Creating a more intuitive method of displaying secure sites to Internet users

Chris Bailey, VP Trust Services

F2F CA/Browser Forum meeting – Bratislava   20 February 2020

Entrust Datacard™

What’s the purpose of the Forum?

Bylaws 1.1 - Purpose of the Forum

“Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for best practices as a way of

- [1] providing a heightened security for Internet transactions and
- [2] **creating a more <u>intuitive</u> method of displaying <u>secure</u> sites to Internet users**.”

We’ve done a lot on #1, but nothing on #2

Copyright Entrust Datacard

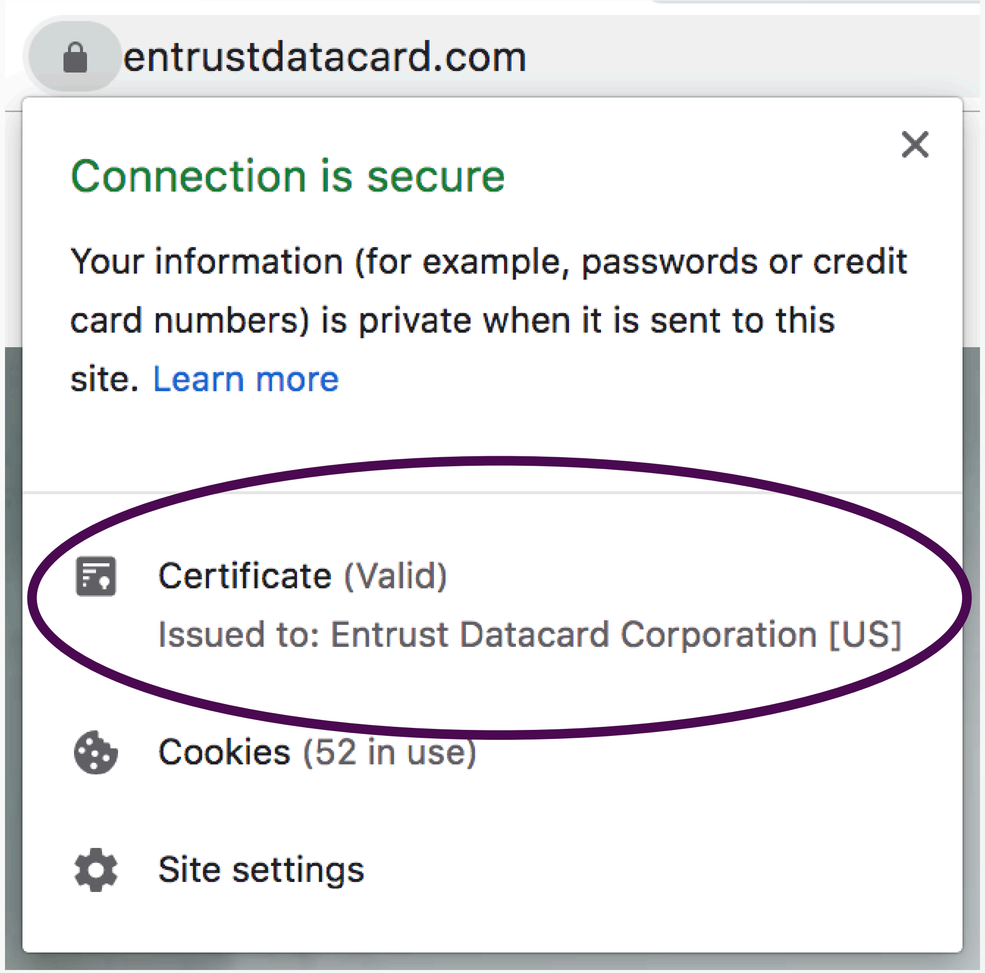
What is the purpose of website security indicators

"Browsers use security indicators to communicate connection *[1] security states*, *[2] website trustworthiness*, or a combination of the two."[1]

How can we make this easy and intuitive for users?

[1] Source: "Rethinking Connection Security Indicators" Authors: Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, Google; Christopher Thompson, University of California, Berkeley; Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo, Google

Recap – Extended Validation UI on or after (Chrome 77) – Organization identity found on second page after user clicks the lock symbol



entrustdatacard.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Issued to: Entrust Datacard Corporation [US]

Cookies (52 in use)

Site settings

This is not an intuitive way to display secure sites with EV to Internet users

1. No EV information in the URL Bar and no standardized way to show EV information in the URL Bar. **All website look the same**.
2. No intuitive or standard way to look up EV identity data

Why did the browsers remove the EV / QWAC distinct UI?

1. Users don’t look at it
2. Browser need the space in the URL bar

Can we address these issues?

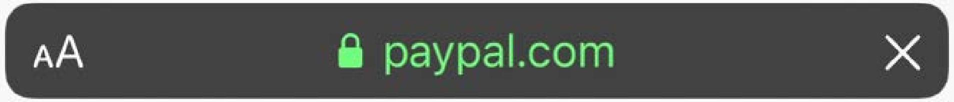
One way to make things *intuitive* is to *standardize*

The STOP sign was Internationally standardized in 1968 via the Vienna Convention on Road Signs and Signals – current octagonal red around the world.

Today the stop sign is so intuitive that most children know what a stop sign means

Recap of Next Steps

- Create a “straw person” set of recommended browser/app UX/UI elements (to generate the most response, pro and con)
- **Even Apple announced that they will be removing the EV UI. Apple’s UI had previously solved a lot of problems.** We believe leveraging Apple’s former UI scheme in the URL Bar for Desktop and Mobile (green lock and green FQDN / DN) is a good start. Then leverage the “click on the lock” for the full identity data in a structured format similar to the “second click” in Firefox.



