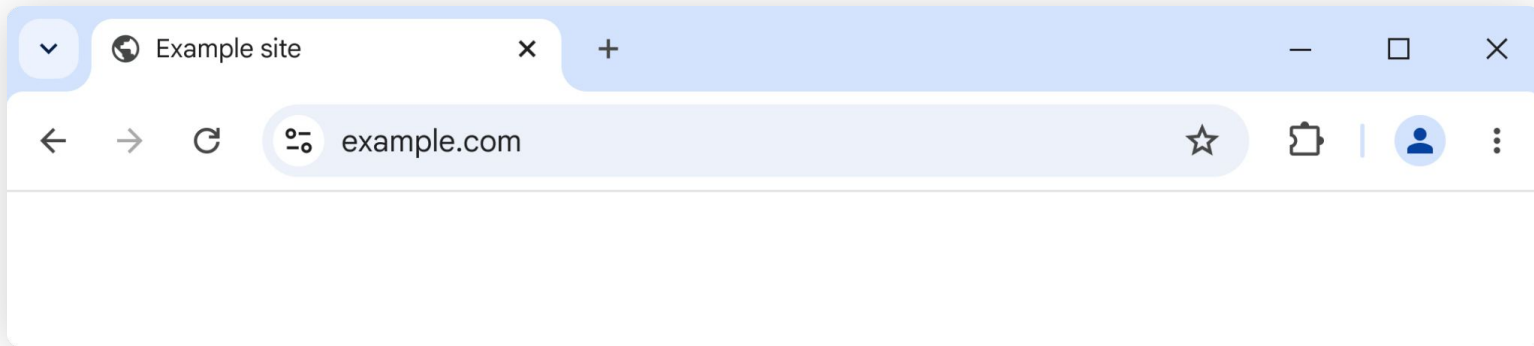
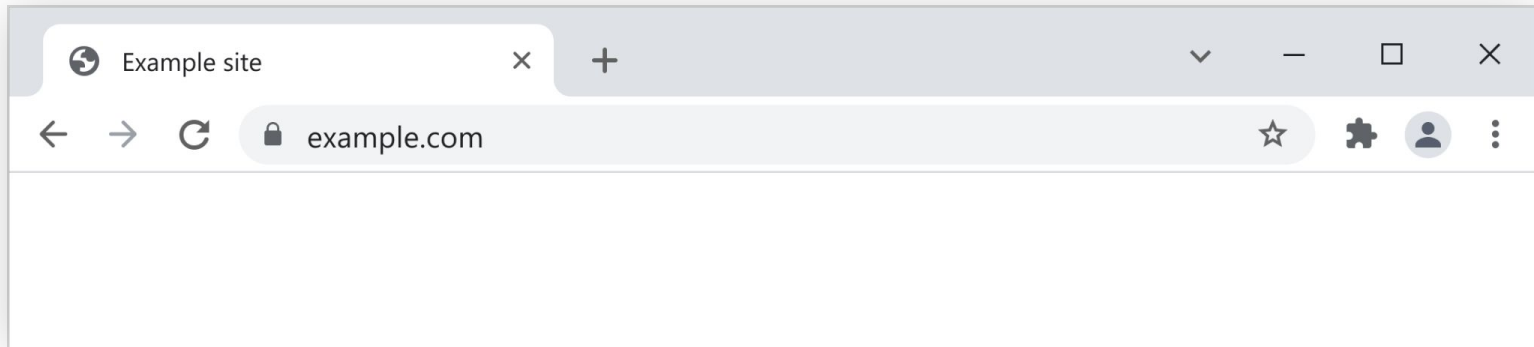
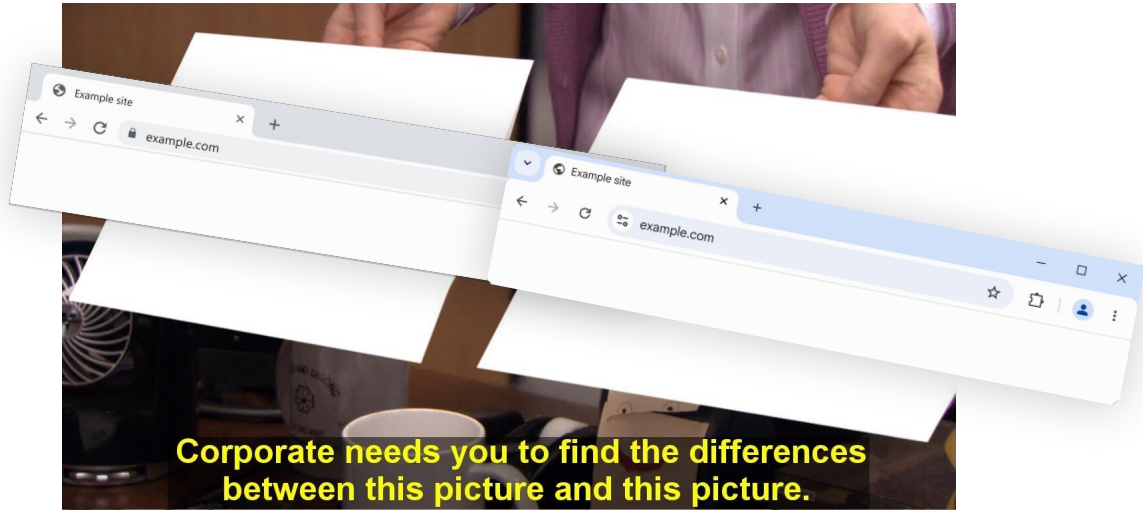


THE YEAR IS 2023...







