BROWSER UI
SECURITY INDICATORS

Examples of recent browser UI security indicators

Browser UI security indicators are constantly changing from one version number to the next, and there is little consistency among browsers even for the UI security indicator for any given type of TLS/SSL digital certificate. For this reason, users have a hard time understanding what any particular browser UI means as to user security.

From time to time, the CA Security Council will update this table to show recent browser UI security indicators among the browsers and for unencrypted websites as well as for encrypted websites using different levels of certificates – domain validated (DV), organization validated (OV), and extended validated (EV). CASC would like to encourage browsers to work together and coordinate their UI security indicators, and then stabilize their choices from one browser version to the next, so that users can better understand how to interpret the UI information for enhanced safety.

Browser UI Security **INDICATORS** as of March 2017:

Updated URL UIs indicated by orange outlined box

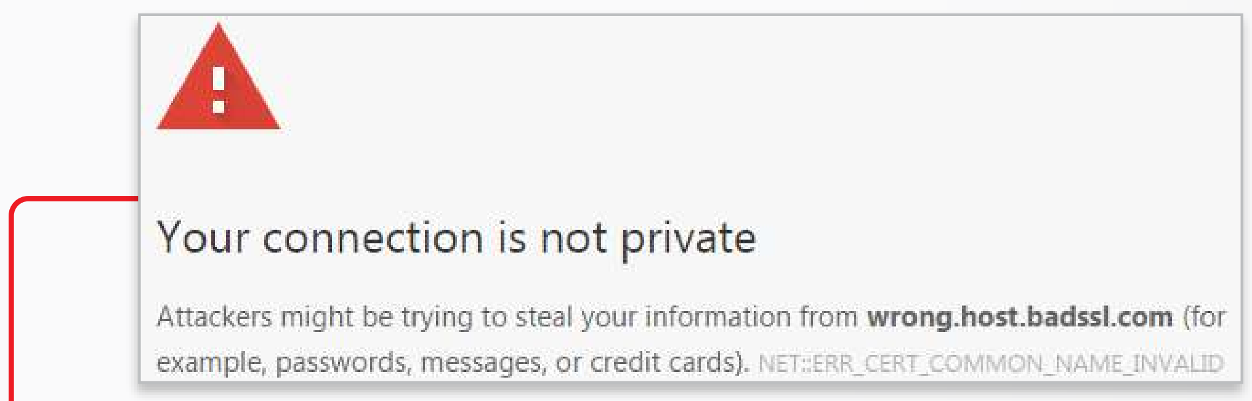
Browser UI Security Indicator:	HTTP only (no certificate)	DV certificate	OV certificate	EV certificate
Chrome 56 (Windows)	www.example.com	Secure https://case	Secure https://www	Trustwave Holdings, Inc. [US] https://www.trust
Chrome 56 (Android)	www.example.com	https://casecurity.cor	https://www.example	https://www.entrust.com
Edge 20 (Windows)	example.com	casecurity.org	example.com	Symantec Corporation [US] symantec.com
Firefox 51 (Windows)	www.example.com	https://casecurity	https://www.exar	COMODO CA Limited (GB) https://crt.sh
Safari 10 (Mac)	www.example.com	https://casecurity	https://www.exar	GMO GlobalSign Inc
Safari 10 (iOS)	example.com	casecurity.org	example.com	DigiCert, Inc.
OperaMini 23 (Android)	www.example.com	casecurity.org	www.example.cor	www.globalsign.com/en/
UC Mini 10 (Android)	Example Domain	CA Security Council	Example Domain	https://www.digicert.com
UC Browser 10.8.6.889 (iOS)	example.com	CA Security Council	example.com	SSL & Digital Certificates by GlobalSign

Browser UI Security **WARNINGS** as of March 2017:

Updated URL UIs indicated by red outlined box

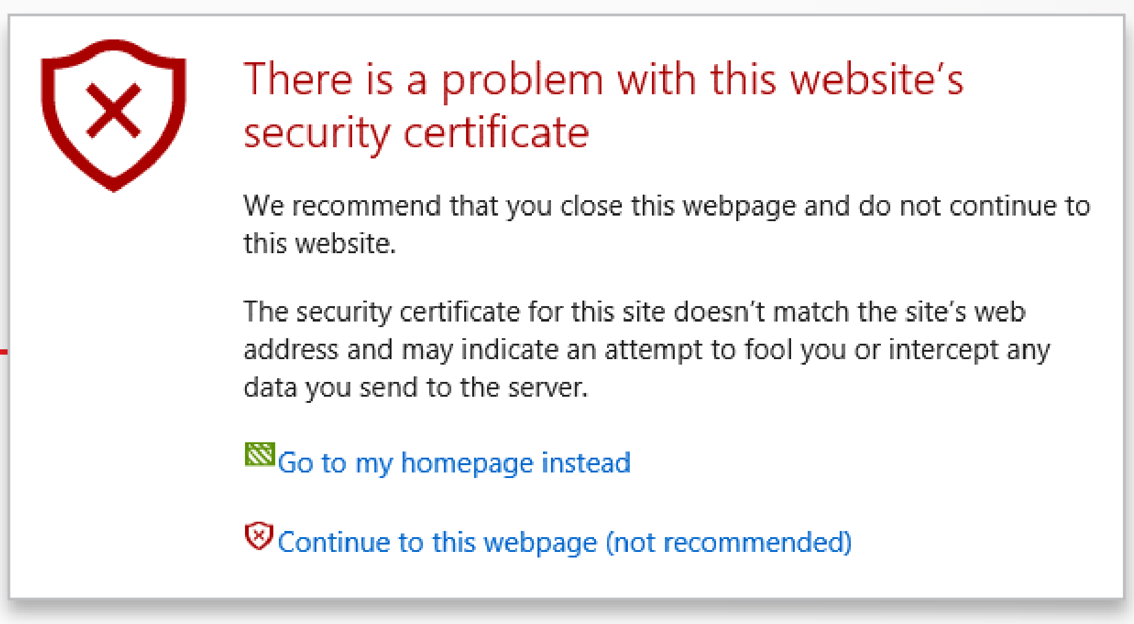
In addition, browsers also provide warnings to users when encrypted (https) pages include minor and major security errors. Here are recent examples of those browser UI security warnings.