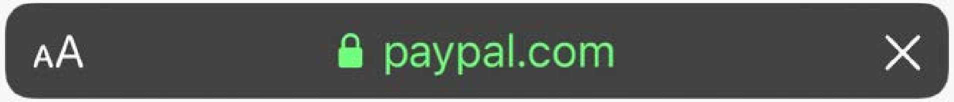
“Straw person” Proposal 1

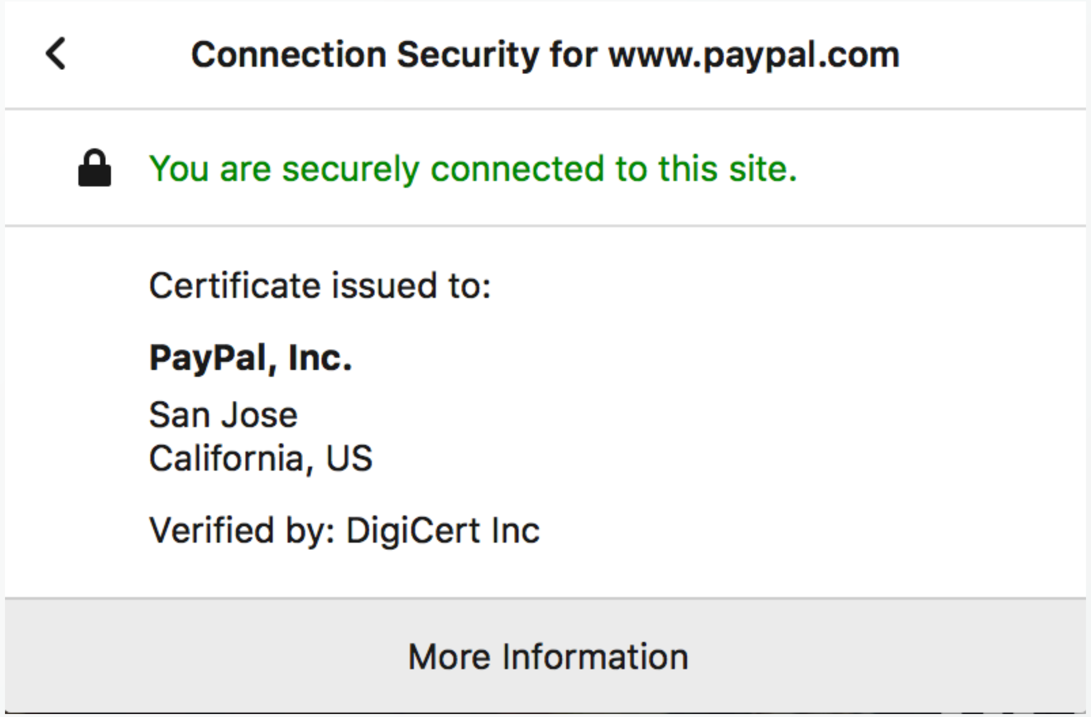
1. Green lock URL Bar text is reserved for Extended Validation

“Straw person” Proposal 1

1. Green lock URL Bar text is reserved for Extended Validation

2. Single Click on lock, shows identity information in a server certificate




Connection Security for www.paypal.com

You are securely connected to this site.

Certificate issued to:

PayPal, Inc.