Example site



example.com

*hmm*

Example site



example.

*hmmmmmm*

2



WAIT WHAT

exam



RIP  
LOCK ICON  
1995-2023



- \* serena
- \* cyber aesthetics doctor
- \* chrome security
- \* pronounces it "owned" not "poned"



I HAVE TRICKED  
THE ORGANISERS  
INTO LETTING ME  
TALK ABOUT AN  
TCON FOR 20 MTNS



1.

WHAT DOES

EVEN

MEAN

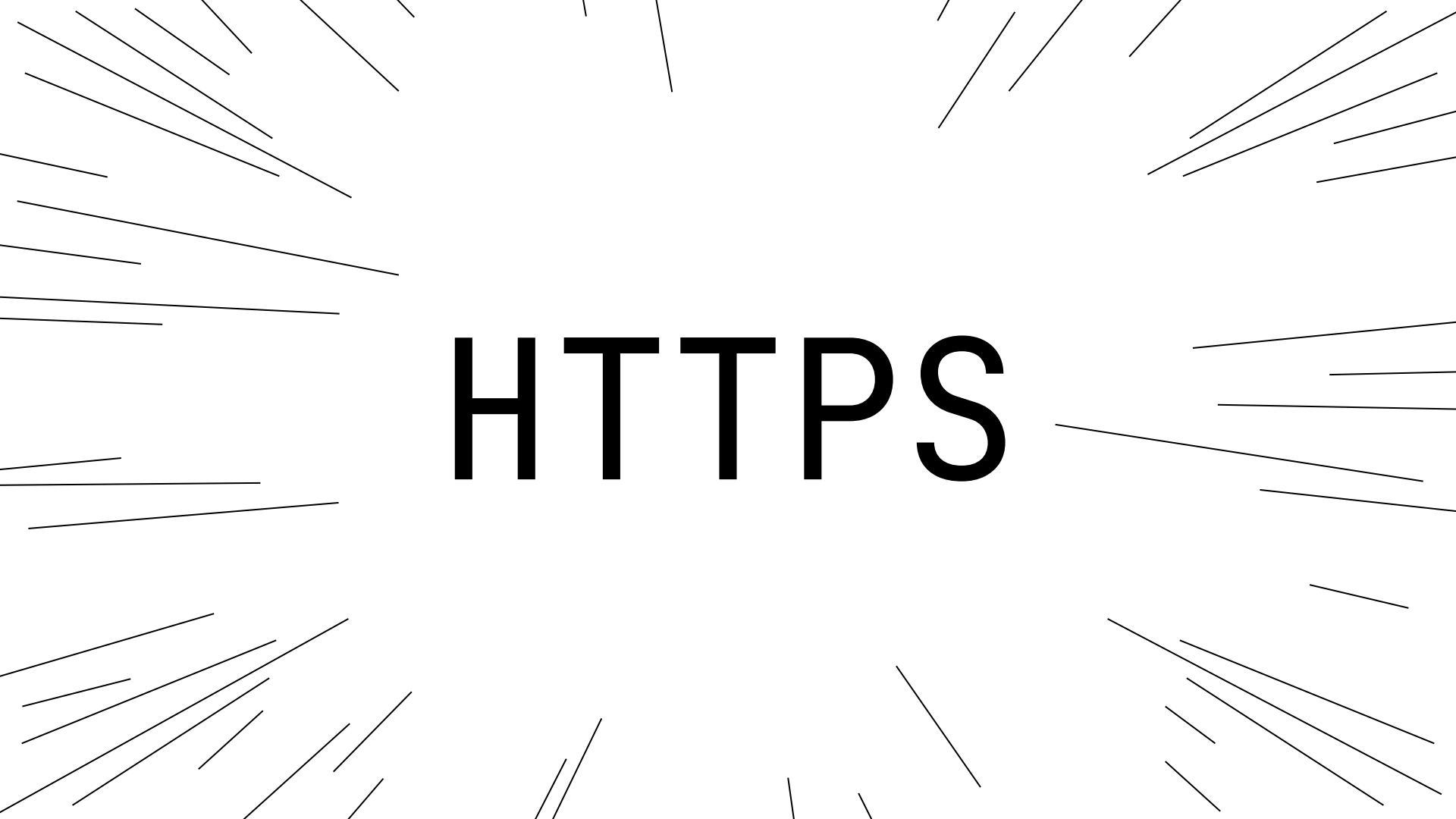




Example site



example.com

The background of the image consists of numerous thin, black, diagonal lines radiating outwards from the center, creating a starburst or sunburst effect. The lines vary in length and angle, filling the white space around the central text.

