

Is your domain portfolio ready?

As of September 2026, if HTTPS is not available on the source domain, a warning prompt will display, and Chrome will force users to confirm before continuing to public sites that do not support HTTPS.

What changes in Chrome 154

Chrome will enable Always Use Secure Connections by default for public sites. It will try HTTPS first and show a prompt when HTTPS is unavailable.



HTTPS is the expectation

98%

of public-site navigations on Windows use HTTPS. But one unencrypted connection can still create risk.

HTTP exposes data in transit

Information sent over HTTP can be potentially viewed or altered.

Redirects are connections, too

The browser connects to the source domain before moving to the secure destination.

Browser expectations are changing

Chrome will warn users before visiting public sites without HTTPS, beginning in October 2026.

Digital risks remain widespread | HTTPS protects data in transit

22%

of breaches began with credential abuse

Verizon 2025 DBIR

24%

of surveyed US and UK users reported a stolen password or compromised account

FIDO Alliance 2024

29%

of Americans have had an online account hacked

Pew Research 2025

79%

call online scams and attacks a major problem

Pew Research 2025

What should you do today?

Review every public domain, subdomain, and redirect source. Confirm HTTPS coverage, certificate renewal, and destination behavior.

Simplify secure redirects with DigiCert UltraDNS

UltraDNS HTTPS Secure Web Forwarding automatically provisions, deploys, and renews DigiCert TLS certificates for secure redirects.

Automated certificates

301 and 302 redirects

Path and query preservation

Wildcard support

Portal and API V3

Audit your domain portfolio

Contact DigiCert to learn more about UltraDNS HTTPS Secure Web Forwarding

Sources: Google Chrome Security; Verizon 2025 DBIR; FIDO Alliance 2024; Pew Research Center 2025.