Browser UI Security Indicator:	HTTPS Minor Error	HTTPS Major Error
Chrome 56 (Windows)	https://mixed.badssl.com	Not secure ~~https~~://wrong.host.b
Chrome 56 (Android)	https://mixed.badssl.com	~~https~~://wrong.host.badssl.com
Edge 20 (Windows)	mixed.badssl.com	wrong.host.badssl.com
Firefox 51 (Windows)	https://mixed.badssl.com	https://wrong.host.badssl.com
Safari 10 (Mac)	https://mixed.badssl.com	https://wrong.host.badssl.com
Safari 10 (iOS)	mixed.badssl.com	wrong.host.badssl.com
OperaMini 23 (Android)	mixed.badssl.com	wrong.host.badssl.com
UC Mini 10 (Android)	mixed.badssl.com	Error!
UC Browser 10.8.6.889 (iOS)	mixed.badssl.com	wrong.host.badssl.com



Your connection is not private

Attackers might be trying to steal your information from **wrong.host.badssl.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID



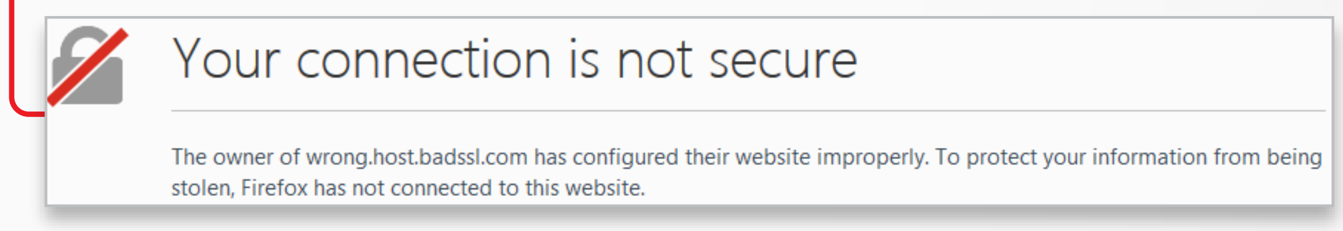
There is a problem with this website's security certificate

We recommend that you close this webpage and do not continue to this website.

The security certificate for this site doesn't match the site's web address and may indicate an attempt to fool you or intercept any data you send to the server.

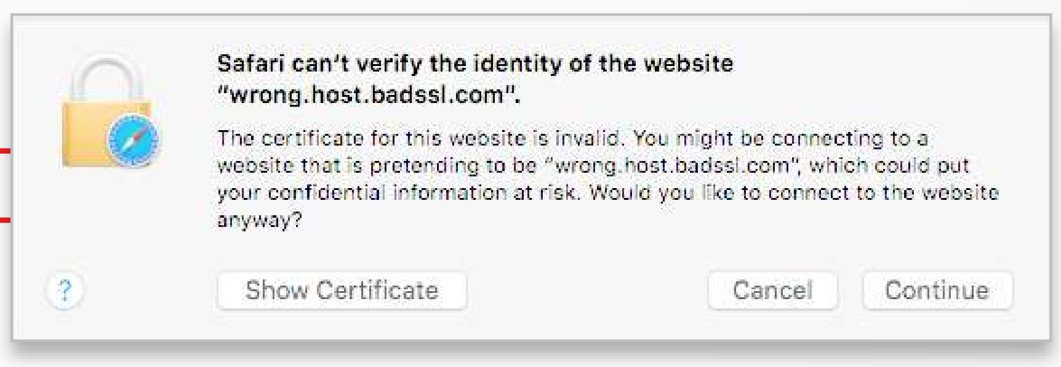
Go to my homepage instead

Continue to this webpage (not recommended)



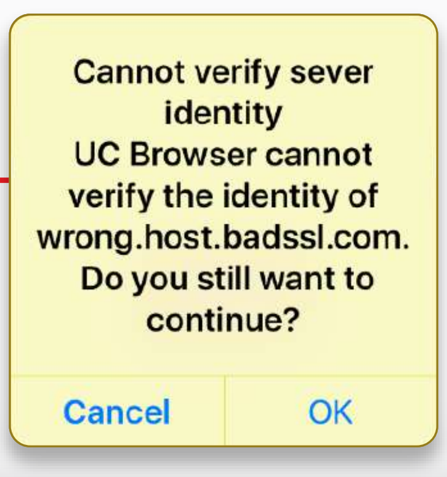
Your connection is not secure

The owner of wrong.host.badssl.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.



Safari can't verify the identity of the website "wrong.host.badssl.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "wrong.host.badssl.com", which could put your confidential information at risk. Would you like to connect to the website anyway?



Cannot verify sever identity
UC Browser cannot verify the identity of wrong.host.badssl.com. Do you still want to continue?

Click to learn more about UI indicators

https://casecurity.org/identity

Click https://casecurity.org/browser-ui-security-indicators/December2016 to view the previous indicators

CA Security COUNCIL