lead developers have indicated they won't change the default behavior when the browser encounters punycode-based domain names.

Such a change "would make all non-Latin domain names show as gibberish," Mozilla developer Gervase Markham wrote. "That's not really a good thing for people, countries and languages which don't use Latin letters. We want every script and language to be treated equally on the Internet."

People who use Chrome should install version 58 as soon as possible. Firefox users can protect themselves by entering "about:config" in the address bar and agreeing to the displayed warning. From there, enter "punycode" in the search box to bring up a line that reads network.IDN_show_punycode. Next, double-click the word "false" to change it to "true." From then on, Firefox will display the "dumb ascii" characters and not the deceptive, encoded ones. Besides Apple's Safari, Microsoft's Edge and Internet Explorer browsers are also not affected, at least as long as they don't have support for a Cyrillic language.

The weakness was reported to Chrome developers in January. Security firm McAfee has more about this problem here.

## Promoted Comments

starglider / Smack-Fu Master, in training / *et Subscriptor* JUMP TO POST

Wow this is just . . . brilliant. And somewhat humbling. I like to think of myself as someone who is pretty careful and hard to fool. As far as I know, I've never been successfully phished.

All that said, if I got an email from "Apple" (or Lastpass or a hundred other sensitive sites) with a link to change my password, and it took me to that page, I'm fairly sure I'd have fallen for it.

66 posts | registered 10/15/2012

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

**EMAIL** dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 109

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

**Related Stories**

**Today on Ars**

SIGN IN

VISIT ARS TECHNICA UK
ABOUT US
ADVERTISE WITH US
REPRINTS