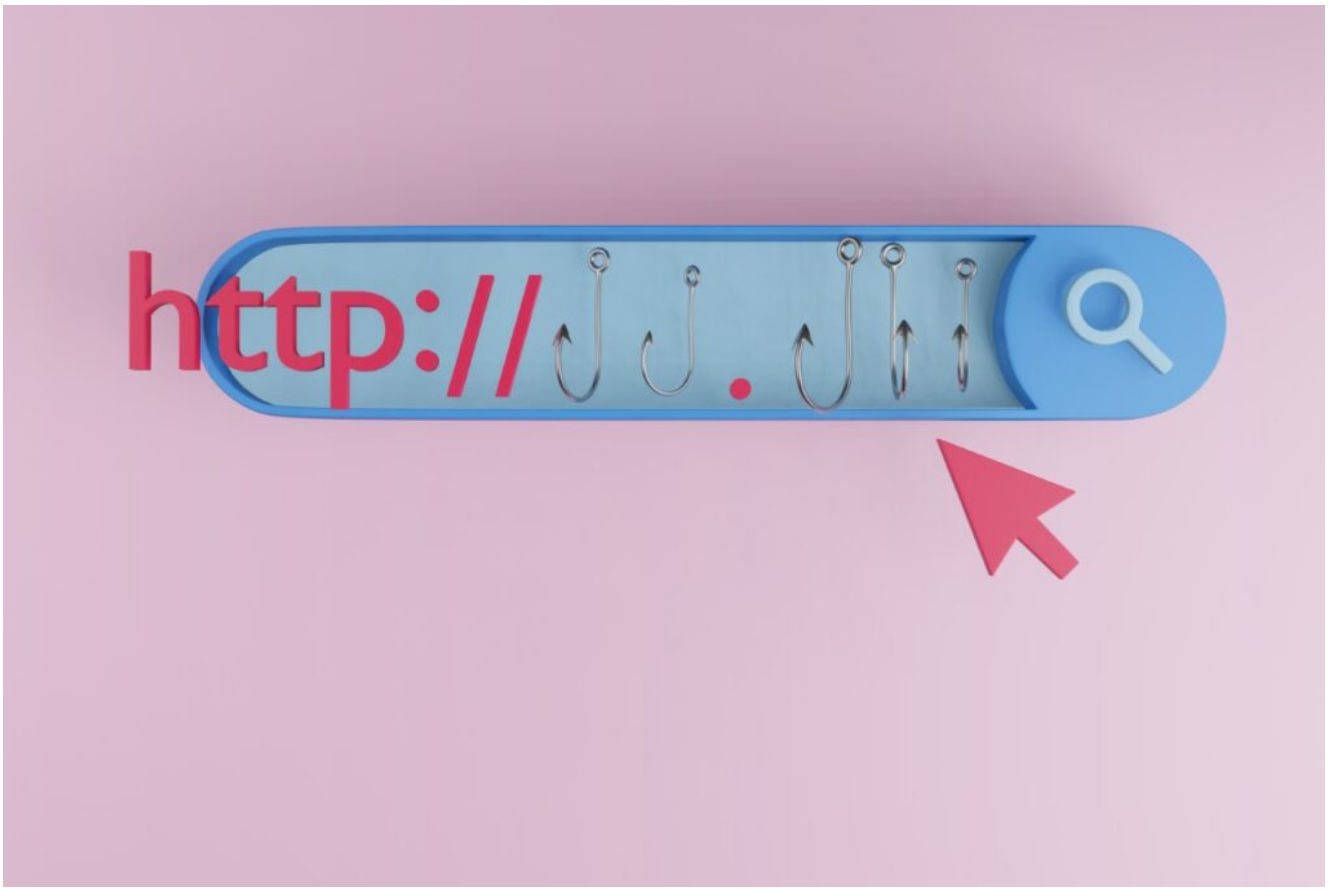
Malicious URLs

written by John Grubb | September 22, 2022

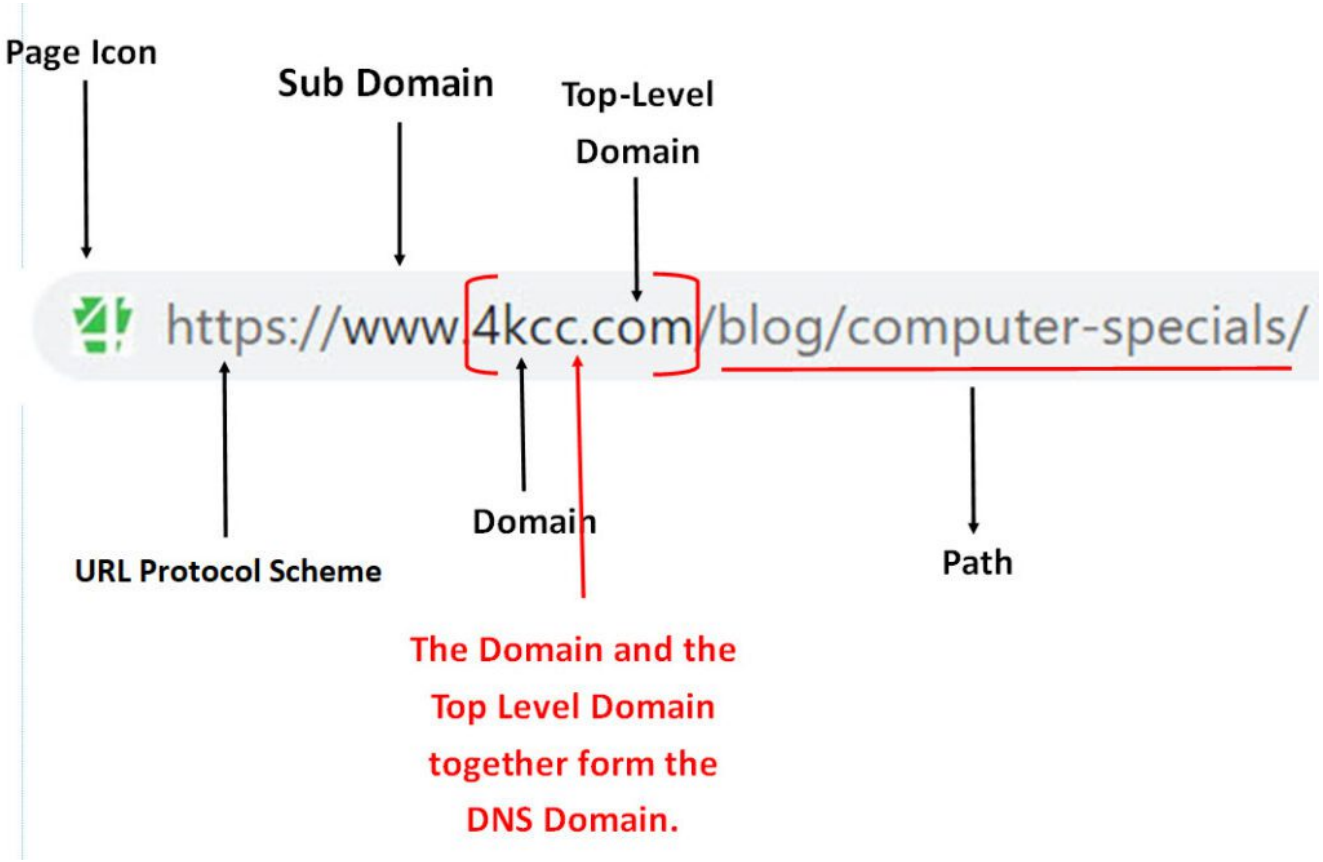


Malicious URLs are found in emails, in searches, on Social Media sites, and in texts. In this post, let’s explore ways to avoid being fooled by these hacker tricks.

