GC HTTPS Everywhere/Communication Material

< GC HTTPS Everywhere



ITPIN 2018-01 (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html)	Implementation Strategy	Implementation Guidance	Communicatio

Contents

Communication Plan
- What is HTTPS?
- Background
- What Should Communications Teams do?
- How to Increase Compliance
- What Departments Need to do to be Compliant

Q&A Scenarios
- My Site Is Only Accessible Internally
- Can I Still Serve My Site Over HTTP If I Also Have HTTPS?
- My Website Works Just Fine Over HTTP
- No Forms or Information Collected
- There is Nothing Sensitive on My Site
- HTTPS Is Going To Slow Down My Website – Encryption Is CPU Intensive
- My Site Is HTTP, But Our Forms Are Submitted Over HTTPS
- Certificates Are Expensive - I Don't Have The Budget This Year.
- I Don't Have The Skillsets Or Resources To Support HTTPS
- My Site Can Still Be Impersonated, Even If I Use HTTPS
- Domain-Validated (DV) Certificates Aren't Secure
- What If A Certificate Authority Misissues A Cert For My Site?
- Phishing Sites Use HTTPS
- Our Site Relies Heavily On 3rd Party Content Over HTTP
- HTTPS Impacts Search Engine Optimization

Enquiries

Communication Plan

Regular and consistent communication across the diverse stakeholder community will be important in achieving HTTPS everywhere compliance organization. A clear communications strategy will also reduce the likelihood of stakeholder resistance to an HTTPS everywhere migration.

The following proposes the essential communications actions required for successful implementation of GC HTTPS:

1. Utilize both formal and informal communications channels as conduits for information flow.
2. Establish a brand to be used in project planning and execution, to provide a common anchor for communications and conversation with stakeholde citizens.
3. Establish clear communication channels throughout the GC for senior leadership as champions of the HTTPS everywhere initiative.
4. Develop technical guidance / briefing material in the form of an ITPIN for CIOs and IT teams across the GC outlining expectations and timelines.
5. Coordinate with service owners to establish media lines to announce the change to GC websites and services, informing citizens of the impact and requirements.
6. Utilize GC Tools and public social media platforms to establish a forum for Q&A discussion with service and technology owners, and industry specia
7. Develop guidance / briefing material for business owners across the GC with respect to the importance of the changes and expected impact on the
8. Develop effective strategies to engage with remote teams across the GC (both governance and information sharing).

HTTPS Speaking Points

What is HTTPS?

- The Hypertext Transfer Protocol (HTTP) is the foundation for data communication on the web. This protocol defines how messages are formatted and trans m actions web servers and browsers should take in response to various commands.
- Hypertext Transfer Protocol Secure (HT TPS) combines HTTP with a security layer to protect user connections to websites. HTTPS guarantees the protecti on between two systems. It will not protect the system itself from being hacked or its information from being breached.

Background

- In June 2018, TBS issued an Information T echnology Policy Implementation Notice (ITPIN) on Implementing Hypertext T ransfer Protocol S ecure (HTTPS) for Connections (https://www.canada.ca/en/government/system/digital-government/modern-em erging-technologies/policy-implementation-notices/implementing-ht onnections-itpin.html) on all publicly accessible websites and web services. The original compliance deadline was September 30, 2019; however , the deadline extended to December 31, 2019. The extended deadline has been communicated to departments.

What Should Communications T eams do?

- Section 6.2.1 of the ITPIN states that newly developed websites and web services must adhere to the ITPIN upon launch. Therefore, communications teams sho requirement as part of the web publication process to ensure that new websites and web services are not published using unsecure connections.
- Section 6.2.2 of the ITPIN states that websites and web services that involve an exchange of personal information or other sensitive information must receive pri migrate as soon as possible. Therefore, communications teams should identify these websites and develop a schedule for immediate migration to HTTPS
- Section 6.2.3 of the ITPIN states that all remaining websites and web services must be accessible through a secure connection by December 31, 2019. Therefor communications teams should ensure that existing sites are being migrated leading up to the compliance deadline. For example, communications teams could e new content is published to existing sites, HTTPS is implemented at the same time to avoid the risk of new content being released on unsecured websites.

