Web Security in 2017

Johann Hofmann

Me.

I am Johann Hofmann

I work on Firefox (Security & Privacy)

Twitter @johannh

GitHub @johannhof

Secure websites

Secure Connections

Secure Web Content

Secure Access to Device Capabilities

moz://a

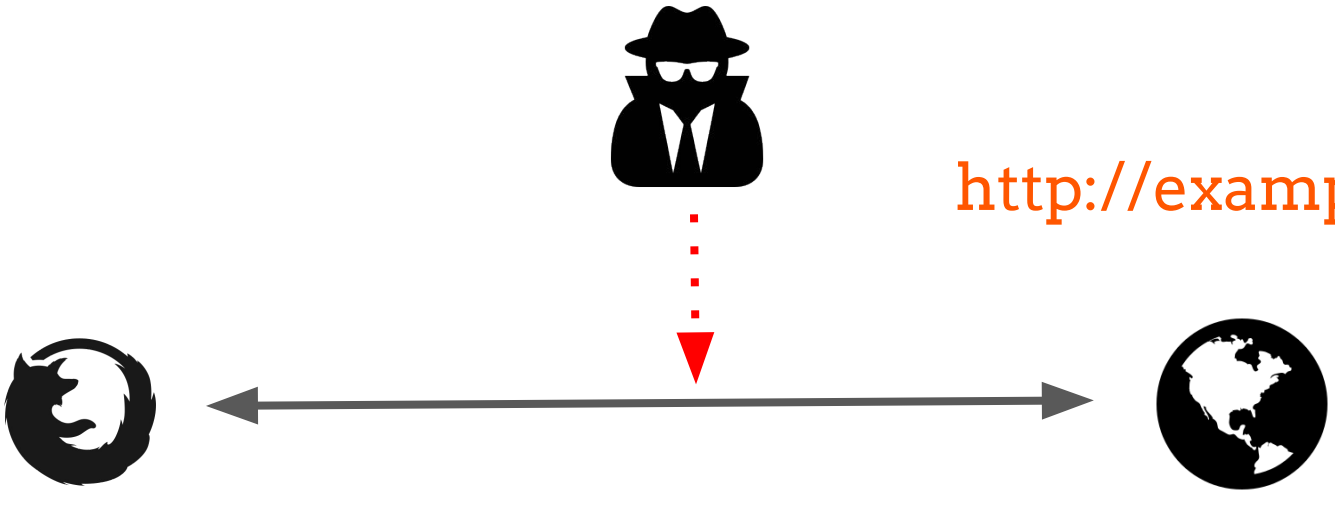
Secure Connections

HTTP

http://example.com

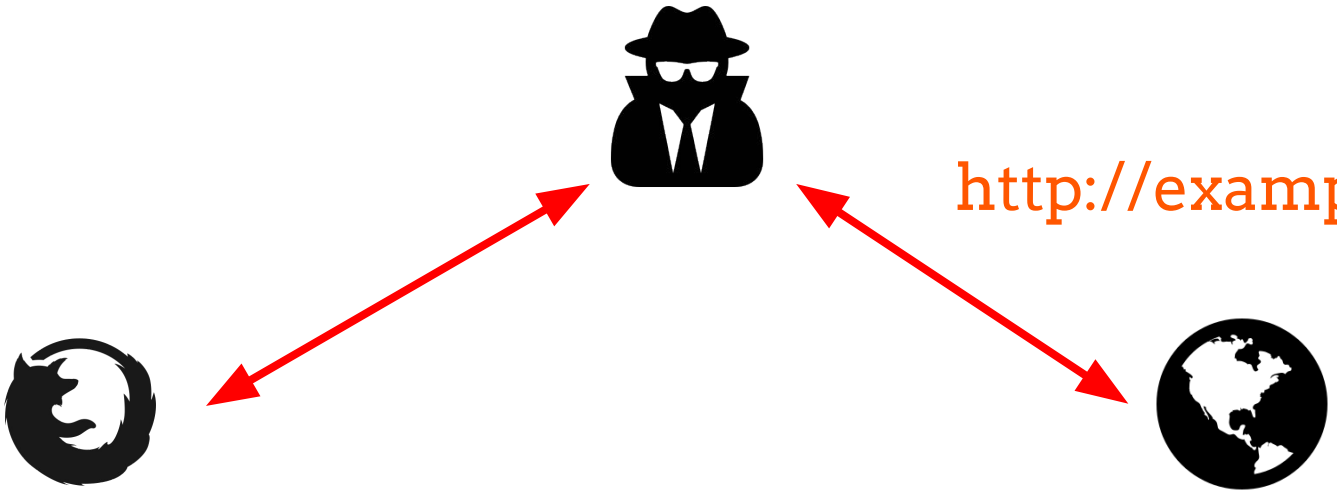
HTTP is the protocol your browser uses to load websites.

