New Phishing Trick That's Almost "Impossible to Spot"

Phishing provides a direct line to identify theft -- by fooling victims into giving away their account sign-on details.

Now, crooks have found new ways to conceal the fake websites they use to steal that information.

Spoofing well-known websites is among the favourite phishing tricks scammers use to steal sign-on information.

They use links in emails to lure victims to websites that look almost identical to the genuine version and then invite them to enter their username and password.

They also rely on people mistyping the name of a site they want to visit, perhaps getting just one letter wrong, ending up on a cloned site, which again seeks sign-on information.

Please check the address line in your web browser to be sure you're at the right place but you can't always be sure the address line is giving you the confirmation or information you're looking for.

A clever trick, recently demonstrated by security experts, exploits the fact that there are all sorts of unusual characters available on a computer -- in addition to the 1 -9 or A - Z and a handful of symbols you'll find on your keyboard.

For instance, the letter "o" is used in some other languages with dots, squiggles, accents and other marks above it.

In fact, there are even different versions of the letter "o" -- for different alphabets like Greek or Cyrillic -- which look identical to each other on screen but are treated differently by web browsers.

These can be used to create fake websites whose addresses look identical to the genuine article.

The way the trick works is a little more complicated than that but, suffice it to say, the result is a web address entry that, according to a recent article in Fortune magazine, is "virtually impossible to spot."

In fact, without a level of technical knowledge that most of us don't have, you likely wouldn't pick up on the fakery.

Security experts have reported the weakness to the makers of the most popular web browsers, but, in case they don't act fast enough, the best safety measures you can take are **not to click on web address links but instead retype them yourself** -- and to make sure your own typing is accurate.

Cell Phone Trickery

Another problem with checking a website location in a browser address bar affects everyone who uses cell phones.

When you visit a website on your cell, the screen is so small that it's sometimes you can't see the whole address, or URL, at the top of the browser, unless you take the time to scroll through it.

Phishing crooks exploit this using a trick known as URL padding.

The scammers add a number of hyphens to a legitimate web address so you never get to see the full fake version.

For example, they might set up a fake site for Scambusters That looks like this: www.essex.police.uk----------phonysite.com.

All you'd see is the first part and maybe a few hyphens but not the "phonysite.com" bit, which is the real website address.

Of course, you don't have to sign on at Scambusters, but security experts have shown how URL padding is being used to trick people into believing they've visited a genuine Facebook page where their sign-on details are requested.

One of the problems is that, unlike with a PC, you don't have a mouse for your cell phone so you can't hover over the address bar to read out the full address. If you put your cursor in the address, it can be to try to scroll through it - another reason for being cautious about clicking on links that seem to come to you from friends on Facebook or via SMS text messages.

Warning of this trick, security researcher and tech blogger Crane Hassold explains: "The trouble with mobile devices is that even people who are normally security conscious treat them differently. As a population, we've been conditioned to check our phones constantly and to browse or follow links in a far more lackadaisical manner than we would on a desktop or laptop.

"As a result, we're generally paying far less attention to any warning signs that might crop up."

Alert of the Week

Did you fall victim to a tech support scam, allowing crooks remote access to your PC and maybe paying them a fee for supposed repairs?

If so, watch out for a call from another scammer, this time pretending he wants to return your fee but needs access to your machine and bank details again first.

It's another fake, so just hang up.

Source – Scambusters.org