How to Increase Compliance

- To assist departments in meeting the requirements in the Policy Implementatio n Notice, TBS has provided departments with the following implementation guida and tools:
  - Project guidance (https://https-everywhere.canada.ca/en/guidance/)
  - HTTPS Everywhere on GCcollab (https://wiki.gccollab.ca/GC_HTTPS_Everywhere) wiki including:
    - Implementation Guidance (https://wiki.gccollab.ca/GC_HTTPS_Everywhere/Implementation_Guidance)
    - Implementation Strategy (https://wiki.gccollab.ca/GC_HTTPS_Everywhere/Strategy)
  - HTTPS Everywhere on GCconnex (https://gcconnex.gc.ca/groups/profile/35218846/gc-https-everywhere-2018-https-partout-dans-le-gc-2018) and GCcoll b.ca/groups/profile/1358152/engc-https-everywhere-2018frgc-https-partout-2018)
    - Regular blog posts
  - HTTPS Everywhere on GCmessage (https://message.gccollab.ca/channel/httpseverywhere-httpspartout)
- TBS has been running bi-weekly workshops since January 2019 to share information and provide technical guidance. TBS will continue to run monthly workshop December 2019. W e encourage depart ments to send their staf f.
- TBS is continuing to work one-on-one with departments and agencies to address challenges to improve overall compliance to the ITPIN. If departments are facin they should contact the TBS Cyber Security Division (zzTBScybers@tbs-sct.gc.ca (mailto:zzTBScybers@tbs-sct.gc.ca)).

What Departments Need to do to be Compliant

- Departments must validate the list of domains on the compliance dashboard,
  - Contact the TBS Cyber Security mailbox with changes, as required (zzTBScybers@tbs-sct.gc.ca (mailto:zzTBScybers@tbs-sct.gc.ca))
- If the department is one of the 43 departments that are Shared Services Canada partners, the department should contact their account executive and service del to initiate planning and implementation of HTTPS.
- Public domains must be configured to redirect users immediately to an HTTPS connection, after which they may then be redirected to pages on subsequent dom Canada.ca).
- Public domains must provide instructions for users' browsers to only connect to the HTTPS domains (i.e. HTTP Strict T ransport Security (HSTS) must be enat
- Public domains must disable known weak connection protocols and encryption ciphers, in accordance Communication Security Establishment guidance (ITSP ITSP.40.111).
- Public domains must use HTTPS certificates issued from a Certificate Authority (e.g.: Entrust via SSC; see Certificates in Implementation Guidance (https://w HTTPS_Everywhere/Implementation_Guidance) for more).

Q&A Scenarios

This material is provided as a starting point for discussions with business and technical partners depending on the scenario/context presented. If the that need to be covered, please contact TBS via the mailbox (below) or engage in the chat on GCmessage (#HTTPSEverywhere-HTTPSpartout (http ab.ca/channel/httpseverywhere-httpspartout)).

My Site Is Only Accessible Internally

The HTTPS ITPIN is only applicable to externally focused public websites and web services. Your site is out of scope of this direction, how recommended to consider implementing HTTPS.

Can I Still Serve My Site Over HTTP If I Also Have HTTPS?

No, all publicly available websites should only offer HTTPS connections by September 30, 2019. Any HTTP connections should be permanently redire website.

My Website Works Just Fine Over HTTP

Not anymore. As of July 2018, Google Chrome will begin alerting all HTTP connections as Not Secure, with other major browsers potentially followi presents a new reputational risk to digital services.

No Forms or Information Collected

HTTPS protects more than just form data. HTTPS keeps the URLs, headers, and contents of all transferred pages confidential.

There is Nothing Sensitive on My Site

Cyberspace is borderless, and HTTP connections are simply a liability. Just as we have no control over detours on surface roads, we have no con traffic will take through the internet.

This lack of control introduces opportunities to inject text, scripts, images, or ad content onto your page so that it looks like you put them there. HT activity, and guarantees content integrity and the ability to detect tampering.