San Jose
California, US

Verified by: DigiCert Inc

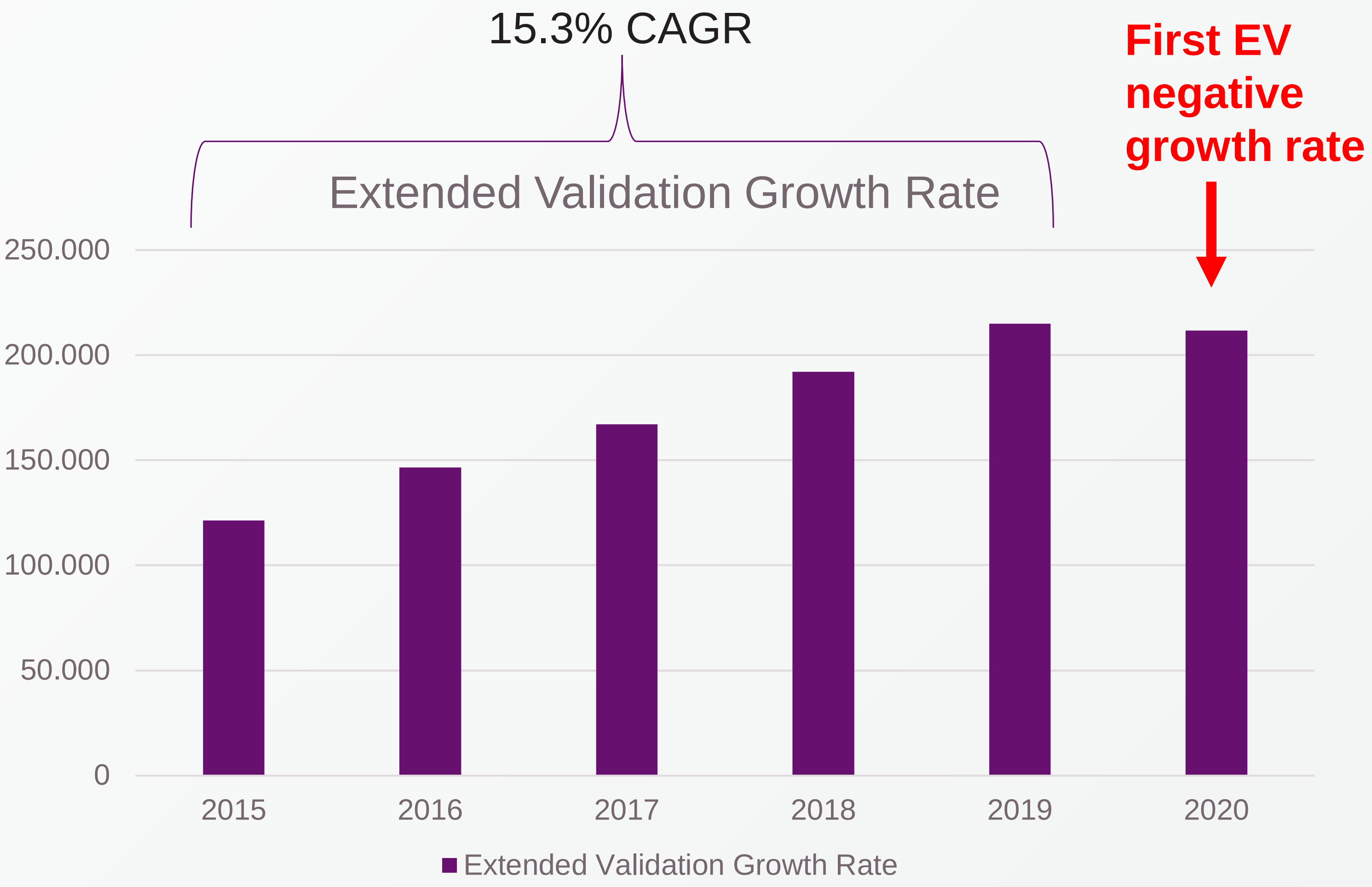
This Addresses Browser concerns

This design moves the conversation forward on addressing the two major concerns.

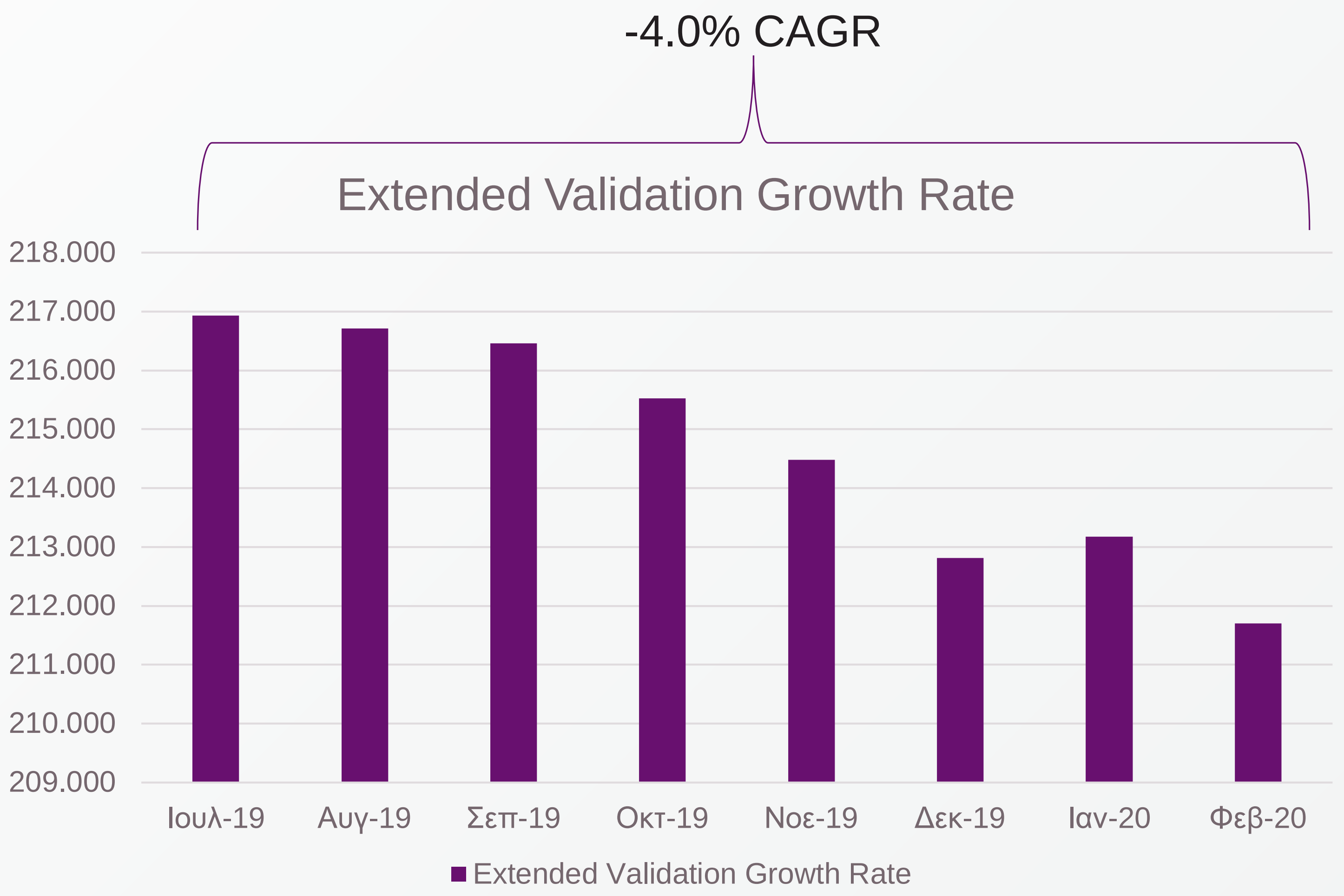
- Users don’t look at it
  – Standardizing UI, makes things much easier to learn

- Browser need the space in the URL bar
  – Uses the same amount of space in the current URL Bar

Since the Extended Validation / QWAC UI has been removed, the incentive for high assurance identification has dropped



Since the Google and Mozilla announcement to remove the EV / QWAC UI the Annual Growth Rate for EV certs is now -4%.