HTTP



Attackers can snoop on HTTP traffic on the same network.

HTTP



Attackers can intercept and replace
(man-in-the-middle) HTTP traffic on the same network.

HTTP

Attackers can impersonate your entire website.

Secure Connections

HTTPS protects confidentiality and integrity of your and your user's data during transmission.

(Yes it's not perfect, but that's a different story.)

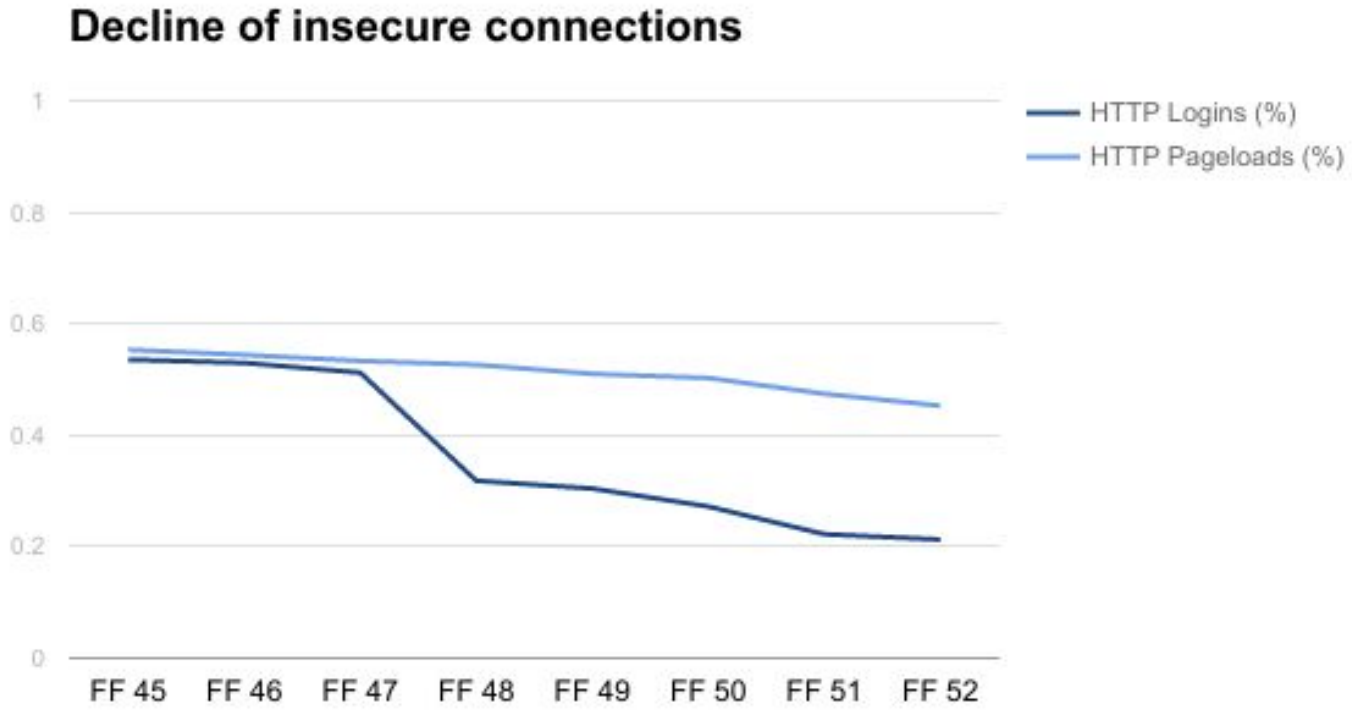
Read more about how protocols on the web work: https://hpbn.co/

The bad news

Over 25% of user credentials are transmitted over HTTP.

https://telemetry.mozilla.org/new-pipeline/dist.html#!cumulative=0&end_date=2016-12-09&keys=__none__!__none__!__none__&max_channel_version=release%252F50&measure=PWMGR_LOGIN_PAGE_SAFETY&min_channel_version=release%252F46&processType=*&product=Firefox&sanitize=1&sort_keys=submissions&start_date=2016-11-04&table=1&trim=1&use_submission_date=0

