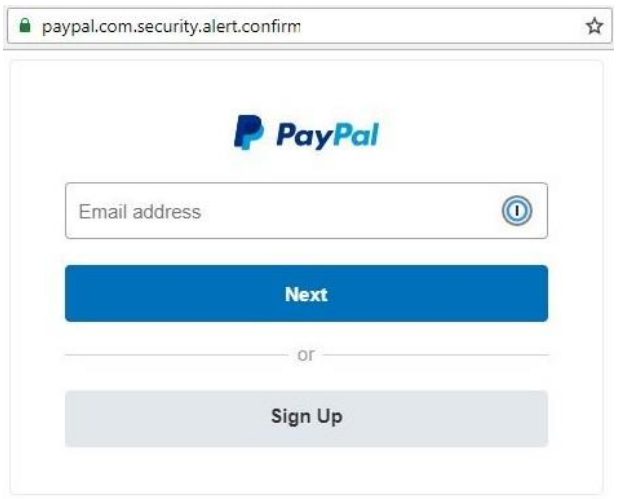
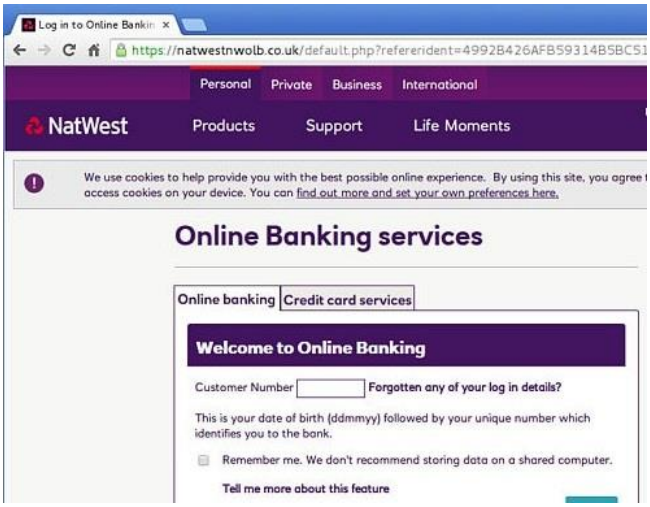
Website identity trust is as important as https encryption

At present, the industry emphasizes the importance of implementing https encryption for websites, which is very good and has achieved great results. However, since free SSL certificates are readily available, fake and fraudulent websites have also deployed SSL certificates, and browsers still display the security padlock. As shown in the figure below, the fake famous payment website PayPal and the fake NatWest bank website, the browser normally displays the security padlock. This subverts the traditional concept that people used to think that a website with a security padlock is secure, and it is very easy for users to be deceived.

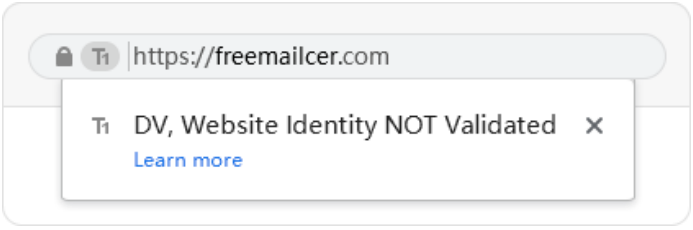




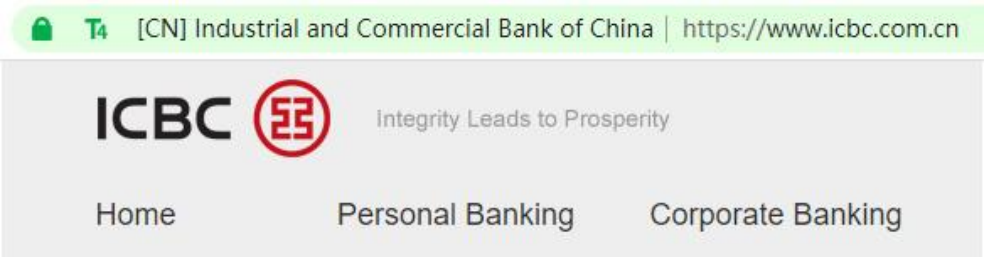
Indeed, there used to be a security padlock, the identity of this website must have passed strict identity validation, the website identity is trusted, and the confidential information entered by the website visitors on this website can be guaranteed to be secure. However, since the DV SSL certificate that only validates the domain name control, the problem came. The CA did not validate the identity of the website, but only validated the control of the website domain name and issued an SSL certificate to the website. There are benefits, but the ease of obtaining a DV SSL certificate also makes it just as easy to obtain for fake and fraudulent sites. The original education user to see if the website has a security padlock does not work, how to do? Browsers as Internet portals should do something about it!

If the browser thinks that it is secure if there is an SSL certificate that implements https encryption, this is really a big mistake! In particular, the green address bar of the browsers familiar to all netizens has been removed by major browsers, which makes it impossible for netizens to identify which is the authentic bank website and which is a fraudulent website, because they are all have security padlock, users can only rely on remembering the correct domain name of the bank. For example, the ICBC domain is icbc, while the fake ICBC website domain is 1cbc and lcbc, it is very easy to confuse users, and if you are not careful, you will be hooked on the fake ICBC website.

What to do? ZT Browser has already taken action in this regard, except that, like other browsers, websites without SSL certificates are displayed as "Not secure", and the DV SSL certificates that only validate domain names are deployed are gray security padlock and gray address bar, and display "Website Identity Not Validated" in the address bar to remind users to pay attention.



For the OV SSL certificate that has validated the identity of the website, a green security padlock, a light green address bar and the organization name of the website are displayed in the address bar. For websites that have deployed an EV SSL certificate for Extended Validated website identity, the ZT Browser address bar turns green, displays a green security padlock, and displays the organization name. Only in this way, the user will know immediately that the fake website is not the ICBC website but the website of a certain company. ZT Browser can effectively help users identify fake websites.



Therefore, in order to prevent websites from being counterfeited, especially famous brands, website owners must not buy cheap DV SSL certificates, but should choose OV SSL certificates or EV SSL certificates for identity validation. Or buy ZoTrus Website Trusted Identity Validation Service, so that ZT Browser can clearly display the identity information such as the name of the website owner, then

users can use the online services with confidence, which can effectively prevent the website from being counterfeited, just tell the user if the address bar is not green, then it is a fake site, very easy to understand and easy to identify.

Whether a website is secure and trusted depends on at least two factors. One is HTTPS encryption, which can ensure that the confidential information entered by the user on the browser can be encrypted and transmitted to the website server and can ensure the security of the transmission of confidential information. The other is the website identity. The authentic and trusted website identity can ensure that users will not be deceived by fake websites and lose money. Both elements are important. Any promotion or product that only has an important strength in one aspect is an unsecure product and irresponsible to users. Only when both elements are achieved can a secure and trusted website ensure the safety of website visitors and allow website visitors to trade with them at ease.

Maybe some readers will say that now I rarely use the browser, I use the App. This problem exposes the security flaw of the App's failure to prominently display the identity of the website and deserves the attention of developers of commonly used Apps. Many counterfeit Apps have been rampant now, so readers should download the online banking App from the official bank official website on the browser. Otherwise, if a counterfeit bank App is installed, property damage will be incurred. However, if the browser cannot clearly display the identity of the website, the user may visit a fake bank website and download a fake bank App, which is the same trick. Therefore, in the final analysis, it is still necessary for browsers (including Apps) to correctly display the trusted identity of the website, to effectively help users make correct security decisions.

Richard Wang

June 1, 2022
In Shenzhen, China