-4.0% CAGR

This decline will likely accelerate with Apple’s announcement to remove the EV UI.

New ideas on intuitive UI based on *existing* user research and security indicators – plus, GDPR and transparency

Protecting User Privacy (Data) is paramount –

GDPR applies

Additional requirements apply to websites – including protecting user privacy and their data. GDPR Article 5 mandates:

***Article 5* - Principles relating to processing of personal data**

1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’); ***

2. The controller [of a data collecting site] shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Fraudulent sites and their lack of a “Controller” violate this core GDPR principle when they collect and mis-use personal data from browser users.

What is the "Transparency" as required by GDPR?

What is transparency?

"Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start **about who you are**, and how and why you use their personal data.

"Transparency is always important, but especially in situations where individuals *have a **choice** about whether they wish to enter into a relationship with you*. If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship."

UK Information Commissioner's Office "Guide to the GDPR"
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Phishing Sites and Anonymity

- Anonymous phishing sites that troll for a user's personal data (name, password, credit card) clearly may be violating the GDPR – and have no Controller ensuring compliance
- But without identity data about the website, users and regulators have no "choice" and no recourse for violations
- Users who know a website is anonymous should "have a choice about whether they wish to enter into a relationship with [the website]" before they supply their personal data – how can we inform and empower users?

We can leverage positive and negative warnings to inform users when a website is *anonymous* and is asking for *data*

Google research says users don’t often use positive UI indicators to make security decisions, but are affected by negative UI warnings. Google used this research in its successful plan[1] to transition websites from *http* to *https*, employing a progressive combination of positive (“**Secure**”) and negative (“**Not Secure**”) indicators.

Past UI changes influenced both website owners (the positive indicators) and users (the negative warnings).

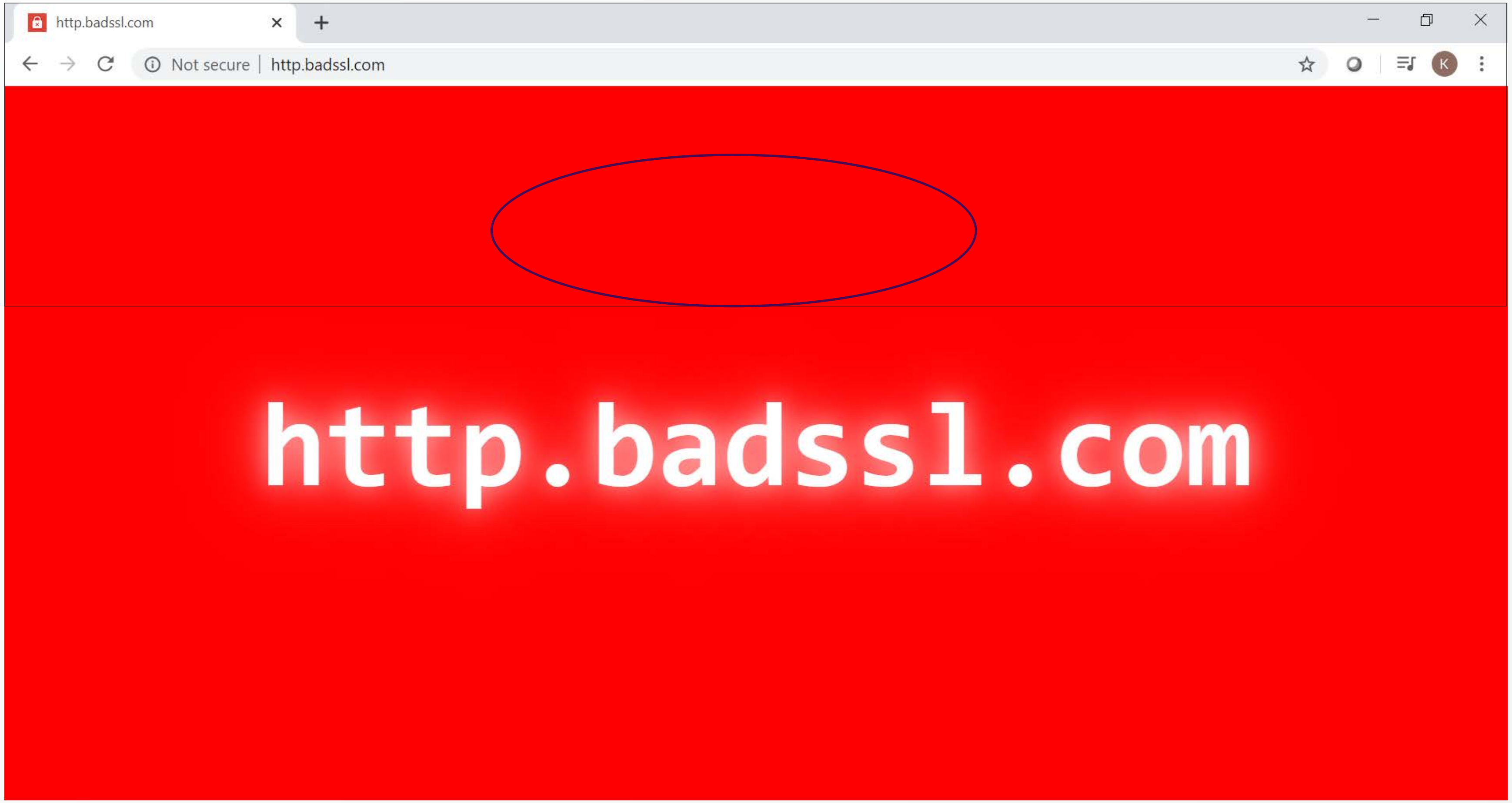
How can we leverage this successful Google experiment?

[1] https://www.usenix.org/conference/usenixsecurity19/presentation/Thompson
https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure
https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

The good news is – the browsers have already shown us how to do this

The website www.badssl.com can be used to test browser behavior and user warnings under different scenarios. Here are the warnings given to users for different types of **http** sites that ask for user data. We can use the same warnings for anonymous sites that ask for user data.

Simple *http* (unencrypted) page warning



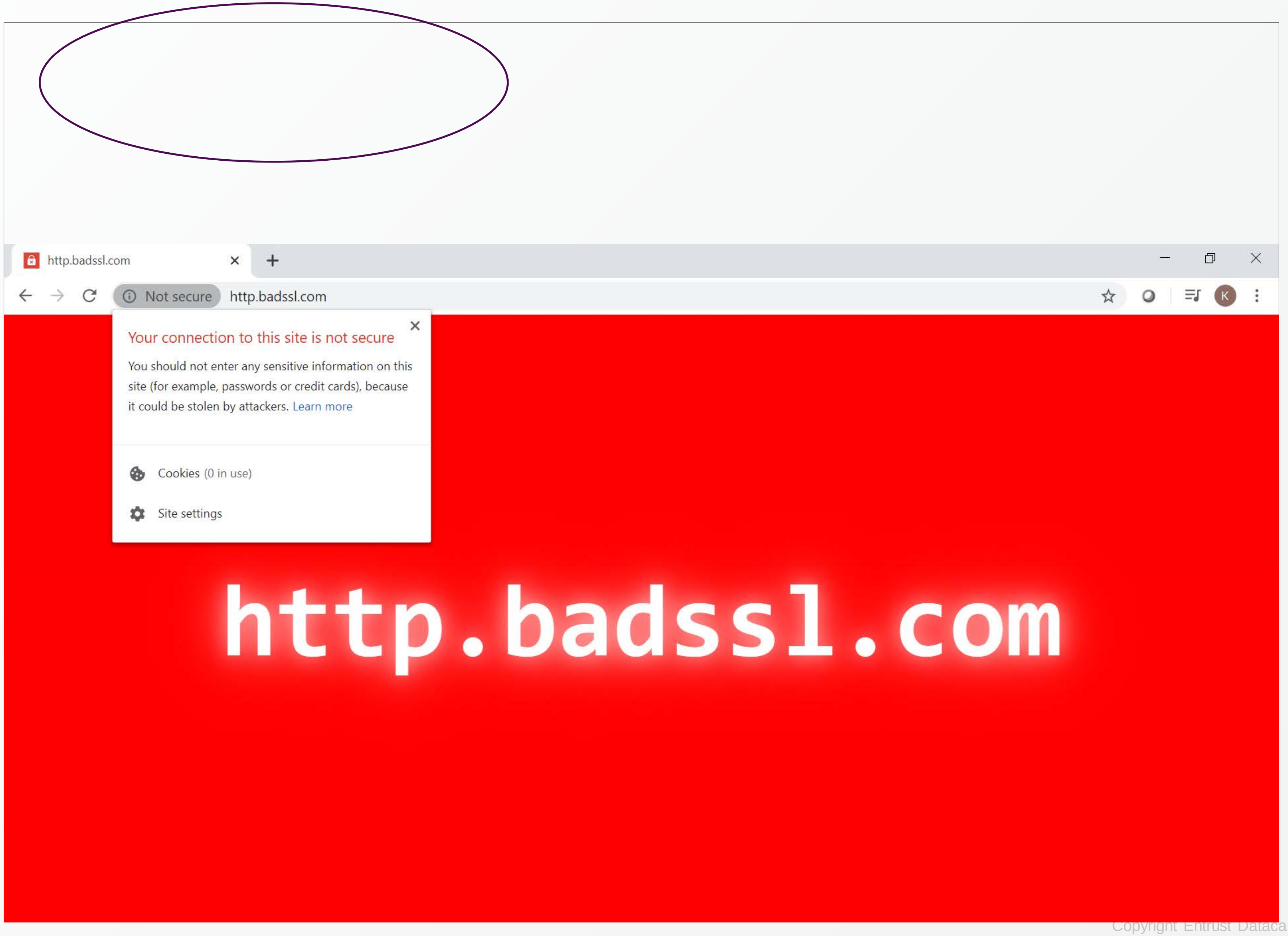
http.badssl.com

Not secure | http.badssl.com

http.badssl.com

http://http.badssl.com/

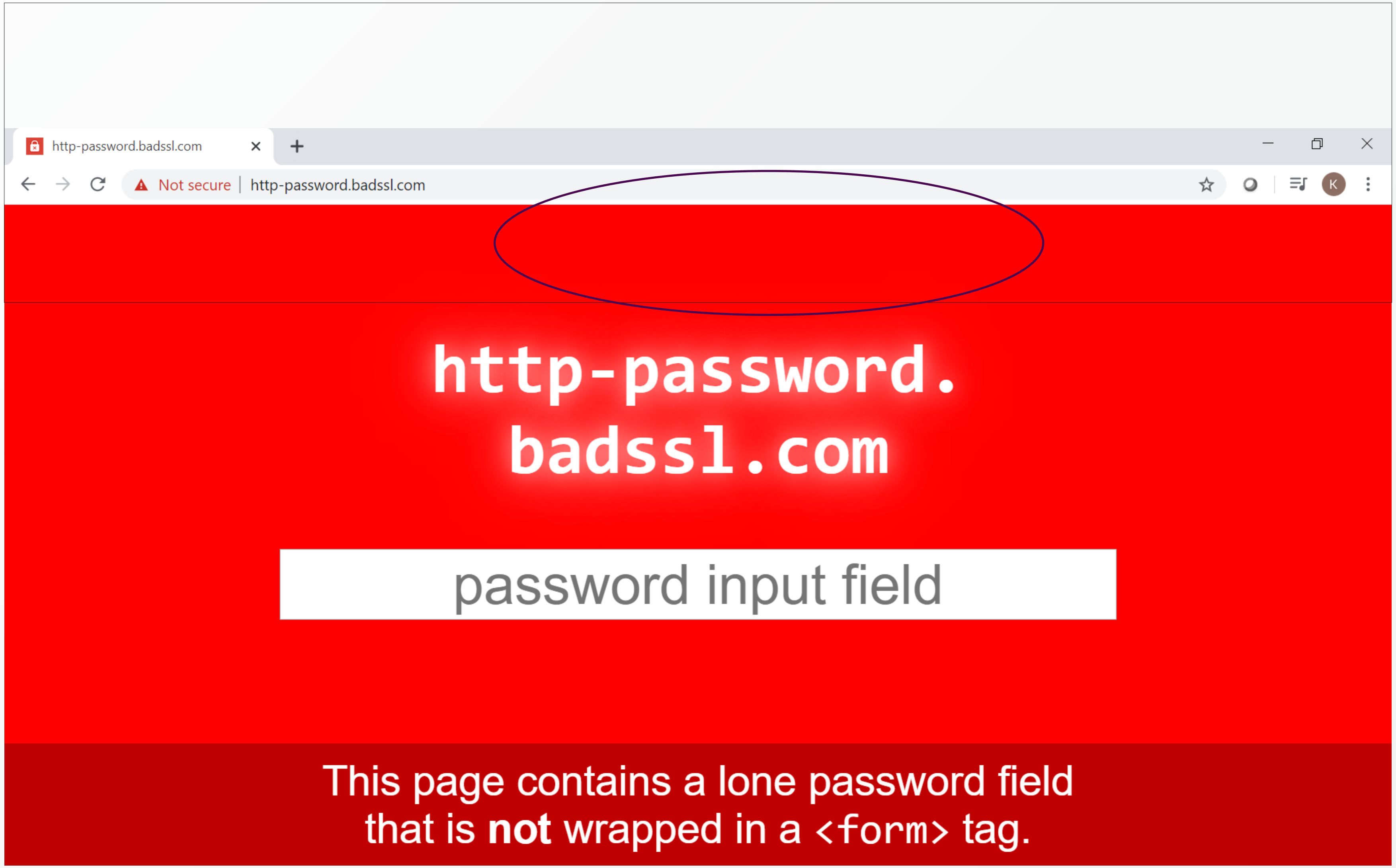
Http page warning – Part 2 A detailed ***warning*** when " Not secure" icon is clicked – *your data could be stolen*



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

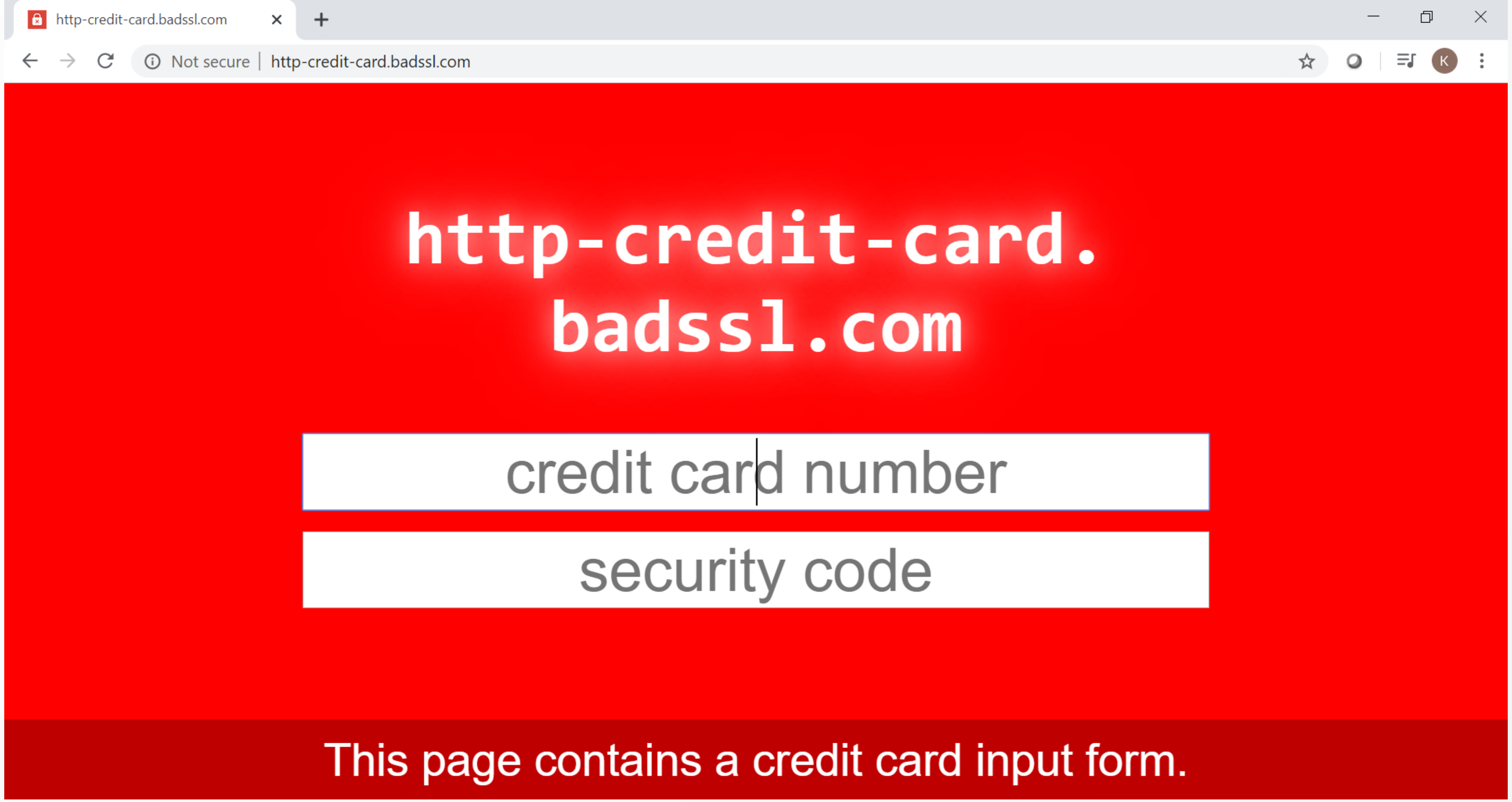
Page with http ***password input field*** – "⚠ Not Secure" warning in address bar (more than simple http warning)



This page contains a lone password field that is **not** wrapped in a `<form>` tag.

http://http-password.badssl.com/

Page with http ***credit card input field*** – Page is actually ***disabled*** when data typed in by user



http-credit-card.badssl.com

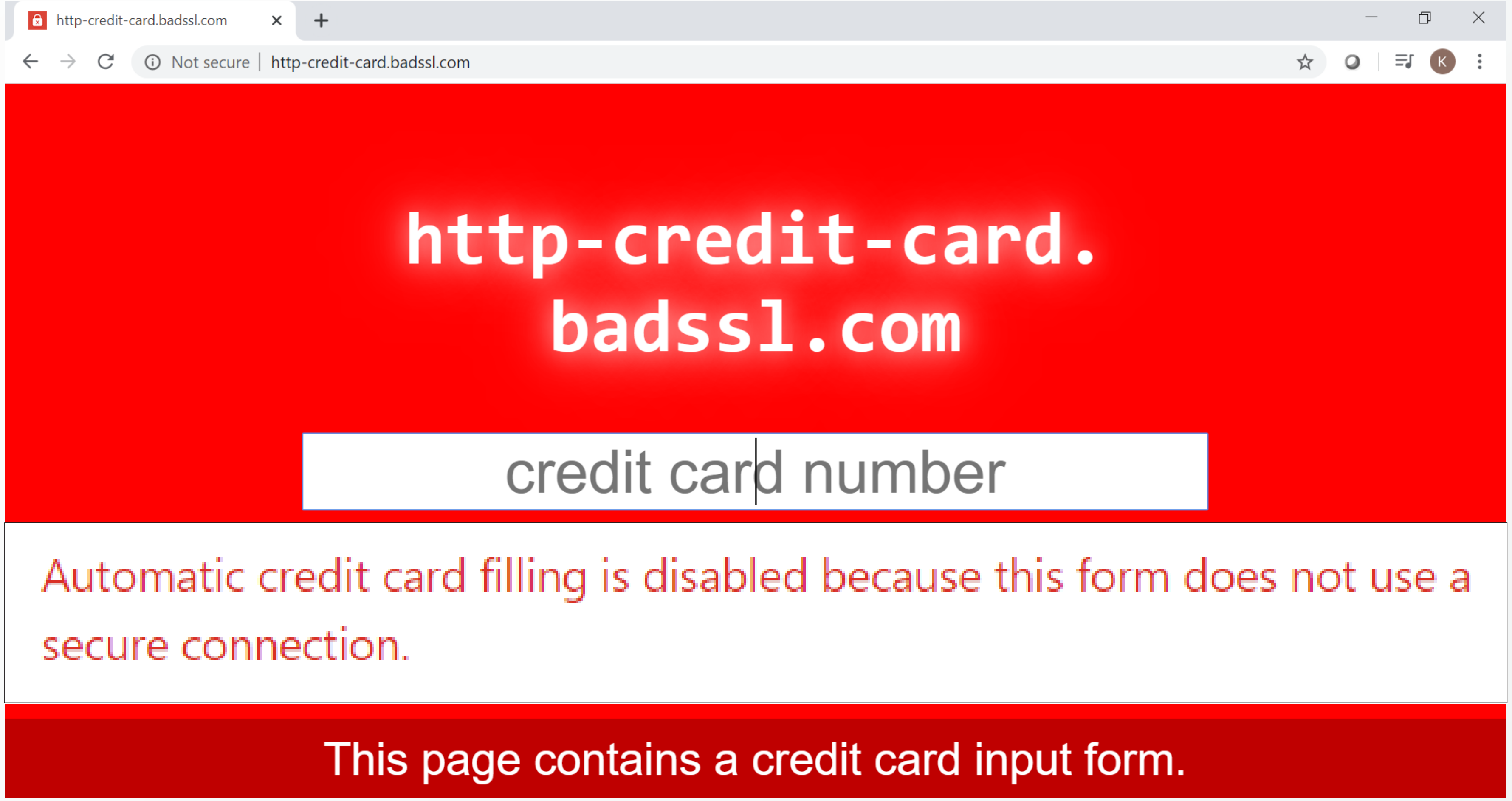
credit card number

security code

This page contains a credit card input form.

http://http-credit-card.badssl.com/

Pop-up warning disables Automatic credit card number typed in by user



http-credit-card.badssl.com

credit card number

Automatic credit card filling is disabled because this form does not use a secure connection.

This page contains a credit card input form.

http://http-credit-card.badssl.com/

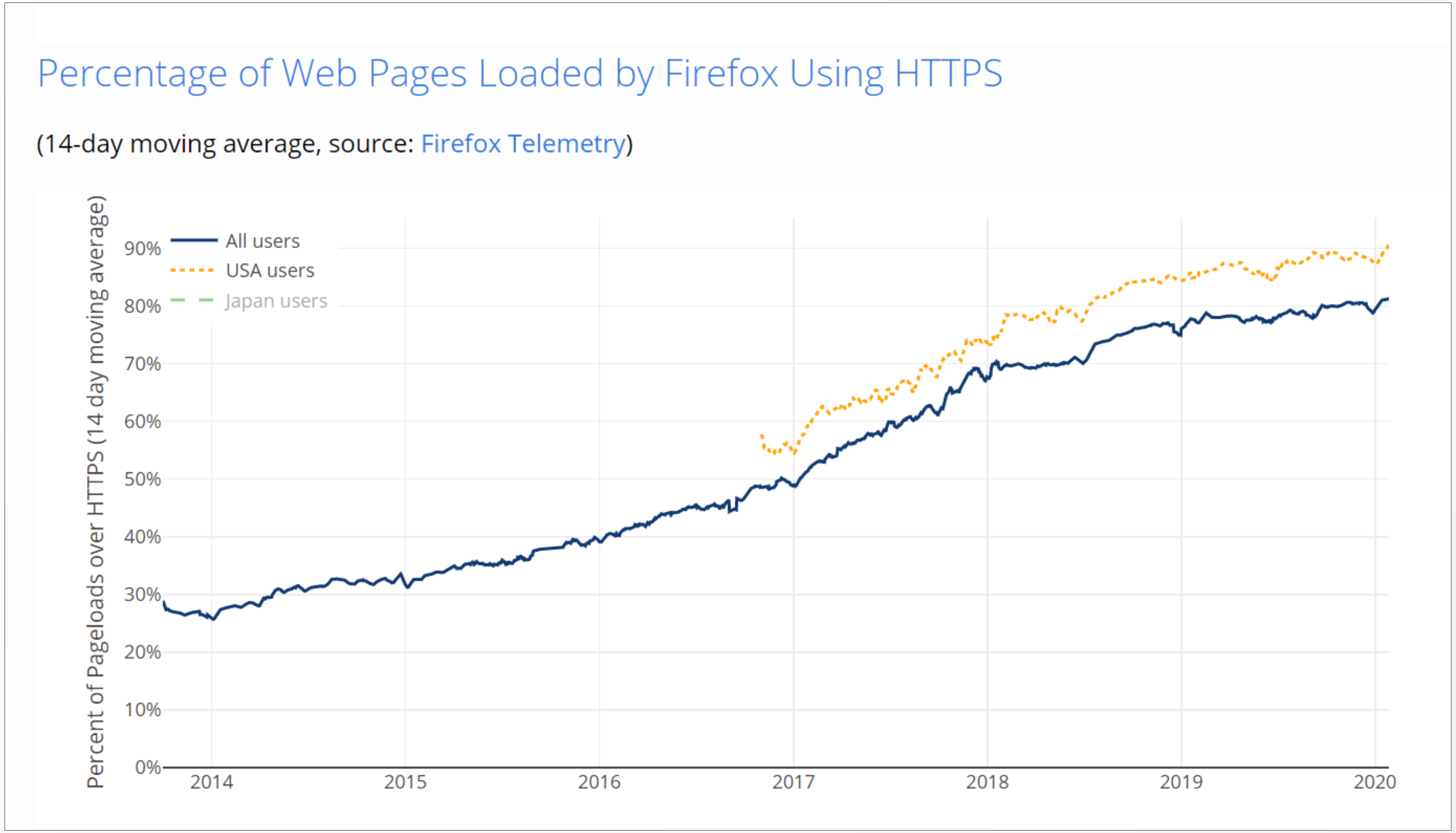
Use progressive warnings for anonymous websites (DV) that ask for user data

- Positive address bar UI for *identity* websites - **green lock symbol with Green DN / FQDN**
- Negative address bar UI information symbols starting with "ⓘ **Not secure**" for anonymous (DV) websites with user warning when *clicked*
- Stronger negative address bar UI information symbols - **red "Not Secure"** if user begins to input data on *anonymous* site page or entering on certain fields (Credit Cards, User Identity, etc…). Maybe users can click "Trust this URL in the future" to avoid future warnings from DV sites asking for data.

But wait - **95%+ of current sites are DV – we can’t show warnings for 95% of the internet!**

- We wouldn’t do this all at once, remember the progressive campaign similar to moving websites from http to https)
- Start with *positive* UI for *identity* sites, simple negative UI “information” for *anonymous* DV sites that ask for user data
- Begin make the warnings *stronger* for anonymous sites that ask for personal data, financial data, healthcare data or other sensitive data.
- Combine with website owner / user education

81% of page loads are now *encrypted in part because of* progressive warnings for http



Source: https://letsencrypt.org/stats/

Conclusion: Gradual use of positive and negative indicators can empower users to decide whether to give data to anonymous *https* sites

- This plan can be accomplished through progressive positive and negative indicators.
- Sites that don’t ask for user data can remain anonymous (DV) without warnings – but may *not* ask for sensitive data (GDPR) without identifying themselves. Minimal site owner / user education needed.
- We would accomplish our Bylaw goal of “creating a *more intuitive method of displaying secure sites* to Internet users” and give users a choice of whether or not to give their data to anonymous DV sites.
- This will inform and empower users so they can make a choice: right now they have no choice

Thank you!

Questions and comments?

Entrust Datacard™

Trusted Identities | Secure Transactions