What Is A URL?

Before we look at malicious URLs, we need to know the definition of the acronym URL. A Uniform Resource Locator (URL) is usually known as a web address. For instance, **https://www.4kcc.com** could be referred to as our main web address or our URL. Now that we know the basic definition, let’s look at parts of a URL.

URL Sections



There’s no need to get real technical as to the parts of a URL but you do need to know the basics. Having this information may help you avoid major issues in the future. Let’s briefly look at each part shown above.

- Page Icon – Not all pages have icons but when they do, they might help you know that you’re on the site you think you are.
- URL Protocol Scheme – For most webpages, the scheme is either https:// or http://. Still, there are other schemes like ftps:// and ftp://. (Remember, the “s” indicates a secure site.)
- Sub Domain – This section can be “www.” or it could be “support.” as in our RTS log in page: support.4kcc.com.
- Domain – In our URL, 4kcc. is our main domain.
- Top-Level Domain – This is the area of the URL that tells the Internet where to look for your domain. Top-level domains include .com, .net, .edu, .info, .org, .us, .biz and many more.

- DNS Domain – The combination of the domain and the top-level domain forms the DNS Domain. Again, I'm not going to go into depth to explain DNS in this post. We'll save that for another time.
- Path – Finally, there's the path so your browser knows what page to go to in your domain.

Malicious URLs – Tricks Used By Hackers/Scammers

Now that you know what a URL is and have a basic understanding of its makeup, let's look at some of the malicious URLs that you might come across.

Malicious URLs – Shortened URLs

Shortened URLs are used all over the web and they can be a good thing. You can find out all the benefits of these types of web addresses by reading my post, ***This Is Not A Short Joke***. However, there are malicious shortened URLs that can easily trick you because you can't read the traditional URL. With this in mind, you need to bookmark a tool that will show you where you'll really be going if you click on a shortened address. You'll find this helpful aid here: **https://expandurl.net/expand**. On this site, you can paste or type a shortened URL and it will tell you where it's really going. The great news is that you can see where you're headed without actually clicking and going there. Why not try it? Here's a shortened URL to expand: **https://tinyurl.com/4r9wrrdm**.

Misspellings

If you're like most of us, you're always in a hurry – especially when you want to find something on the Internet. You might misspell a URL when you type it in or you may click on a malicious link that has been sent in email. For instance, www.goggle.com could easily fool you. (I'm not making that

address clickable because it takes you to a phishing site. On my computer, Malwarebytes blocks me from going there but that might not be true for everyone reading this post.)

Fortunately, many companies have purchased misspelled domains and those pages re-direct you to the real domain. For instance, try clicking or tapping on this misspelled URL: **http://www.micrsoft.com/**. Still, it's important that you are careful when you type a URL and when you go to click on one in an email or a text message.

Brand Name In Email Address But Doesn't Match The Brand's Domain

Here's a perfect example of this hacking trick: If you received an email from TD Bank <TDBank@customers.account.com.> and you are a TD Bank customer, you might be fooled. Even though TD Bank is in the email address, it is NOT in the domain. If you replied to this email, you would not be sending anything to TD bank but, instead, you'd be communicating with the scammer.

Malicious URLs – The Wrong Domain And/Or Top-Domain

This is a trick hackers love to use after they've hacked someone's email account. However, it can be used as a web address aimed at fooling you, too. How does it work? Simply put, a scammer will take a legitimate email or web address and change the domain or the top-domain. For example, you are used to seeing my email address which ends in @4kcc.com. A scammer might take that and change it to @4kcc.info. Or if they were using my personal email address which ends in @gmail.com they might substitute the end to @yahoo.com. If you were hurried, you might click on or reply to the Yahoo address without realizing it's not me.

There Are More

There are more Malicious URL tricks that hackers use and I’ll expand on them in a future post. For now, though, I think I’ve given you more than enough to consider. Always take a breath and think before you click or tap.