# HTTPS blokovacia stránka – problém s falošným certifikátom TLS

V prípade blokovania založeného na DNS upraví Online ochrana požadovanú IP adresu (ktorá sa vráti späť do zariadenia používateľa) na rozlíšenie domény, aby sa používateľovi poskytla blokovacia stránka.

Ak používateľ na začiatku odošle požiadavku https, prehliadač bude reagovať "chybou certifikátu" a mala by sa načítať blokujúca stránka, pretože ide o neznámu doménu vrátenú späť namiesto očakávanej domény. Ako sa zobrazí v tomto prípade chybová hláška pre používateľa, závisí od prehliadača.

#### 1. Google Chrome (Android)

Používateľ dostane z prehliadača internú správu, že pripojenie nie je súkromné z dôvodu chyby certifikátu (pretože očakávaná doména je iná ako prijatá doména).

Používateľ sa môže vrátiť do bezpečia v prípade, že nechce pokračovať, alebo môže kliknúť na tlačidlo Rozšírené. Tu sa mu ponúkne možnosť pokračovať na webovú stránku.

Keď naň klikne, zobrazí sa mu blokovacia stránka.



Aj v prehliadači Firefox sa používateľovi zobrazí interné varovné hlásenie z prehliadača, ktoré naznačuje, že pripojenie je nedôveryhodné. Po kliknutí na "Rozumiem rizikám" sa zobrazia ďalšie informácie vrátane možnosti "Navštíviť stránku".

Keď naň klikne, zobrazí sa mu blokovacia stránka. Vo Firefoxe má tiež možnosť pridať trvalú výnimku pre túto stránku.



### **3.** Mozilla Firefox (Windows desktop)

V PC prehliadači Firefox pre Windows sa používateľovi zobrazí interné varovné hlásenie z prehliadača, ktoré naznačuje, že existuje potenciálne bezpečnostné riziko. Po kliknutí na "Rozšírené…" sa zobrazia ďalšie informácie vrátane možnosti "Prijať Riziko a pokračovat".

Keď naň klikne, zobrazí sa mu blokovacia stránka.

Δ	Warning: Potential Security Risk Ahead	Δ	Warning: Potential Security Risk Ahead
	Firefox detected a potential security threat and did not continue to the state of the site, attackers could try to steal information like your passwords, emails, or credit card details.		Firefox detected a potential security threat and did not continue to the stead of the site, attackers could try to steal information like your passwords, emails, or credit card details.
	What can you do about it?		What can you do about it?
	The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.		The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.
	Learn more		Learn more
	Go Back (Recommended) Advanced		Go Back (Recommended) Advanced
			Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for the certificate is only valid for the certi
			Go Back (Recommended) Accept the Risk and Continue

## 4. Apple Safari (iOS)

V prehliadači Safari sa používateľovi zobrazí interné varovné hlásenie z prehliadača, ktoré naznačuje, že pripojenie nie je súkromné. Po kliknutí na "Zobraziť podrobnosti" sa zobrazia ďalšie informácie vrátane možnosti "Navštíviť túto webovú stránku".

Keď naň klikne, zobrazí sa mu blokovacia stránka.



#### 5. Microsoft Edge (Windows desktop)

V PC prehliadači Edge pre Windows sa používateľovi zobrazí interné varovné hlásenie z prehliadača, ktoré naznačuje, že pripojenie nie je súkromné. Po kliknutí na tlačidlo "Rozšírené" sa zobrazia ďalšie informácie vrátane možnosti "Pokračovať na <xyz> (nebezpečné)".

Keď naň klikne, zobrazí sa mu blokovacia stránka.

	<b>A</b>	
Your connection isn't private	Your connection isn't private	
Attackers might be trying to steal your information from (for example, passwords, messages or credit cards).	Attackers might be trying to steal your information from (for example, passwords, messages or credit cards).	
NET-ERR_CERT_COMMON_NAME_INVALID	NET:ERR_CERT_COMMON_NAME_INVALID	
Advanced Go back	Hide advanced Go back	
	This server couldn't prove that it's <b>security</b> certificate is from This may be caused by a misconfiguration or an attacker intercepting your connection.	
	Continue to unsafe)	