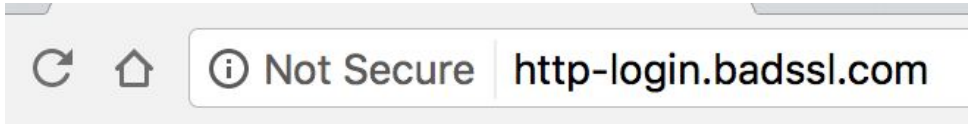
The good news

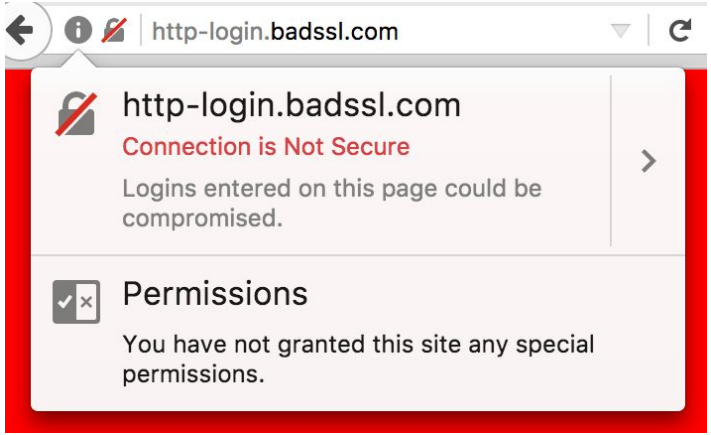


https://telemetry.mozilla.org/

The switch to HTTPS

Browsers now aggressively flag insecure sites.





The switch to HTTPS

The switch to HTTPS

Landing Page
source: firefox-console-errors
1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. /en-US/docs/Web/Security/Same-origin_policy

* MDN Google Analytics: Pageviews in /en-US/docs/Web/Security from utm_medium=firefox-console-errors

The switch to HTTPS

It’s getting easier to obtain free certificates

https://certbot.eff.org/

Secure Connections

So I just need to turn on HTTPS?

Mixed Content

Landing Page
source: firefox-console-errors
1. /en-US/docs/Web/Security/Mixed_content
2. /en-US/docs/Web/Security/Insecure_passwords
3. /en-US/docs/Web/Security/Weak_Signature_Algorithm
4. /en-US/docs/Web/Security/Mixed_content/How_to_fix_website_with_mixed_content
5. /en-US/docs/Web/Security/Securing_your_site/Turning_off_form_autocompletion
6. /en-US/docs/Web/Security/Same-origin_policy

* MDN Google Analytics: Pageviews in /en-US/docs/Web/Security from utm_medium=firefox-console-errors

Mixed Content

Mixed Passive Content (The bad kind)

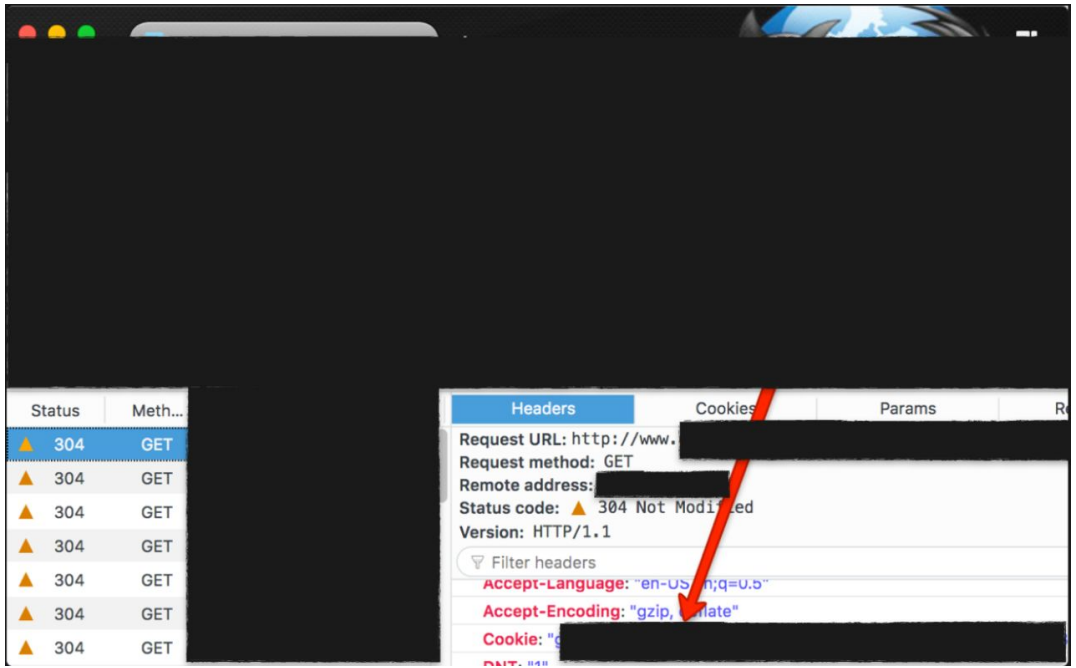
Mixed Active Content (The really bad kind)

