



## #4 / Why HTTPS matters

You should always protect all of your websites with HTTPS,  
even if they don't handle sensitive communications.

비록 HTTPS 가 민감한 통신까지 일일이 다루어 줄 수는 없지만,  
당신은 당신의 모든 웹사이트들을 HTTPS 로 보호해야 합니다.

Type '/' for commands

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.

HTTPS 가 당신의 웹사이트와 당신의 사용자들의 개인정보에  
중요한 보안 기능과 데이터 무결성을 제공하는 걸 차치하더라도,  
HTTPS 는 브라우저의 여러 새 기능들에 있어,  
특히 progressive web apps(?) 에 있어서 꼭 필요한 것입니다.

Real Talk about HTTPS (Chrome Dev Summit 20...)



---

## Summary

### 요약

- Intruders both malignant and benign exploit every unprotected resource between your websites and users.

악의적인 침입자이든 그렇지 않은 침입자이든 간에  
그들은 당신의 웹사이트와 사용자들의 보호되지 않은 리소스를 이용합니다.

- Many intruders look at aggregate behaviors to identify your users.

많은 침입자들은 사용자인지 알아보기 위해 전체적인 행동들을 살펴봅니다.

- HTTPS doesn't just block misuse of your website.

HTTPS 는 단지 당신의 웹사이트가 부정적으로 사용되는 것만을 막는 것이 아닙니다.

It's also a requirement for many cutting-edge features and an enabling technology for app-like capabilities such as service workers.

HTTPS 는 여러 최첨단 기능들을 위해 꼭 필요하며 service workers(?) 와 같은 app-like capabilities(?) 를 가능하게 하는 기술입니다.

---

## HTTPS protects the integrity of your website

### HTTPS 는 당신의 웹사이트의 무결성을 보호합니다

HTTPS helps prevent intruders from tampering with the communications between your websites and your users' browsers.

HTTPS 는 침입자들이 당신의 웹사이트와 당신의 사용자들의 브라우저들 사이의 소통에 함부로 손대려 하는 것을 막는데 도움을 줍니다.

Intruders include intentionally malicious attackers, and legitimate but intrusive companies, such as ISPs or hotels that inject ads into pages.

여기서 침입자들이란 의도적으로 악의를 가지고 있는 공격자나  
페이지에 광고를 넣는 ISPs 나 호텔처럼 합법이지만 공격적인 회사들을  
포함합니다.

---

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.

침입자들은

당신의 사용자들이 민감한 정보를 주거나 malware 를 설치하도록 속이기 위해,  
또는 그들만의 광고를 당신의 리소스에 넣기 위해서  
보호되지 않은 통신들을 이용합니다.

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

그 예로는,  
제 3자가 사용자 경험을 해치고 보안 취약점을 만들기 위해  
광고를 웹사이트에 집어넣는 경우가 있습니다.

Intruders exploit every unprotected resource  
that travels between your websites and your users.

침입자들은 당신의 웹사이트와 당신의 사용자들을 오가는  
보호되지 않은 모든 리소스들을 강탈합니다.

Images, cookies, scripts, HTML... they're all exploitable.  
이미지, 쿠키, 스크립트, HTML... 그들은 착취적입니다.

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.

침입은 사용자의 machine 이든, Wi-Fi 핫스팟이든,  
보안이 미비한 ISP 이든, 네트워크안에서라면 언제든지 발생할 수 있습니다.

---

**HTTPS protects the privacy and security of your  
users**

## **HTTPS 는 당신의 사용자들의 안전과 사생활을 보호한다**

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

HTTPS 는 당신의 웹사이트와 당신의 사용자들 사이에서 일어나는 통신을 수동적으로 들을 수 없도록 막습니다.

One common misconception about HTTPS is that the only websites that need HTTPS are those that handle sensitive communications.

HTTPS 에 대한 한가지 흔한 오해는  
오직 민감한 통신을 다루는 웹사이트들에게만 HTTPS 가 필요하다는 인식입니다.

Every unprotected HTTP request can potentially reveal information about the behaviors and identities of your users.

모든 보호되지 않은 HTTP 요청은  
당신의 사용자들의 신원이나 행동에 관한 정보를 널리 퍼뜨릴 수 있는  
잠재적인 위험성을 가지고 있습니다.

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.

비록 당신의 보호받지 않는 웹사이트들 중 하나를 한번 방문하는 것은  
대수롭지 않아 보일 수 있습니다만,  
몇몇 침입자들은  
그들의 행동이나 의도를 통해 추론을 해서 그들의 신원을 밝혀내기 위해  
당신의 사용자들의 전체적인 브라우저 활동내역을 봅니다.

For example, employees might inadvertently disclose sensitive health conditions to their employers just by reading unprotected medical articles.

예를 들어, 직원은 아마 보호받지 않은 의료관련 기사들을 읽은 것 만으로도  
고용주에게 자신의 민감한 건강 정보를 의도치않게 드러낼 수 있습니다.

---

## **HTTPS is the future of the web**

### **HTTPS 는 바로 웹의 미래입니다**

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.

service workers(?) 와 함께하는 오프라인 앱 경험이나 progressive web apps(?) 를 만드는 것을 가능케 하는 `getUserMedia()` 로 사진을 찍거나 오디오를 녹음하는 등의 강력하고 새로운 웹 플랫폼의 기능들은 사용자가 그러한 행위를 하기 전에 명백한 인증을 요청합니다.

Many older APIs are also being updated to require permission to execute, such as the Geolocation API.

Geolocation API 와 같은 많은 오래된 API 들 또한 인증을 요청하기 위해 업데이트되고 있습니다.

HTTPS is a key component to the permission workflows for both these new features and updated APIs.

HTTPS 는 새로운 기능들과 업데이트되어가는 API 를 모두에게 있어 인증을 밟는 절차에 관여하는 핵심요소입니다.