As internet 'spoofing' gets better, you may surf into a sea of sharks

August 20 2018, by Tim Johnson, Mcclatchy Washington Bureau

Credit: CC0 Public Domain

It's easier than ever to get waylaid on the internet, diverted to dangerous territory where scam artists await with traps baited for the unsuspecting user.

It's all about devious misdirection, fumble-fingered typing and how our brains can confuse what our eyes see. Big money can await the clever scamster, and costs are rising for corporations and politicians who do not take heed.

The problems lie in the inner workings of the internet, and touches on issues like the vast expansion of the combination of words, dots and symbols that comprise internet addresses.

It's no longer just .com, .net., .org and a handful of others. Now, there are 1,900 new extensions, known as top-level domains, things like .beer, .camera, .city, .dating, .party and .shop.

"We see a ton of them being used maliciously," said Mikko Hypponen, chief research officer at Finnish security company F-Secure, who called the new endings "a big headache."

The problems revolve around what computer scientists refer to as "spoofing" of the Domain Name System, or DNS, which has been called the phone book of the internet. It's been going on for a while, and touches on what users type into the address bar of a browser window or click on at a website. There are new ways to make phony addresses look real.

"Creating a spoofed domain name, or even hijacking a domain name, has become a lot easier today," said Israel Barak, chief information security officer at Cybereason, a cyber security firm based in Boston.

Just a few years ago, spoofing an internet address, say, microsoft.com, was primitive.

"You would have to maybe change that 'i' to a 1. I'm going to be M1crosoft with a 1 today, or even change the 'o' to a zero, or change the 't' to a seven. For senior citizens with fuzzy vision like I'm starting to get, you might squint at that and say, 'Looks like Microsoft to me,'" said Paul Vixie, chief executive of Farsight Security, a San Mateo, Calif., company.

An internet pioneer, Vixie has been involved in its governance for three decades. He is an architect of some of the protocols used in the DNS system and advises the non-profit Internet Corporation for Assigned Names and Numbers, the Los Angeles non-profit that serves as the guardrails for the borderless global internet.

But Vixie said the internet is still in its Wild West phase. He compared the online world today to the era of highways before seatbelts and airbags.

"It just takes us some time to catch up. First, you innovate, you kill a lot of people or steal a lot of money, whatever it is, and then somebody comes along and says we got to secure this somehow. We're still in that first phase here," Vixie said.

To bridge the gap between English-speaking and non-English-speaking worlds, internet organizers have incorporated domain names utilizing characters covering 139 modern and historic scripts. It's not just major scripts like the Cyrillic alphabet and Chinese characters. It's also Runic, Buhid, Rejang and dozens of other obscure language scripts.

Scamsters have had a field day with parts of those scripts. They've inserted look-alike characters into internet addresses, sending users to bogus malicious, websites.

Vixie said numerous distinct characters look like the Roman letter "i."

"They are completely visually the same down to the last pixel on your screen to the real lower-case 'i.' So there is no way that you're going to tell the difference," he said.

Inserting such exotic characters into a link is one technique criminals employ to send users to look-alike sites that may appear to be a bank

website, a Gmail troubleshooting page or some other page that asks for a username and password. Other techniques are also used.

In some cases, adversaries target employees of a corporation, nuclear plant, military unit or other high-value facility where they seek a digital foothold. The hackers send the targets tailored emails with the malicious links.

"It's easy(and) it's cheap," said Tom Richards, co-founder and chief strategy officer for GroupSense, a Virginia cyber threat intelligence firm.

As a hacker, Richards said, "All I need to do is register a website that looks like my target and then send that to a handful of employees or people affiliated with the organization or potentially even customers. And then I can trap them. I can send them malware. I can get them to fill out a form.

"It's embarrassingly effective."

Not so long ago, companies would buy common domain names that were almost like their normal websites, but off by a letter to ensure clumsy typists wouldn't go astray. So, in the case of Walgreens.com, if you type in walgreen.com or walgrens.com it will still take you to the drugstore chain's site.

With the proliferation of new domain names, the task has grown more difficult.

"It is getting harder and harder for companies. There are just so many combinations," said Steve Manzuik, director of security research at Duo Security, an Ann Arbor, Mich., vendor of cloud-based security services.

Some cybersecurity experts suggest that average internet users need to get savvier about phony websites, reading the components of what is in the address bar, like domain names and suffix paths. Others say that expects too much of average internet users.

Most users see "dots and slashes and question marks. They don't know what this means," said Rich Smith, director of Duo Labs, the advanced security research team at Duo.

As election season approaches, some politicians are taking special care to ensure variants of their website addresses aren't snatched up and registered by foes. Other politicians are less aggressive. At a recent talk at the DefCon hacker convention, a father-son election research team, Kevin and Joshua Franklin, cited two websites that troll incumbent politicians.

One targets Rep. Devin Nunes, the California Republican who chairs the House intelligence committee and is a sharp critic of special counsel Robert Mueller's probe into Russian efforts to interfere in the 2016 election. Users who click on a website with an address similar to his re-election site arrive at a website partly in Russian with a photo of Nunes in a Stalinesque pose.

At least one congressional candidate, Republican Pete Stauber of Minnesota, has prepared well, registering 37 domain names that are variants to ensure an opponent doesn't troll him., Joshua Franklin said. Stauber's campaign didn't respond to a message seeking comment.