[Internationalized Domain Names](https://www.icann.org/resources/pages/idn-2012-02-25-en%22%20%5Ct%20%22_blank) (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.

There has been a renewed focus over the past week with security articles telling of a script-mixing technique that phishing scammers could potentially use to trick Internet users into visiting malicious websites.

This particular 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 “а” and the [ASCII](https://en.wikipedia.org/wiki/ASCII%22%20%5Ct%20%22_blank) “a” look virtually identical, but are in fact different letters. When letters are combined to visually appear in the location bar of the browser identical to another website, such as someone seeking to divert visitors from MERGE.show to ΜERGE.show (actually xn--erge-knd.show). Visually, these appear to be the same, but they are different websites.

This technique is known as a homograph attack, and we will explain a little bit more about how that works and what it is later in the article. First, let us help with some context on scaling the level of concern one might want to have about this issue when considering supporting IDN (with all the benefits of global reach and audience that might come with it).

These articles are drawing attention homograph attacks are elevating attention to something that is not a new security issue, but rather an existing and well known matter that has existing precautions that are in place and constantly evolving over the course of years.

The other important thing to know, which is not always included in the articles, is that years of efforts and solutions have constantly reduced the likelihood of an attack happening, which was very low to begin with, and after years of measurement, statistically the technique measures extremely low, where it even appears.

According to the Anti-Phishing Working Group (APWG.ORG) surveys in 2010 and 2013, the incidences of IDN were as follows (from over 100M domains registered globally):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Period | Total Malicious Names (TMN) | # IDN | % IDN | # Homographs (H) | %H/IDN | %H/TMN |
| 2H2010 | 42,624 | 10 | 0.0235% | 1 | 10% | 0.0023% |
| 1H2013 | 53,685 | 78 | 0.1453% | 3 | 0.0385% | 0.0056% |
| 2H2013 | 82,163 | 82 | 0.0998% | 0 | 0.0000% | 0.0000% |

https://www.apwg.org/reports/APWG\_GlobalPhishingSurvey\_2H2010.pdf

Only 10 of the 42,624 domain names we studied were IDNs, and only one was a homographic attack.

[https://docs.apwg.org/reports/APWG\_GlobalPhishingSurvey\_1H2013.pdf](https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf%22%20%5Ct%20%22_blank)

Seventy-eight of the 53,685 domain names were internationalized domain names (IDNs), and three of them were homographic attacks.

[https://docs.apwg.org/reports/APWG\_GlobalPhishingSurvey\_2H2013.pdf](https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf%22%20%5Ct%20%22_blank)

Eighty-two of the 82,163 domain names were internationalized domain names (IDNs), and none were homographic attacks.

Homographic phishing efforts associated with IDNs are not new. In fact, they date back to the early 2000s. Registries have since implemented policies that preclude mixing scripts[[1]](https://mail.google.com/mail/u/0/%22%20%5Cl%20%22m_2952204634411187622__ftn1%22%20%5Co%20%22)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, certificate authorities, developers and browsers are constantly working in proactive manners to mitigate potential threats, and there are already certain browser-set protections in place, that work in harmony with registry IDN policies in TLDs.

Strong headlines make news articles more attractive to potential readerships, and often overstate or magnify an issue beyond a typical scenario in order to call attention to a matter. Statistically In the meantime, Internet users should practice the same basic security hygiene that is always recommended: avoid clicking suspicious links, and use a good password manager that will only enter login credentials on trusted sites.

Equally important is 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](https://uasg.tech/whitepaper/%22%20%5Ct%20%22_blank)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.

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. 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](https://uasg.tech/contact/) to learn more.