# Why HTTPS Matters

**By** Kayce Basques
Technical Writer for Chrome DevTools

You should always protect all of your websites with HTTPS, even if they don’t handle sensitive communications. Aside from providing critical security and data integrity for both your websites and your users' personal information, HTTPS is a requirement for many new browser features, particularly those required for progressive web apps.

## TL;DR

- Intruders both malignant and benign exploit every unprotected resource between your websites and users.
- Many intruders look at aggregate behaviors to identify your users.
- HTTPS doesn't just block misuse of your website. It's also a requirement for many cutting-edge features and an enabling technology for app-like capabilities such as service workers.

## HTTPS protects the integrity of your website

HTTPS helps prevent intruders from tampering with the communications between your websites and your users’ browsers. Intruders include intentionally malicious attackers, and legitimate but intrusive companies, such as ISPs or hotels that inject ads into pages.

Intruders exploit unprotected communications to trick your users into giving up sensitive information or installing malware, or to insert their own advertisements into your resources.

For example, some third parties inject advertisements into websites that potentially break user experiences and create security vulnerabilities.

Intruders exploit every unprotected resource that travels between your websites and your users. Images, cookies, scripts, HTML … they're all exploitable. Intrusions can occur at any point in the network, including a user's machine, a Wi-Fi hotspot, or a compromised ISP, just to name a few.

## HTTPS protects the privacy and security of your users

HTTPS prevents intruders from being able to passively listen to communications between your websites and your users.

One common misconception about HTTPS is that the only websites that need HTTPS are those that handle sensitive communications. Every unprotected HTTP request can potentially reveal information about the behaviors and identities of your users. Although a single visit to one of your unprotected websites may seem benign, some intruders look at the aggregate browsing activities of your users to make inferences about their behaviors and intentions, and to de-anonymize ↗ their identities. For example, employees might inadvertently disclose sensitive health conditions to their employers just by reading unprotected medical articles.

## HTTPS is the future of the web

Powerful, new web platform features, such as taking pictures or recording audio with `getUserMedia()`, enabling offline app experiences with service workers, or building progressive web apps, require explicit permission from the user before executing. Many older APIs are also being updated to require permission to execute, such as the geolocation ↗ API. HTTPS is a key component to the permission workflows for both these new features and updated APIs.

Next
Important Security Terminology →

*Last updated July 2, 2018.*