

IDNs and Phishing: What You Need to Know

April 27, 2017

[Internationalized Domain Names](#) (IDNs) are growing in popularity, a testament to their role in the expansion of the global Internet and the value they provide in connecting non-English speakers to the Web. However, a renewed focus was raised in April 2017 of a script mixing technique that phishing scammers could potentially use to trick Internet users into visiting malicious websites. This phishing method takes advantage of the fact that characters from various languages and scripts are sometimes visually similar to each other. For example, the Cyrillic “a” and the Latin “a” look virtually identical. This technique is known as a homograph attack.

Homographic phishing efforts associated with IDNs are [rare](#). They’re also not new. In fact, they date back to the early 2000s. Registries have since implemented policies that preclude mixing scripts¹ within a domain name label and different browser software have implemented a variety of methods to reduce the opportunity for user confusion.

While this issue should be taken seriously and serves as an important reminder of consumer safety, various IDN and anti-abuse groups are actively working to mitigate potential threats, and there are already certain browser-set protections in place. In the meantime, Internet users should practice the same basic security hygiene that is always recommended: avoid clicking links from suspicious sources, manually enter the URL when in doubt, and use a good password manager that will only enter login credentials on trusted sites.

The context for this news is the important and welcome spread of [Internationalized Domain Names](#) (IDNs). These make global Internet accessible to billions of people who use languages other than English. It is important to recognize the benefits of IDNs and avoid disabling them, which could lead to an unpredictable user experience and eventually a decrease in adoption. IDNs are essential in bringing non-English speakers – the majority of the world’s population – online, and allowing those users to create their own highly relevant online identities as well as navigate the Internet in their native languages. In addition to the social and cultural benefits of IDNs, they also represent a significant economic opportunity; a recent [report](#) commissioned by the Universal Acceptance Steering Group (UASG) found that online spending from new IDN users could start at USD 6.2 billion per year. This number is conservative and is specific to the millions of NEW internet users who could come online thanks to IDNs.

The UASG’s mission is to help software developers and website owners keep pace with the evolving Domain Name System (DNS) – and this includes issues around the adoption and acceptance of IDNs. The UASG has a range of [documentation](#) available toward that end. If you’d like to get involved in helping work toward a solution to this and other IDN-related issues, please visit <https://uasg.tech/> or [get in touch](#) to learn more.

¹ Exceptions are practiced for languages with established orthographies and conventions that require the commingled use of multiple scripts, e.g. the Japanese writing system.

IDNs: <https://www.icann.org/resources/pages/idn-2012-02-25-en>

APWG Phishing Report: http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2H_2014.pdf

UASG White Paper: <https://uasg.tech/whitepaper/>