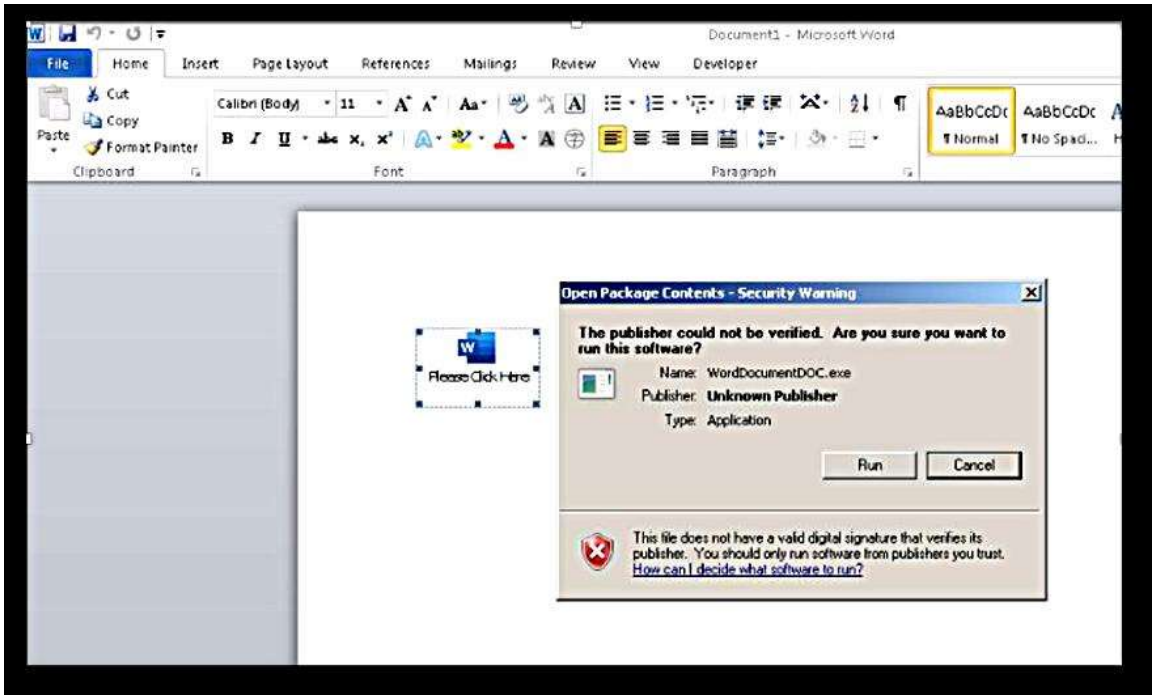
The anatomy of an address
There is more than what meets the eye

My frame was not hidden from You
When I was made in secret
And skillfully wrought in the depths of the earth;
Your eyes have seen my unformed substance;
—Psalms: 139:15-16



Source: Joseph Edwards, Senior Malware Researcher at ReversingLabs
https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

Using our existing image of a rogue MS Word attachment, when we carefully examine the filename we can clearly see that the attached file IS NOT A WORD DOC or DOCX file. NO! The rogue attachment filename ends in .EXE. Really, that's all we need to know in order to feel confident that we delete this entire email. Do not send to Recycle Bin. Hold down SHIFT & delete. Bye bye executable.

Any filename that ends in EXE is an installer of some kind. Of course, everyone knows this. Unless you have downloaded a specific application file, never ever click on an EXE file. But here, in June 2022, we have malware spreading by dimwitted so and so's who do not have a grasp of this very basic computer information.

A large part of taking responsibility for your own security online is to become familiar with exactly what does a Uniform Resource Locator (URL) tell you upon reading the URL. Let's use this exact page you reading right now as a good example for how to read a web address or URL.

The complete URL to this page is:
http://www.eppresents.com/Newsletter-Jul07-2022/address-anatomy.html.

The first important piece information conveyed here is that the address begins with **"HTTP:" hypertext transport protocol.** That tells us that this is an address to a page somewhere on the Internet.

Next comes what may be the most important information conveyed by the URL. The domain name this page points to is **eppresents.com**. This is critical information because if the URL said eppresents.net; or eppresents.org; or eppresents.biz; those possible URLs would not point you to this website. In fact, if you received some communication about the Dispatches From the Front, and the communication pointed to eppresents.net, for instance, then you would immediately know that communication was fake. The Dispatches are only live at eppresents.com. This is known in the trade as the **root domain of the website**, or the Top Domain.

Similar to the folder/filename scheme of Windows and all other OS's, we use folder names when building websites to organize the pages (files) into groups. Considering the Dispatches have been back in production now for close to a year (judicious editing has been done), imagine the organizational nightmare this project would become without subdivision by folders. Moving along the sample URL after the top domain, we have a subfolder named **Newsletter-Jul07-2022.** Now it is important to look closely at subfolders. If the subfolder name **is not followed immediately by a slash (/)**, but **instead by a DOT (.)** and then anything else, that part of the path does not indicate a folder, but a file of some kind.

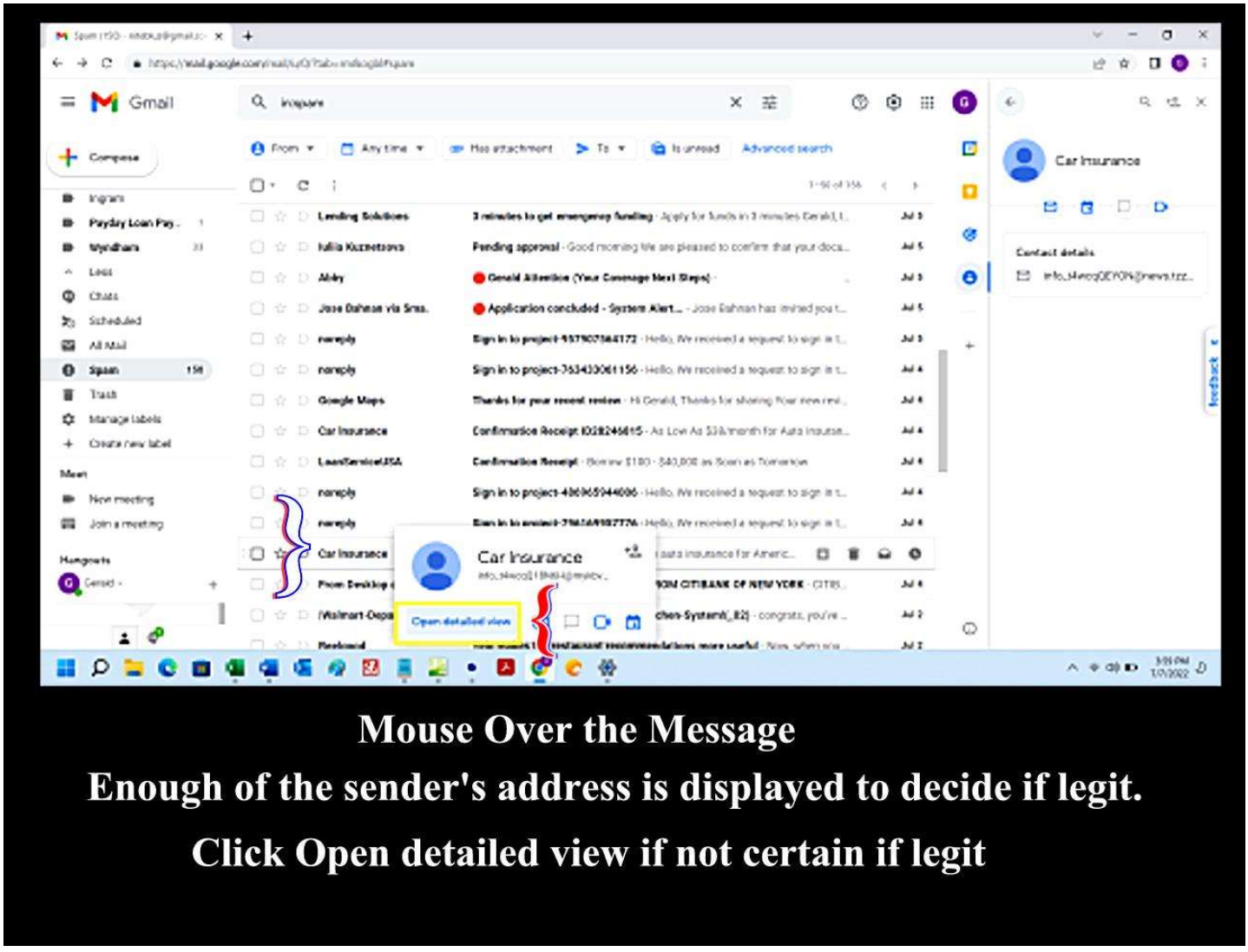
The last entry in our sample URL DOES INDICATE that a file will open at this location. That filename is **address-anatomy.html. HyperText Markup Language (HTML) is the coding language of the Internet.** Modern browsers are made to intrepret HTML and display objects it can create. If the full URL path does not end in ".html" or ".htm" then any such URL most likely does not point to a webpage.

The exception to this HTML standard are sites generated with PHP or WordPress. Any such extension that clearly defines the type of file the URL may not be present, but the page may nonetheless be an otherwise legitimate webpage. It is no wonder to me that **WordPress generated sites are often the most vulnerable, and thus hacked and reversed engineered to spread malware. — Just saying.**

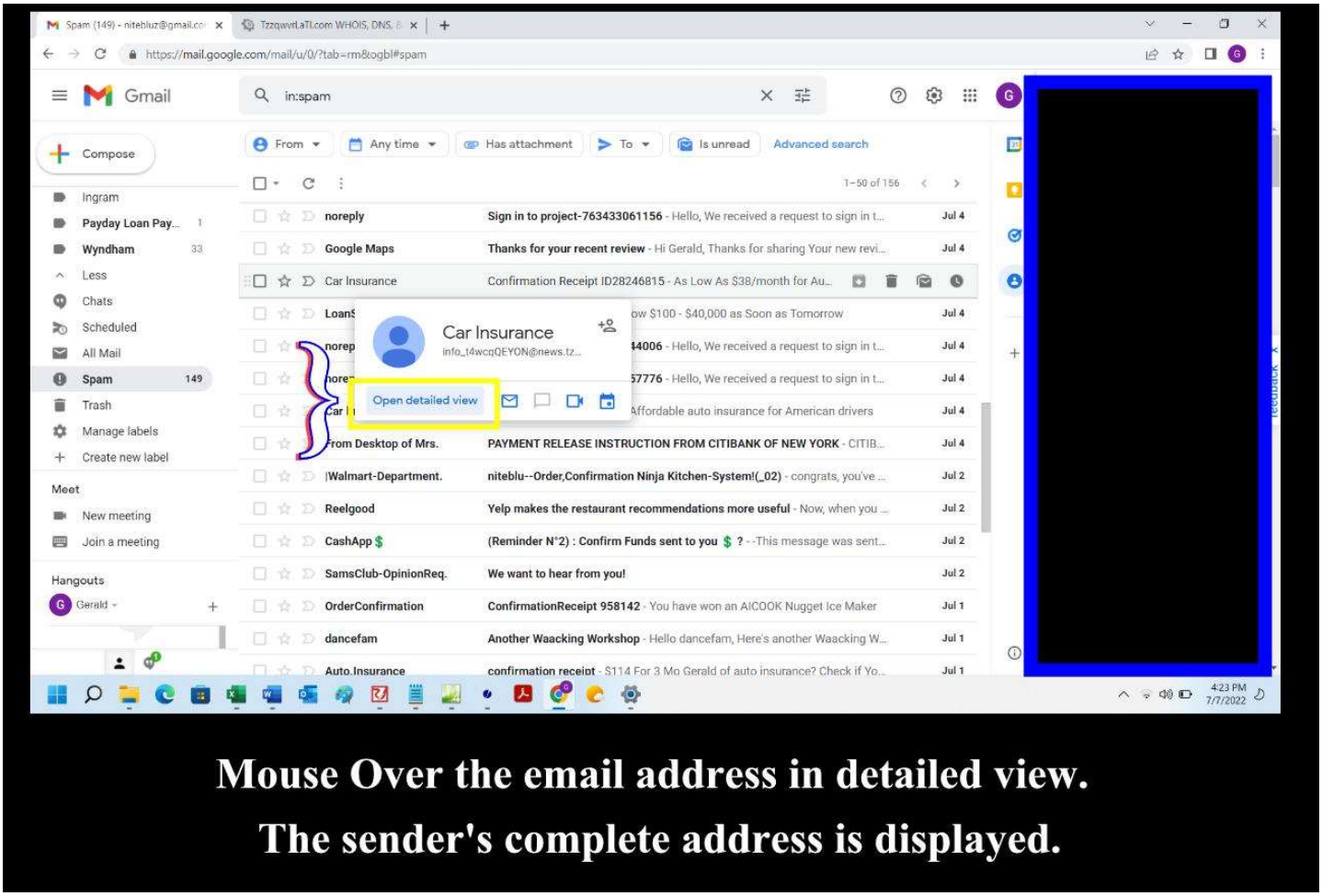
Another exception to the standards of HTML pathnames are truncated links you will often see in smishing SMS text messages. Yes, some people do use URL truncating to positive effect, but I say: Why take the risks? As a general rule, we usually know where we intend to go before we put the car in drive. Knowing the complete story of where our hyperlinks want to take us should be a big part of your own personal online security protocol.

All this becomes even more critical when examining an email sender's actual address. Spamming might seem like a fool's errand these days, but there still seems to be more spam than ever. I am going to use my Gmail account as an example of how to determine if a sender is legit by examining the sender's address.

When we look in the Spam folder of the Gmail account, we can find many possible examples. I will pick car insurance spam. When we mouse over the Sender "Car Insurance," we see a very suspicious sender's email address. When we mouse over the sender's address we can clearly see the sender's full email address is even more suspicious.



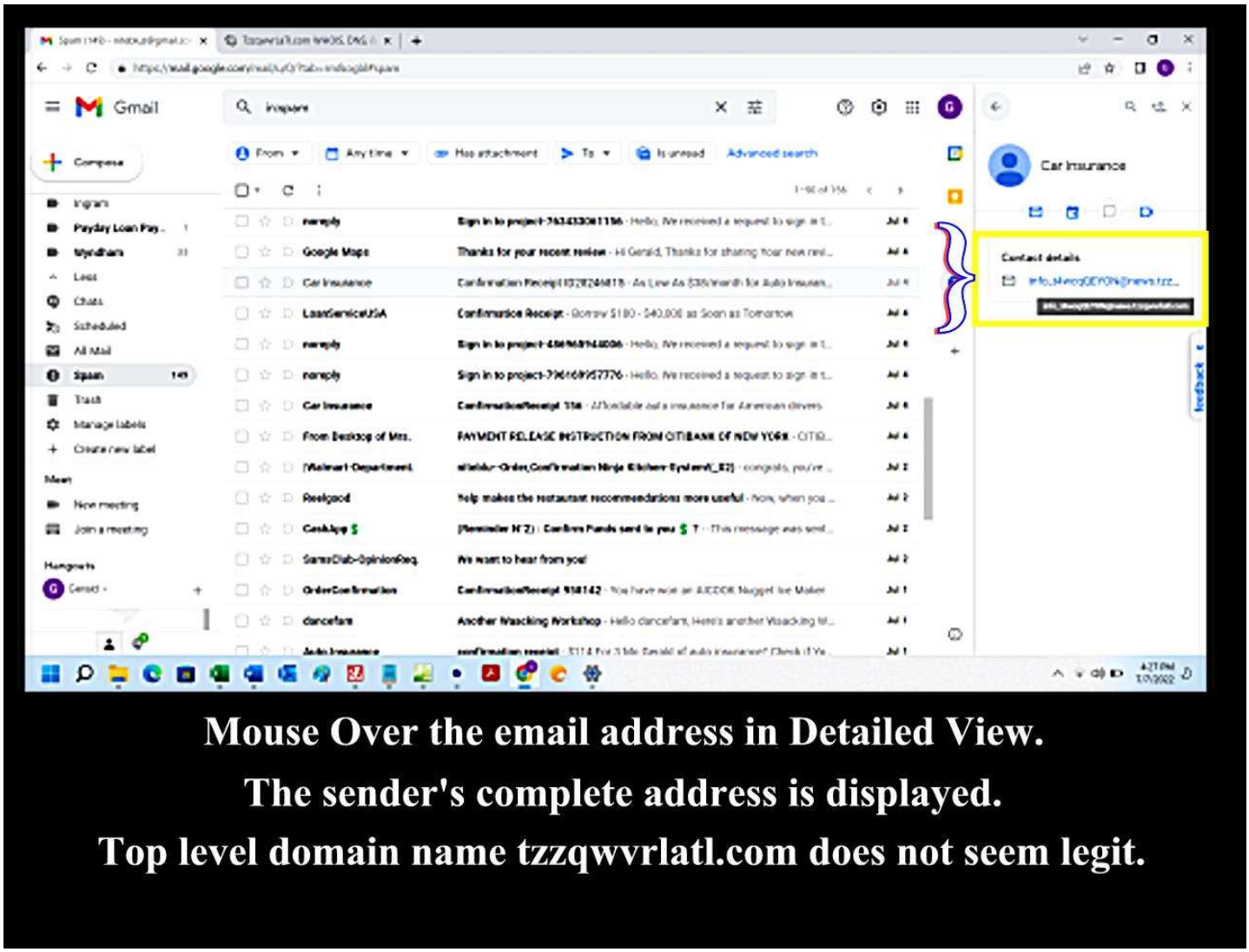
To further examine the sender's address, we click "Open detailed view" to get a clear reading of the sender's address.



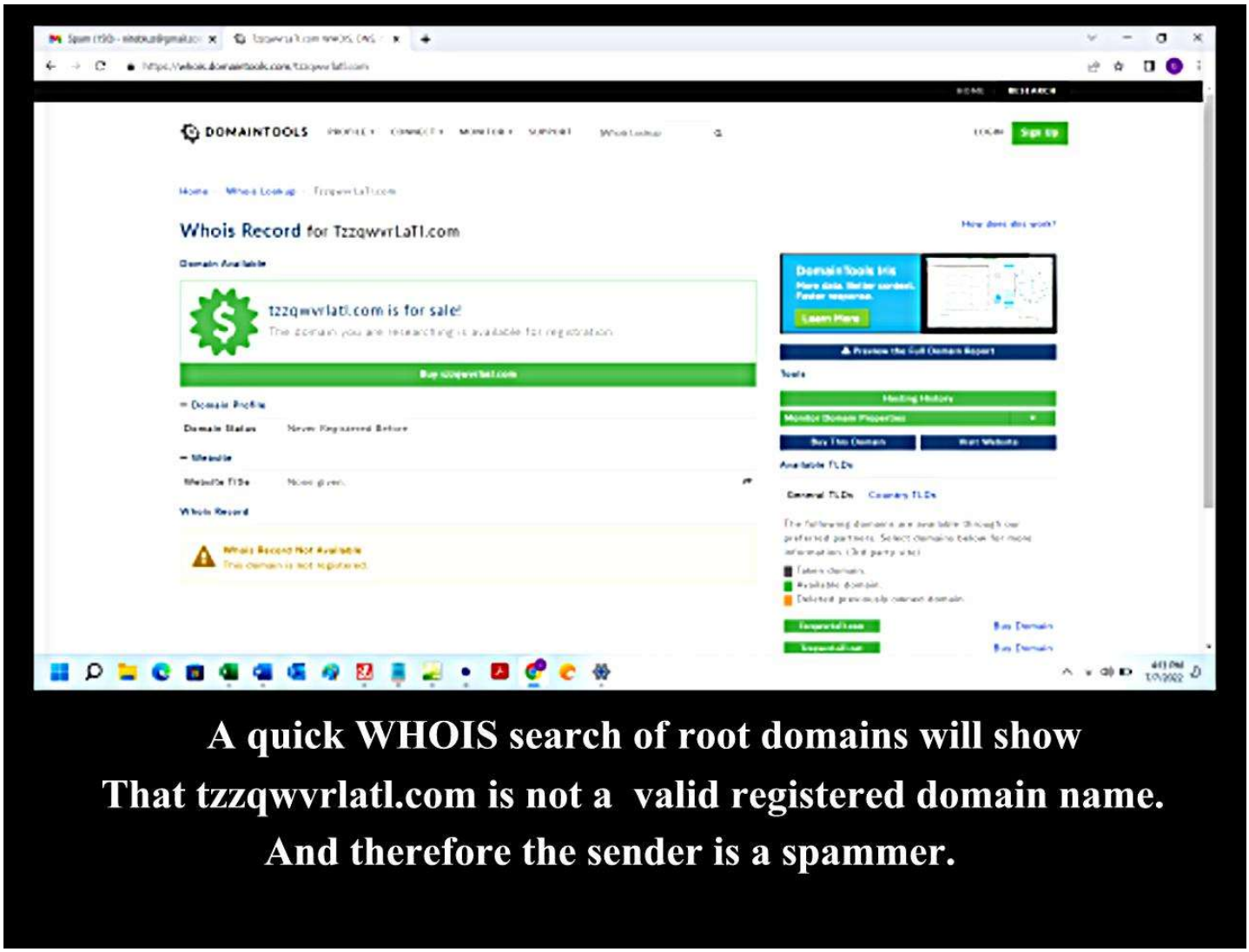
Mouse Over the email address in detailed view.

The sender's complete address is displayed.

In Detailed View we can mouse over the email address and see the complete address for the sender.
Clearly "tzzqwvrlatl.com" is not a legit top level domain name.



In fact, a domain name WHOIS search reveals that tzzqwvrlatl.com is not a registered domain name. It is most likely a spoof of the spammer's actual email address. The message, however, is certainly spam and should be **<SHIFT> <DELETE> to bypass the Recycle Bin.**



Jerry Seinfeld : But are you still "Master of your Domain?"
George Costanza : I am king of the county. You?
Jerry Seinfeld : Lord of the Manor.
— Seinfeld, "The Contest" (Season 4 Episode 11)

Back to Top

next post →