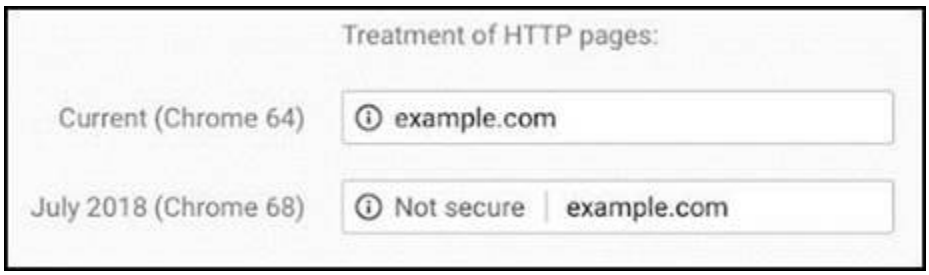
Hyper Text Transfer Protocol Secure (HTTPS)

What it is: *Hyper Text Transfer Protocol Secure (HTTPS) is an Internet communication protocol used to encrypt and securely transmit information between a user's web browser and the website they are connected to.* It is designed to better protect the integrity and confidentiality of user's information when they visit websites. HTTPS accomplishes this through the use of a Secure Sockets Layer (SSL) certificate, which establishes an encrypted connection. The certificate also helps authenticate that the website and the user are who they say they are when communicating. These features make it more difficult for malicious actors to tamper with the communication. HTTPS is built on Hyper Text Transfer Protocol (HTTP), the communication protocol used to transmit data between a website and a user, but HTTP transmits content unencrypted. HTTPS is becoming the norm across the Internet. For instance, as of December 31, 2016, HTTPS is required on all Federal government websites.

Why does it matter: When communication is transmitted unencrypted, it is sent via plaintext between the user and the connected website. This may expose the communication to malicious actors sniffing traffic on a network or seeking to tamper with the contents. Encryption is especially important on webpages that collect information through forms or require a user to login, such as online voter registration.

Additionally, beginning in July 2018, the Google Chrome web browser will begin marking websites that do not use HTTPS as "Not secure". Google Chrome has over a 50% market share and ranks as the most used web browser as of 2018. Users will still have access to election office websites that continue to use HTTP after the July deadline, but will see the "Not Secure" tag in their address bar, as depicted below. This label may adversely affect the public's confidence in election websites that do not use HTTPS.



What you can do: If your election office website does not currently use HTTPS, consider implementing it prior to July 2018. This includes verifying that your organization has a valid SSL certificate from a Trusted Certification Authority. Resources such as the Office of Management and Budget's HTTPS website, Google's guide to Enabling HTTPS on Your Servers and Qualys Labs' documentation on SSL certificates, provide additional information to assist in implementation.

For a refresher on encryption generally, please review the March 30, 2018 EI-ISAC Cybersecurity Spotlight.

24×7 Security Operations Center
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Learn, Get Assistance, and Collaborate

- For information on DHS cyber programs, visit https://www.dhs.gov/cyber
- To access the full range of DHS cyber resources, email SLTTCyber@hq.dhs.gov
- To learn about regional protective security advisors and cybersecurity advisors, visit https://www.dhs.gov/protective-security-advisors
- To become an EI-ISAC member, visit https://learn.cisecurity.org/ei-isac-registration
- To learn about the HSIN Portal, contact HSIN.Outreach@hq.dhs.gov
- For information on the Federal Virtual Training Environment, visit https://fedvte.usalearning.gov

Homeland Security