

Website security changes are one of the only constants on the web today. By using the right certificates for your website and each webpage, you'll be prepared for any updates as they occur.

Is your site affected?

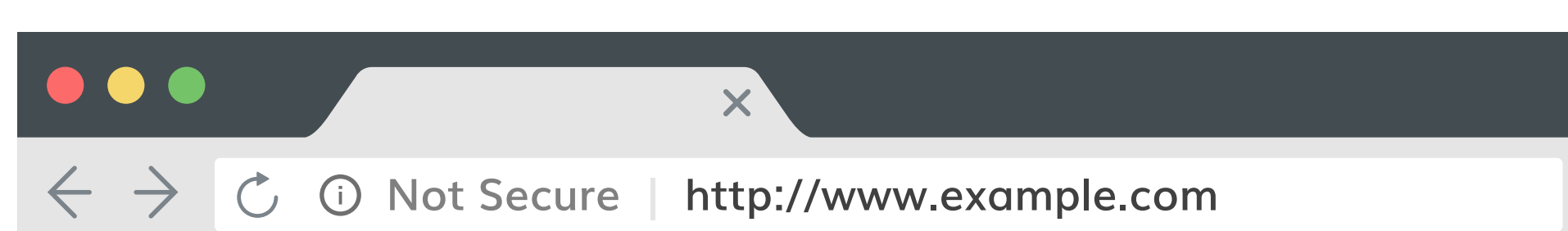
Google Chrome and Mozilla Firefox already warn users when web pages ask for login or credit card information without using SSL certificates. From July 24, 2018, Google Chrome was the first browser to show users prominent "Not Secure" warnings on any page on your site which isn't secured with an SSL certificate.

What does the warning look like?

Pages without SSL Certificates



CURRENT CHROME:
Page DOES NOT ask for login or credit card info.



CURRENT CHROME:
Page DOES ask for login or credit card info.

Chrome 68 (July 2018):
ALL pages

The right certificate can make all the difference.

Although all SSL certificates provide the same level of encryption, high-assurance certificates provide added layers of authentication to give users proof they can trust who you are—which elevates the trustworthiness of your entire site. Here's how the certificates stack up.

Domain Validation (DV)

KEY DIFFERENTIATORS:

- Fastest issuance
- No company information on certificate
- Easier for phishing sites to obtain

USER PERSPECTIVE:

"I'm on a site that appears to be secure."



VALIDATES:

Domain ownership/control

TYPICALLY USED FOR:

- Internal/non-public-facing sites
- Web-based applications (no risk of fraud)
- Sites where credibility matters less than data security

Organization Validation (OV)

KEY DIFFERENTIATORS:

- Higher assurance with more options to demonstrate visible site legitimacy
- Vetted company information displayed within the certificate

USER PERSPECTIVE:

"I'm on a secured site that belongs to a legitimate organization."



VALIDATES:

Domain ownership/control

Additional information about the organization which controls the site (registered/legal name, location, etc.)

TYPICALLY USED FOR:

- Public-facing sites limited to less-sensitive transactions
- Searchable information sites
- Government and educational sites

Extended Validation (EV)

KEY DIFFERENTIATORS:

- Highest assurance with the strongest visual confirmation of identity
- Green address bar featuring organization name
- Extensive vetted information displayed within the certificate

USER PERSPECTIVE:

"I feel confident I can trust this secured website with my most sensitive personal information."



VALIDATES:

Domain ownership/control

Additional information about the organization which controls the site (registered/legal name, location, etc.)

Extensive identifying details (legal status, physical and operational existence, contract signer authority, etc.) via rigorous cross-referencing of third-party sources

TYPICALLY USED FOR:

- Sites that require login, accept payments or handle private information or other sensitive data such as eCommerce, banking, and healthcare sites
- Sites that want to reassure their visitors with a visual indicator in the address bar

It's more than just HTTPS.

High-assurance OV or EV SSL on every page ensures users can easily identify your website as authentic, making it harder for phishing sites to mimic you and defraud your visitors.

[Contact a sales representative](#) today for a full site review.