Title A: What is the IDN Homograph Attack and How Can You Protect Users Against It

Subtitle: Domain spoofing is a common and surprisingly easy way to impersonate a secure site.

Title B: Protect Your Users Against the Danger of Domain Spoofing

Subtitle: It is surprisingly easy for cybercriminals to forge well-known domain names.

Title C: Domain Name Forgery is Alive and Well – Find Out How to Protect Yourself

Subtitle: Cybercriminals have begun to forge domain names to trick unsuspecting users.

https://unsplash.com/photos/FFgcWvplwsc

Click here and take a look at your browser's address bar.

Most modern browsers will display "Apple.com" in the address bar, but it's obvious that this isn't the *real* Apple.com. This particular example is already famous, but what happens when a cybercriminal uses the same approach to trick you into sending sensitive data, such as your log-in and password credentials to a secure web platform?

This is the danger of what cybersecurity specialists call the IDN Homograph Attack. It is especially common in email phishing campaigns because email users tend to click the embedded links in emails instead of writing out URLs in their browser search bars – it's a very natural thing to do, and people rarely think twice about it.

These forged websites can be made to look exactly like their target website, and even get SSL certification! It is very difficult to protect users from IDN homographs. Broad strategies don't work – you need a customized list of IDNs generated for each email user and a powerful system for catching homographs in real-time.

We offer customized services for protecting against homograph attacks. Nonetheless, understanding how IDN homographs work is key to protecting yourself and others from being exploited by clever cybercriminals.

What is an IDN homograph and how does it work

IDN stands for *Internationalized Domain Name*, which broadly refers to domain names written in languages other than English.

Since the Internet was invented in the United States and the World Wide Web was invented in Great Britain, it makes sense that the network addressing systems used by Sir Tim Berners-Lee, Vint Cerf, and Bob Kahn were written in the English language.

The obvious limitations of a global digital communication system that only supports a single language became clear pretty quickly. People countries that don't use the Latin alphabet had no means of representing their respective languages in the domain name system.

The Internet's early architects knew this and began working on a solution. After a lengthy and, sometimes, culturally tone-deaf development effort, undertaken mostly by American engineers who did not always understand the languages they were attempting to develop support for, Punycode was born.

The problem here is that some languages use characters that look exactly the same as characters in the Latin alphabet. The Russian language, for instance, uses the Cyrillic character " **ʐ** " to describe the sound English-speakers associate with the letter "N."

The Cyrillic "ʐ" and the Latin "H" are *homographs* of one another. Web browsers, designed for multi-lingual support, show both characters as written.

So, a cybercriminal can register a counterfeit website that *looks* exactly like a legitimate website by replacing one or more letters with a homograph. There is nothing that prevents such a website from receiving SSL certification, so users who click on links to arrive at that site have no way of knowing whether it is the legitimate website or not.

In most cases, cybercriminals use these fraudulent websites for email phishing. But that is not the only use for this attack vector. Fraudulent websites made by using homographs can be used for:

- Unwanted advertising and malvertising
- Hosting exploit kits or malicious mobile apps
- Websites designed to create botnets for illicitly mining Bitcoin

Any one of these malicious purposes can easily become an existential threat to your business. The key is to protect yourself against domain name forgery – but how?

Who can protect you against IDN spoofing

At first glance, it might seem like ICANN, the organization that coordinates domain name registration on the Internet, should be able to implement some kind of solution to this problem. In reality, beyond a 2005 announcement and request for public comment, the organization's hands have been tied on the matter.

Browser developers at Apple, Google, Opera, and Mozilla are in a similar position. Limiting the accessibility of foreign character sets *implicitly* makes their products more difficult for non-English-speaking users – they just can't do it without excluding hundreds of millions of potential customers.

https://pixabay.com/en/dictionary-languages-learning-2317654/

To be fair, most browsers do attempt to protect users against IDN homographs, but they don't always do so automatically. In Firefox, for instance, you have to manually enable protection by accessing browser configuration code – something that non-technical users are unlikely to feel comfortable doing.

This puts the responsibility squarely on users' shoulders. It also means that IDN homograph attacks are likely to continue unabated or even increase in frequency, especially when email is used as a vector.

Fortunately, an email security vendor like DuoCircle can mitigate the threat of domain name spoofing. Since there is no elegant solution to the IDN problem, we go about it the hard way.

How to protect users against domain spoofing

The peculiar set of circumstances that led to IDN homographs becoming a tool for cybercriminals make preventing homograph attacks difficult. Many email security vendors apply broad phishing protection that includes well-known homograph-based website forgeries, but no comprehensive solution to preventing new homograph attacks.

https://pixabay.com/en/hacker-hacking-cyber-security-hack-1944688/

One user-oriented solution is to compel users to use bookmarks or manually type in URLs when connecting to websites. The problem with this approach is that some users will still click on links embedded in email messages simply because it saves a few seconds of time – and cybersecurity vulnerabilities only have to be exploited *once* to cause trouble.

Our solution is designed to prevent business email compromises, a $5 billion industry that often relies on homograph attacks to impersonate trustworthy websites and pilfer victim's bank accounts.

What we do is simple. We create a customized list of IDNs for each of our customers on an individual basis. We obtain these IDNs using our customers' actual domain names so that we can catch any cybercriminal attempting to counterfeit a domain name associated with one of our customers.

By creating a customized list of potential IDNs, we can catch suspicious behavior before our customers give up sensitive information or download malware. We do this for every one of our customers, regularly curating the list so that domain name forgeries don't go undiscovered.

Sources:

https://securityledger.com/2017/05/fbi-business-email-compromise-is-a-5-billion-industry/

https://www.forbes.com/sites/leemathews/2017/04/17/chrome-and-firefox-adding-protection-against-this-nasty-phishing-trick/#510db3622823

https://blog.newskysecurity.com/fake-adobe-website-delivers-betabot-4114d1775a18

https://www.icann.org/news/announcement-2005-02-23-en

https://www.livescience.com/20727-internet-history.html

https://www.dynadot.com/community/help/question/what-is-punycode

https://webfoundation.org/about/vision/history-of-the-web/