<script src="http://example.com/script.js"></script>

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

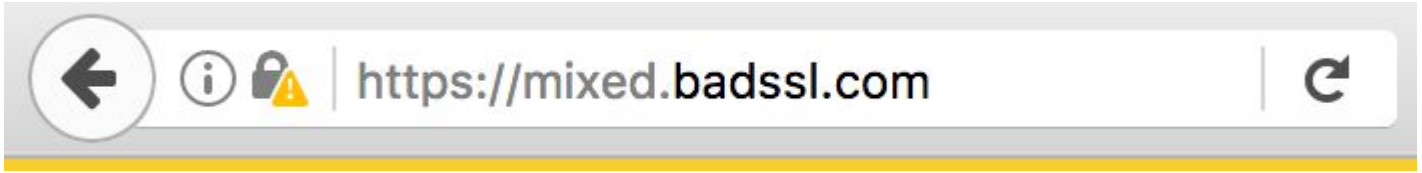
Mixed Passive Content - Session Snooping

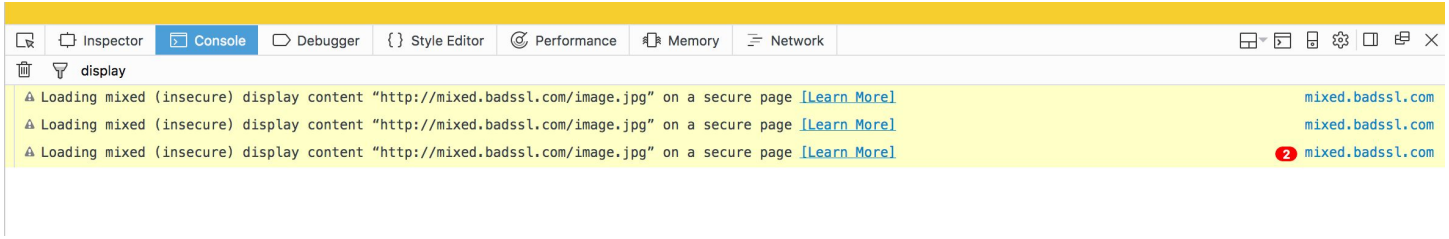
So... mixed passive content is fine, right? Nope.



By Luke Crouch (@groovecoder)

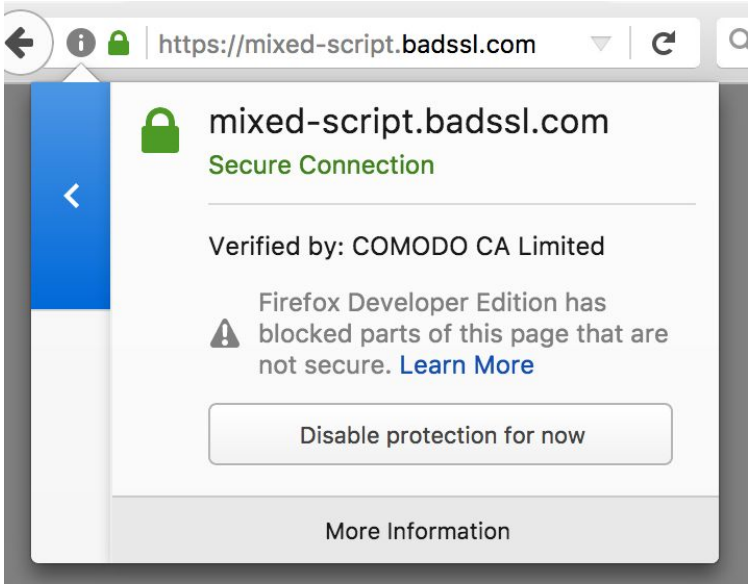
Mixed Passive Content





Mixed Active Content

Browsers block mixed active content by default



Mixed Active Content

Can it alter the DOM?

It's Mixed Active Content (The really bad kind).

Secure Connections

The web is moving to HTTPS, don't be a dinosaur!

