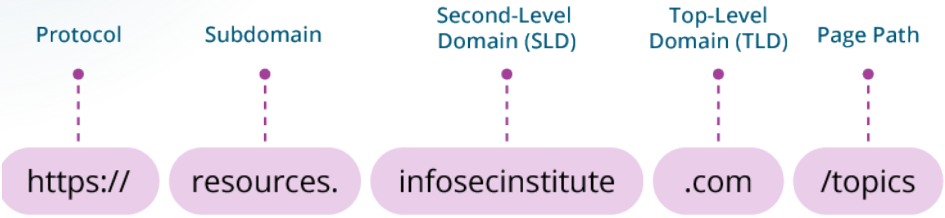
NEED TO KNOW NEWSLETTER | JUNE 2023

Zip, zap, don't click on that!

New top-level domains are causing chaos, but we're here to keep you informed and safe while browsing the web

Parts of a URL



Protocol

Knowing a few important parts of the URL will help you stay safe. First, the Protocol is where you will see https:// or http://. The HyperText Transfer Protocol (HTTP) requests the contents of the website and allows you to see it on your end. Make sure your connections use HTTPS — the 'S' stands for secure. HTTPS encrypts your browser connection, making it more difficult for hackers to steal your data. HTTPS connections can be identified by the lock icon next to the URL.

Top-Level Domain (TLD)

When you type in a website address, the last part you enter is called the top-level domain. It's the part after the dot. Like .com, .org and .net. There are even country-specific domains, like .uk and .au. In fact, there are over a thousand top-level domains currently in use.

Recently, Google released several new top-level domains to the public. They include some fun ones like .phd, and even .dad for fathers who want to start a blog. Seriously, that's the description!

Links and attachments in email

But two new domains are causing a lot of concern in the cybersecurity community: .mov and .zip.

.zip and .mov are common file types. With both of those now available to use as TLDs, we'll see more of them being used by hackers in phishing emails. Review these important tips about opening links and attachments in your email:

1. Always take time to investigate links and attachments in emails you receive. You can hover your mouse over the link and see where it is going to take you. If anything is suspicious, avoid that link!

2. Verify the sender. Look at who sent you the email and what domain they are sending from. This is a big giveaway to who really is the author of the email. If it looks off, it probably is!

3. Contact the sender directly in a different form or a new email. This way, if it is legitimate, you can verify it.

4. Let your IT or security team know immediately. If it's a real email, they can let you know it's safe. If it isn't, you just helped save your organization from a breach!

Use your bookmarks

Saving your most used websites to your bookmarks is both convenient and safe. When you use your saved bookmarks to head to a website, you ensure that you are actually going to a safe page and not stumbling onto a fake one.

For example: You receive an email that says you have been sent a shared file from a coworker using Google Drive or Sharepoint. There's a link. But instead of clicking on the link in the email, you use the bookmarked link to where you store data and log in that way.

Hackers send links that look real. When you put your username and password into a realistic login page, they are able to collect your credentials. Using your bookmarked pages can help you avoid the trap!

Cybersecurity roles — Digital forensics analyst

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

Digital forensics analyst

Digital forensics analysts help recover damaged or deleted data like documents, photos, emails from computer or mobile devices, hard drives and other data storage devices, such as zip folders and flash drives. They carefully follow the chain of custody rules for digital evidence and provide evidence in acceptable formats for legal proceedings. Digital forensics analysts are especially important when investigating data breaches and criminal activity.