Additionally, if we encrypt only sensitive content, then we automatically paint a target on that content. Keep your secrets secret by encrypting everythin

HTTPS Is Going To Slow Down My Website – Encryption Is CPU Intensive

No it's not. Sites with modern servers load faster over HTTPS than over HTTP because of HTTP/2. Over 75% of the world's websites are now HT largest banks, social media sites.

Latency metrics provided by them over time have proven that properly implemented HTTPS is faster than HTTP. https://istlsfastyet.com/

My Site Is HTTP, But Our Forms Are Submitted Over HTTPS

A site using HTTP is susceptible to interception and manipulation, meaning you lose control over the actions associated with the forms you pres regardless of how they're submitted.

Attackers are provided the chance to modify how/where the data is submitted, and there's no way to detect this because it happens over the wire with

Encrypting your whole site with HTTPS from the start prevents this.

Certificates Are Expensive - I Don't Have The Budget This Year.

They're free. (Let's Encrypt)

I Don't Have The Skillsets Or Resources To Support HTTPS

HTTPS doesn't have to be complicated; many web servers such as Caddy are designed to be run natively with HTTPS as default now, and se generators are available from organizations like Mozilla. Certificate management has been made exponentially easier with the introduction of automatic

My Site Can Still Be Impersonated, Even If I Use HTTPS

The dangers presented by impersonation online are greatly mitigated by the use of HTTPS and a properly issued certificate (one logged in certificate logs, with a strong signature algorithm (at least SHA-256), from an authorized CA (CAA)).

As long as your server is secured, and your private key remains private, any mismatched certificate will be flagged by browsers as such, or invalid, Secure alert to the user. Internal processes reviewing CT logs for mis-issued certs will catch illegitimate certificates.

Finally, if the impersonator doesn't use HTTPS at all, browsers will alert the malicious site as insecure immediately.

Domain-Validated (DV) Certificates Aren't Secure

Domain Validated certificates offer the same technical security as Extended Validation (EV) certificates, and it has been shown increasingly that the EV certs has not been realized.

As long as you don't lose control of your DNS entries or domain hosting, and choose a competent certificate authority, DV certs are perfectly ac absolutely no difference in the cryptography in a DV certificate compared to that of an extended validation (EV) certificate.

What If A Certificate Authority Misissues A Cert For My Site?

The GC is working to establish governance around the issuance of certificates through the use of CAA records to restrict which CAs can issue certif Until that time, the system will rely on certificate transparency and oversight to manage the infrastructure.

Phishing Sites Use HTTPS

Yes, they do, but this isn't a good reason not to use HTTPS.

Our Site Relies Heavily On 3rd Party Content Over HTTP

The inclusion of HTTP content from a 3rd party provider is a proven vector for attack, as you do not have control over the security of that content. means any content included in your website should be from HTTPS-enabled sources, to avoid both mixed-content errors and the inherent vulnerabilitie

As this may require renegotiation or termination of contracts with content providers, it is recommended to begin sooner rather than later, or con providers to move to HTTPS as well.

HTTPS Impacts Search Engine Optimization

HTTPS improves SEO!

It is true that switching and redirecting site URLs incorrectly may impact your search rankings, but overall HTTPS has been taken into consideration t rankings.

Ensure you follow the guidance of the search engine you're optimizing for, and everything will be fine.

Adapted from: https://doesmysiteneedhttps.com/

Enquiries

Feel free to join the conversation on GCmessage (https://message.gccollab.ca/channel/httpseverywhere-httpspartout) (#HTTPSEverywhere-HTTPS your questions to TBS Cyber Security at ZZTBSCYBERS@tbs-sct.gc.ca (mailto:ZZTBSCYBERS@tbs-sct.gc.ca).

Retrieved from "https://wiki.gccollab.ca/index.php?title=GC_HTTPS_Everywhere/Communication_Material&oldid=1103"

This page was last edited on 18 July 2019, at 08:14.

Content is available underCreative Commons Attribution 4.0 International Licenseunless otherwise noted.