Time to Double Check the Website Addresses You're Visiting

Starting tomorrow, the Internet Corporation for Assigned Names and Numbers (ICANN) will start allowing companies to register for new top level domain names. Examples of current top level domains include .com, .net, .edu and .org. The new registrations are designed to allow companies to register virtually any string of characters as a top level domain. So, for instance, General Motors might want to register .cars and .gm domains. Unfortunately, the new registrations are also likely to give scam artists and criminals new opportunities to defraud consumers. The new ICANN plan means that consumers will need to be a lot more vigilant when typing in an internet address.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Under the domain registration scheme, it is highly unlikely that your recently laid off next door neighbor will register a new top level domain and turn to a life of crime to support himself. The application fee for a top level domain will be $185,000. The fee alone will exclude most petty criminals.

But there are a number of criminal rings on the internet that are multimillion dollar enterprises in their own right. There are also a number of governments around the world that are less than friendly to American interests. These entities have the money and resources to invest in domain names, and there is no reason to think that they won't.

The registration scheme will make it easy for criminals and other organizations to register domains that are commonly fat fingered when typing. Things like .ccm or .nrt - both one letter off from a legitimate top level domain - are good examples.

Let's say that someone registers one of these names and then sets up websites that look the sites of every major bank on the internet. A small but consistent number of people will be bound to type in the wrong extension and get to a site

that they believe belongs to their bank. They'll go through the motions of logging into their account. In the process they'll give the crooks all of the information they need to access all of their money. When their logon fails, they'll be kicked out, back to the real bank's home page, never realizing that all of their account information has been compromised. This is just one example.

New, look-alike websites can be used to install Trojan horses and viruses on computers. They can be used to drain bank accounts and steal identities. They can be used for a lot of bad things. And because the public is so used to the internet working in a specific way, it is going to take some time before everyone gets used to the new system and the pitfalls it brings.

Consumers need to make sure that their antivirus software is up to date and to pay close attention when they type in internet addresses. Even this is no guarantee that you won't become a victim of fraud, but it will help.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS