Fake websites are rampant, what must browsers do?

According to some media reports, during the recent May Day holiday, the United States Postal Service (USPS) fake phishing website was visited as much or even more than the official website, and the fake USPS website is designed to steal people's sensitive information and payment data through phishing. A new report from cybersecurity research company Akamai Technologies warns consumers to be skeptical when shopping online and always keep in mind to beware of fraud.

1. Browsers must do something to stop the proliferation of fake and fraudulent websites.

To effectively prevent fake websites from harming users, it is not enough to warn consumers to pay attention, and browsers for users' internet access should do something useful to prevent users from being deceived. The key to this problem is that browsers do not display the trusted identity of the website, and they cannot clearly distinguish between authentic websites and fake websites. When users use Google Chrome and Microsoft Edge browsers to visit the authentic USPS website and the fake UPPS website, they will display the same page, and it is impossible to distinguish between the authentic website and the fake website.

Only reminding users to see the domain name of the website clearly is a useless reminder, because the domain name of the fake website must be a very similar domain name, and it is impossible for users to distinguish which domain name is an authentic domain name, and even users do not understand what a domain name is. It's no wonder that fake websites have the same traffic as authentic websites, which is equivalent to up to 50% of users visiting fake websites without being able to identify them. This is very worthy of reflection by browsers, should browsers do something to prevent the proliferation of fake websites? Are there any browsers on the market that have improved in this regard?

2. **ZT Browser displays the organization name in the green address bar, which correctly identifies authentic websites and fake websites.**

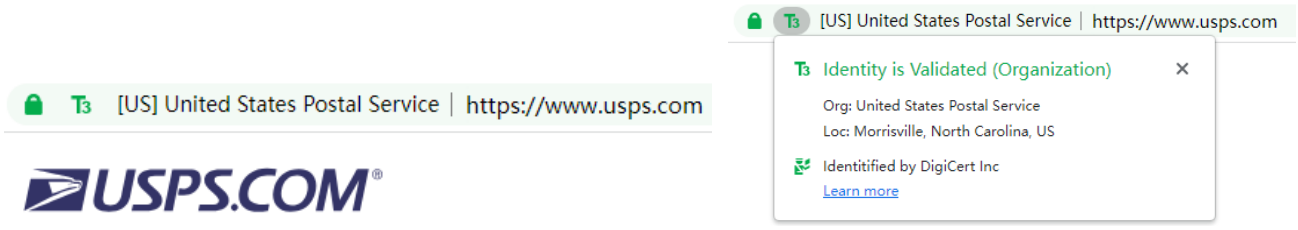
Please use ZT Browser to visit the official website of the United States Postal Service (USPS), and the green address bar displays "United States Postal Service". Even if the webpage of any fake USPS website is exactly the same page design, ZT Browser's address bar cannot display "United States Postal Service", nor can it be a green address bar. ZT Browser displays the authentic USPS website not only in the green address bar, but also the user can click on the T4 icon, it displays the detailed identity information of this website, and also displays who identified this website's identity.

In other words, ZT Browser can accurately identify and distinguish between authentic websites and fake websites, and it can clearly tell users whether the website they are visiting is a fake website, so that users can stop visiting in time without being deceived. Only ZT Browser in the world has done it, which can efficiently, directly, and clearly prevent users from encountering fake website fraud.

3. **ZT Browser displays the trusted identity information in the OV/EV SSL certificate deployed on the website.**

The above website trusted identity information comes from the Trusted Website Identity Database of ZT Browser, which is an innovative service provided by ZT Browser - Website Trusted Identity Validation Service. If a website has not applied for this service, or ZT Browser is unable to update the Trusted Website Identity Database due to some reasons, it will get the identity information of the OV/EV SSL certificate deployed on the website. For USPS website, it deployed an OV SSL certificate, ZT Browser will display "United States Postal Service" in the light green address bar, which can also immediately identify the authentic USPS official website and can also prevent fake websites from being deceived. When the user clicks on the T3 icon, the website identity information in the SSL

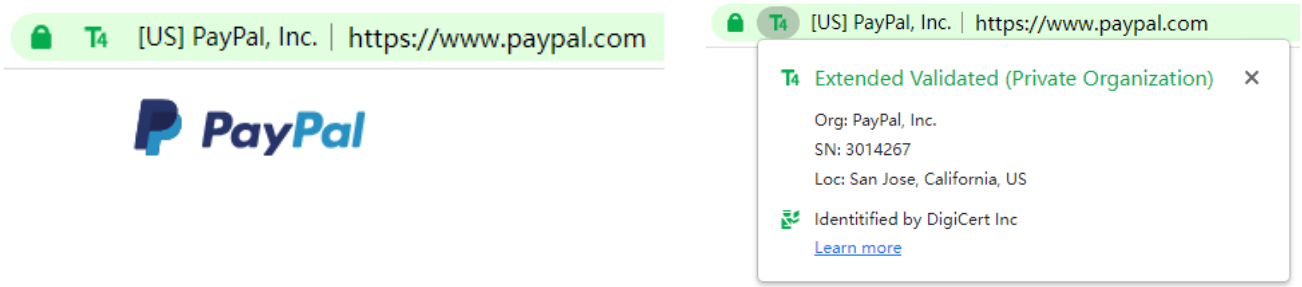
certificate is displayed, and this identity information is identified by the CA that issued this SSL certificate.



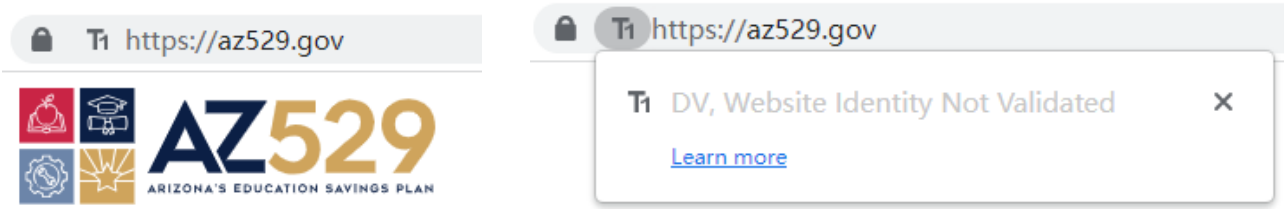
This is the important value of deploying an OV SSL certificate or EV SSL certificate for websites, and it is highly recommended that all website owners who do not want their website to be impersonated should deploy an OV SSL certificate or EV SSL certificate with identity information.

As early as 2007, CA/Browser Forum already had a solution to prevent fraudulent websites with the green address bar of EV SSL certificates, but unfortunately the four major browsers abandoned this excellent feature in 2019. To effectively help users identify fake websites, the author calls on the four major browsers to restore the green address bar of EV SSL certificates. At present, only ZT Browser in the world not only retains this excellent function, but also adds a new scheme of light green address bar for OV SSL certificate, the authentic USPS official website deploys the OV SSL certificate, and ZT Browser can directly read the certificate O field information and displays it on the light green address bar.

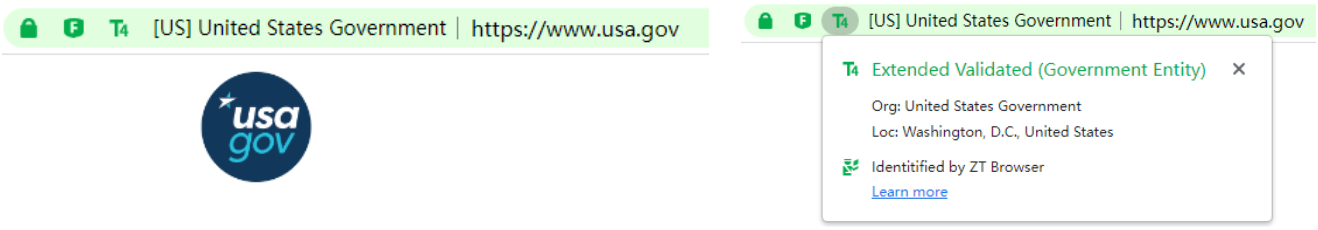
If the website is deployed with EV SSL certificate, ZT Browser will read the SSL certificate O field information and display the organization name on the green address bar, such as the most likely to be counterfeited PayPal official website is deployed EV SSL certificate, ZT Browser displays trusted identity information strictly verified by the CA in the green address bar, PayPal only needs to tell the user that the site that doesn't display green address bar is a fake site.



If the website is deployed with DV SSL certificate (including 90-day free SSL certificates), ZT Browser only displays the padlock and does not display the website identity information, because the DV SSL certificate only validates the domain name control, but it does not validate the website identity.

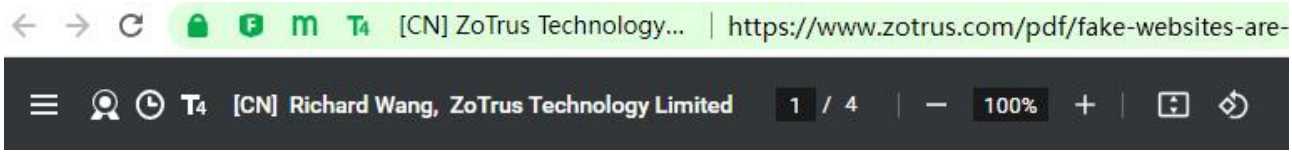


Careful readers may notice that the official website of the US government (www.usa.gov) deploys a free DV SSL certificate, why ZT Browser displays green address bar and displays "United States Government"? This is because this website identity is included in the Trusted Website Identity Database of ZT Browser, it is EV Certified that let the websites that deploy DV SSL certificates to be displayed the organization name in the green address bar as if they have deployed an EV SSL certificate. When the user clicks on the T4 icon, it will display “Identified by ZT Browser”.



4. To prevent being deceived on fake websites, use ZT Browser to surf the Internet now!

For your online security and prevent being deceived on fake and fraudulent websites, now, please use ZT Browser immediately, which uses the same Chromium open source as Google Chrome and Microsoft Edge browser, with the same excellent browsing performance, but with a different address bar to display the trusted identity of the website, and can also validate the digital signature information of PDF documents in real time and display the trusted identity of the document signer.



To prevent being deceived on fake websites, use ZT Browser to surf the Internet now! Download it now and enjoy a safe online life.

Richard Wang

May 13, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.