Secure Connections

If you've moved to HTTPS (yay), consider turning on the HSTS header

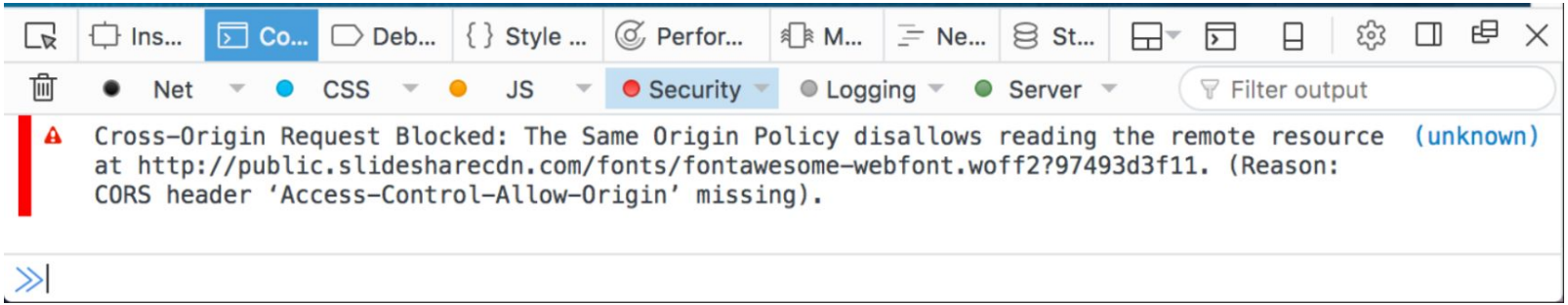
Strict-Transport-Security: max-age=31536000; includeSubDomains

Why? https://moxie.org/software/sslstrip/

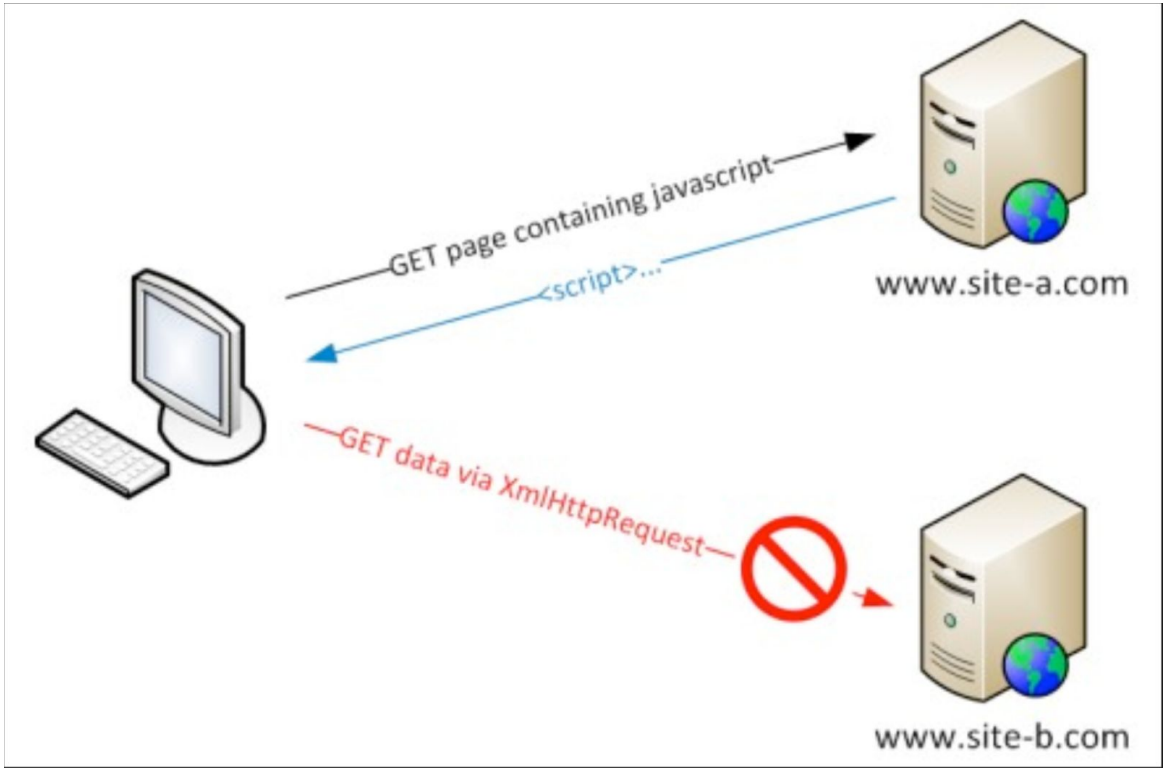
moz://a

Secure Web Content

Same-Origin Policy



Same-Origin Policy



Secure Web Content

What is affected by Same-Origin Policy?

- XHR requests
- window.opener/window.parent, etc.
  - https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

Secure Web Content

<form method=”Post”>?

Not protected!

Use a CSRF token. Don’t rely on cookies.

Secure Web Content

It's very easy to use

```
Access-Control-Allow-Origin: *
```

to work around this issue. In many cases you should not have to.

Secure Web Content

How can I make sure that user generated content doesn't break my website security?

CSP (+ common sense & sanitization)

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

CSP

A set of rules that define how a site may load resources.

```
<meta http-equiv="Content-Security-Policy" content="default-src 'self'; image-src https:*; child-src 'none';">
```

You can use **Content-Security-Policy-Report-Only** to test it without breaking things

CSP

CSP features recording violations!

```
Content-Security-Policy: default-src https:;
report-uri https://report.example.com
```

You can set up endpoints at https://report-uri.io/

Secure Web Content

How can I make sure that the third-party content I receive has not changed on the server?

Subresource Integrity

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Subresource Integrity

Specify an integrity attribute that is the hash digest of the referenced file.

```
<script src="https://example.com/example-framework.js"
        integrity="sha384-oqVuAfXRK...234234234"
        crossorigin="anonymous"></script>
```

https://www.srihash.org/

moz://a

Secure Device Access

Secure Device Access

The web is getting more native capabilities...

Secure Device Access

… but we can’t let websites access them without permission.

Secure Device Access

The web platform was not built with a permission system in mind.

"User agents must acquire permission through a user interface"

https://dev.w3.org/geo/api/spec-source.html

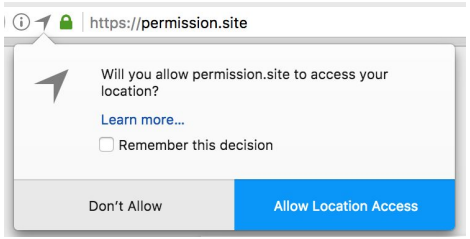
Secure Device Access

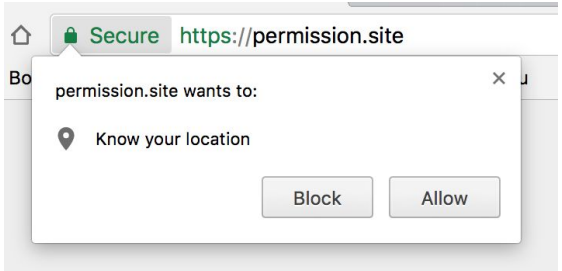
Requesting permission

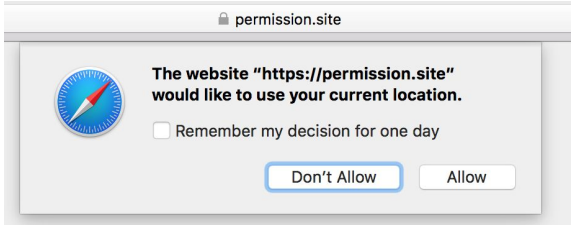
```
navigator.mediaDevices.getUserMedia({audio:
true}).then(stream => ...);


Notification.requestPermission().then(result => ...);


navigator.geolocation.getCurrentPosition(result => ...);
```

Secure Device Access

Different prompts from browsers.







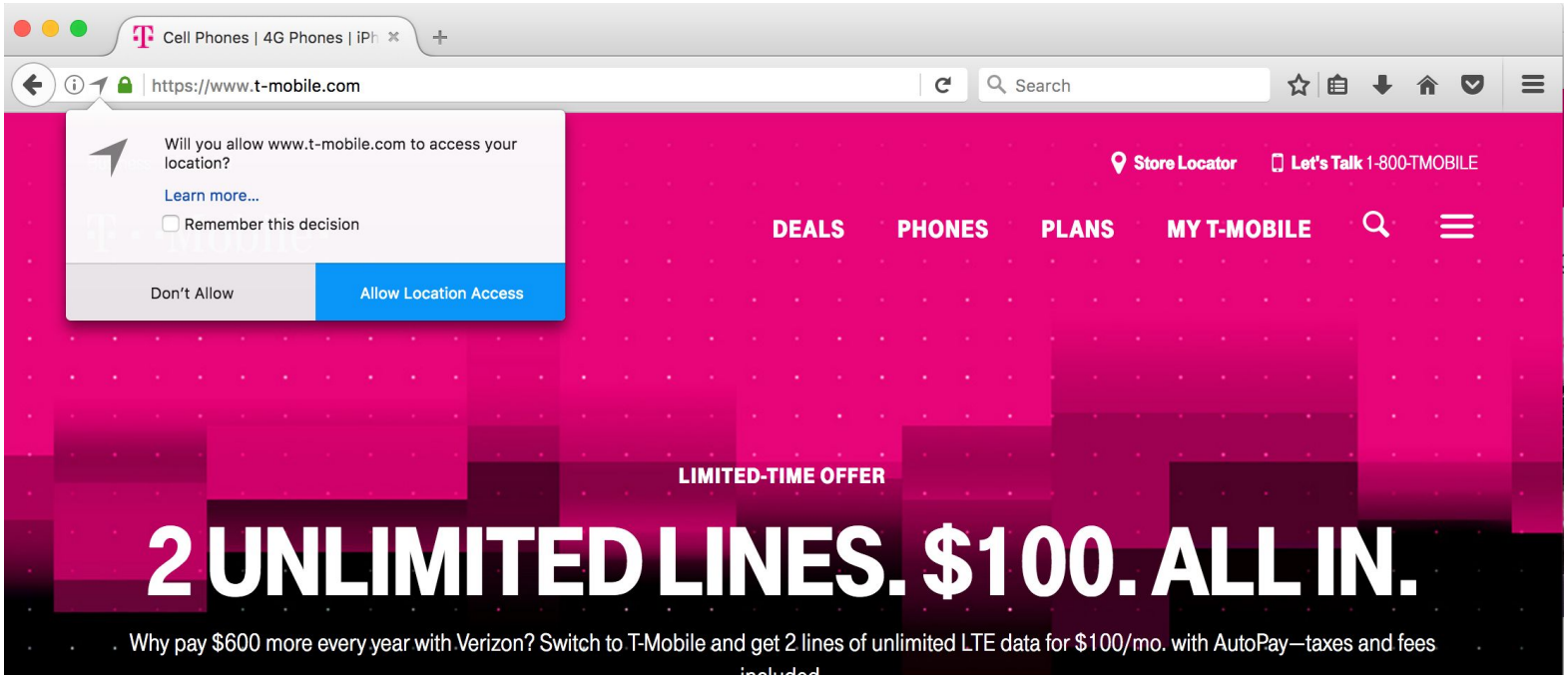
Secure Device Access

Browsers will start to penalize intrusive and surprising permission prompts.

https://bugzilla.mozilla.org/show_bug.cgi?id=1206232

https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/fHI9GNxPPpA/VwhB6h5cDwAJ

Secure Device Access

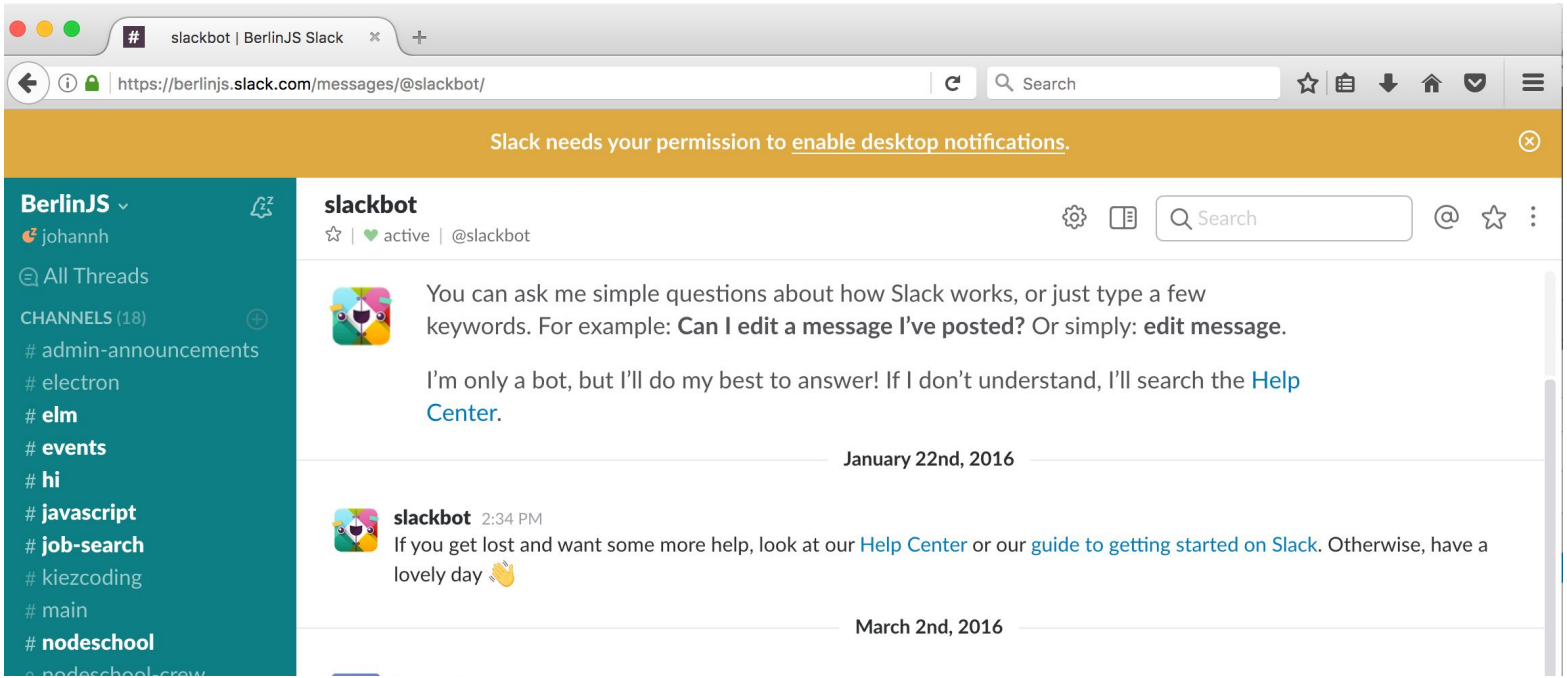


Secure Device Access

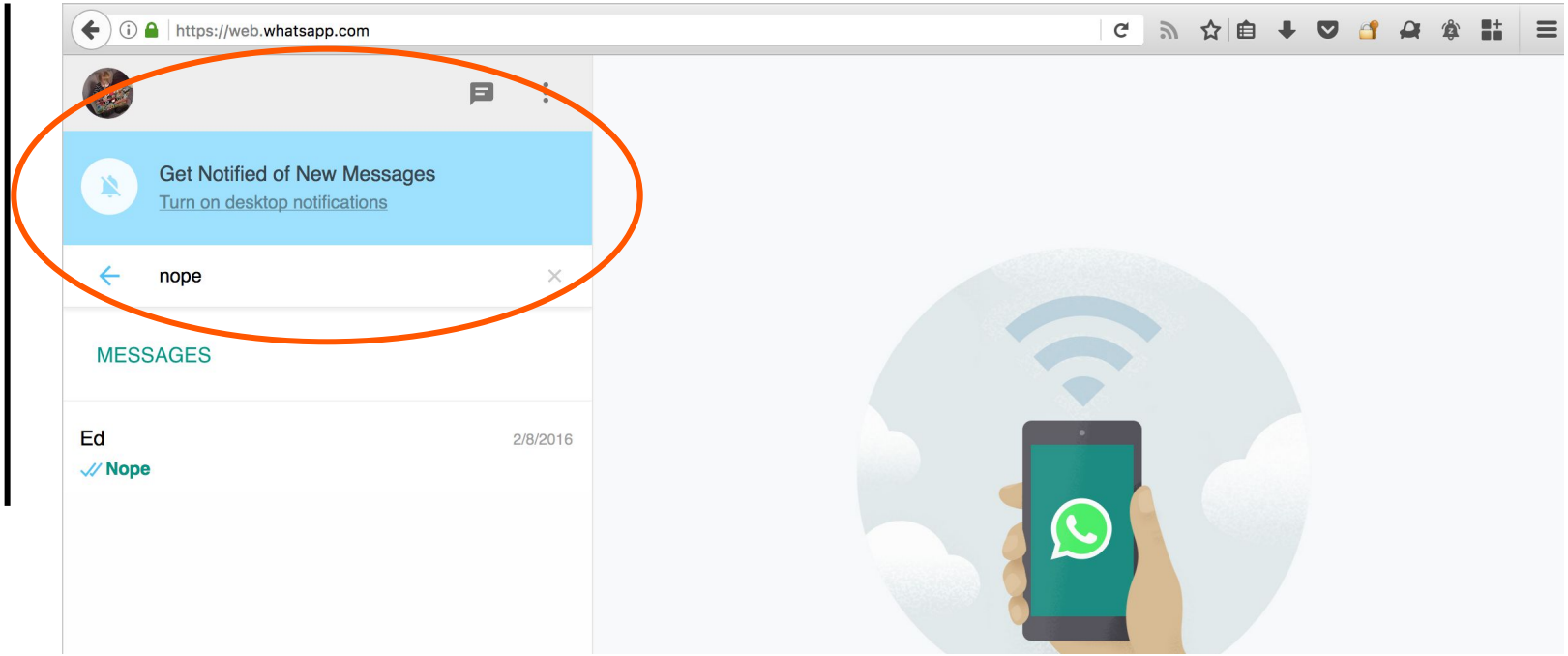
Pre-prompt to give the user context and avoid the element of surprise.

(Browsers might actually force you to do that at some point)

Secure Device Access



Secure Device Access



Secure Device Access

Soon:

Browsers will start to restrict web permissions from iframes

https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/n37ij1E_1aY/JA-1R_pJDwAJ

Secure Device Access

With great power...

Secure websites

Secure Connections

- HTTPS All the Things!
- Take care of mixed content
- Set an HSTS header

Secure Web Content

- Embrace Cross-Origin restrictions
- Have a CSP
- Use Subresource Integrity

Secure Access to Device Capabilities

- Don’t prompt from iframes or HTTP
- Pre-prompt to give the user context

Thanks!

Johann Hofmann

Twitter @johannh

GitHub @johannhof

Website johannh.me

Questions