**HTTPS**

HTTP...*Secure*

Netscape Navigator creates  
HTTPS with SSL v1

it is never released



**1994**

gator creates  
th SSL v1

r released

94

SSL v2 is released

It has a number of  
security flaws

1995

SSL

19



released

number of  
y flaws

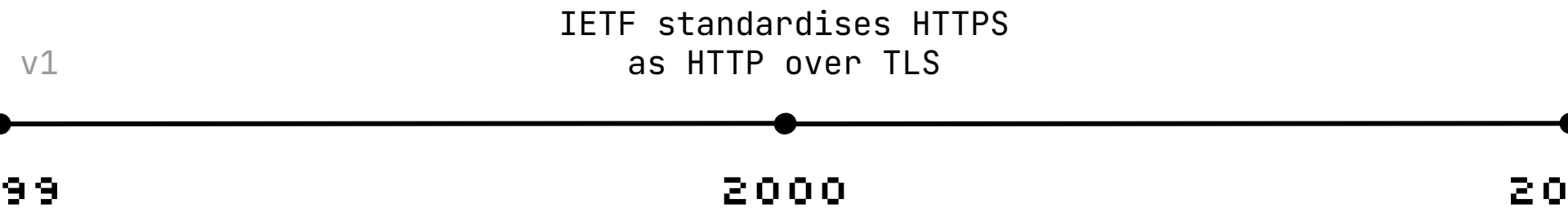
SSL v3

95

1996

19





Adopted HTTPS  
over TLS

2000

2001

2002





03

2004

20

Gmail launches!

It is available over  
HTTPS (wow)





03

2004

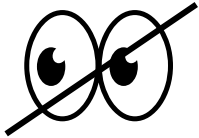
20

Gmail launches!

It is available over  
HTTPS (wow)

# HTTPS means 3 things:

1. Authentication

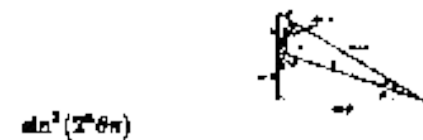
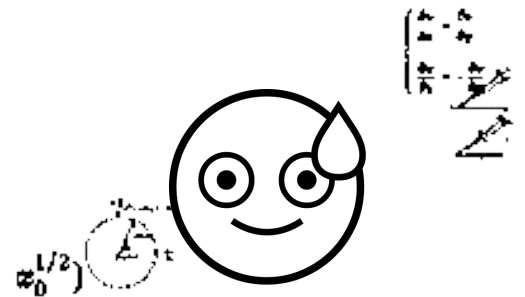
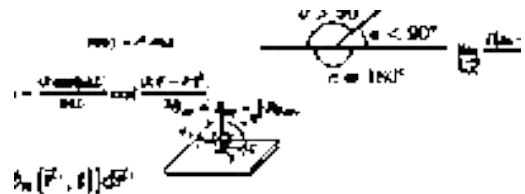


2. Encryption

3. Data integrity

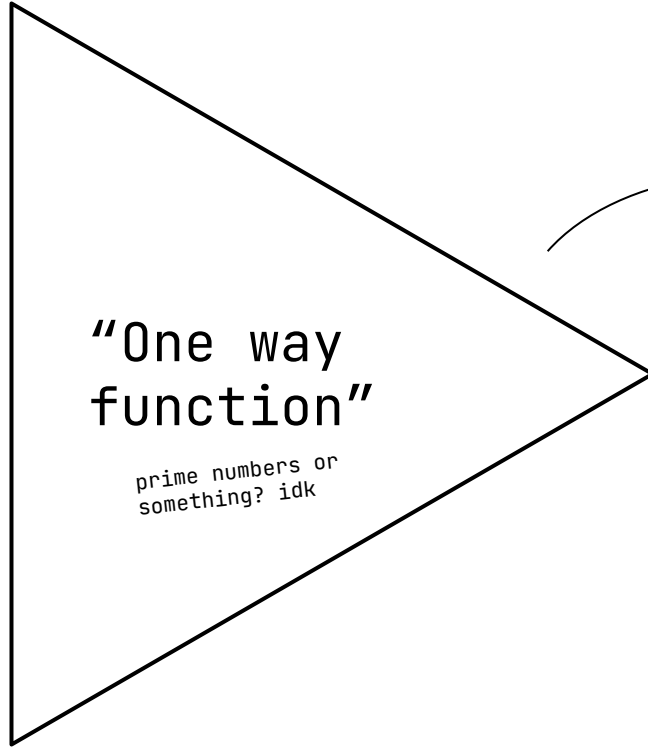
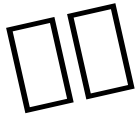


# PUBLIC KEY CRYPTOGRAPHY

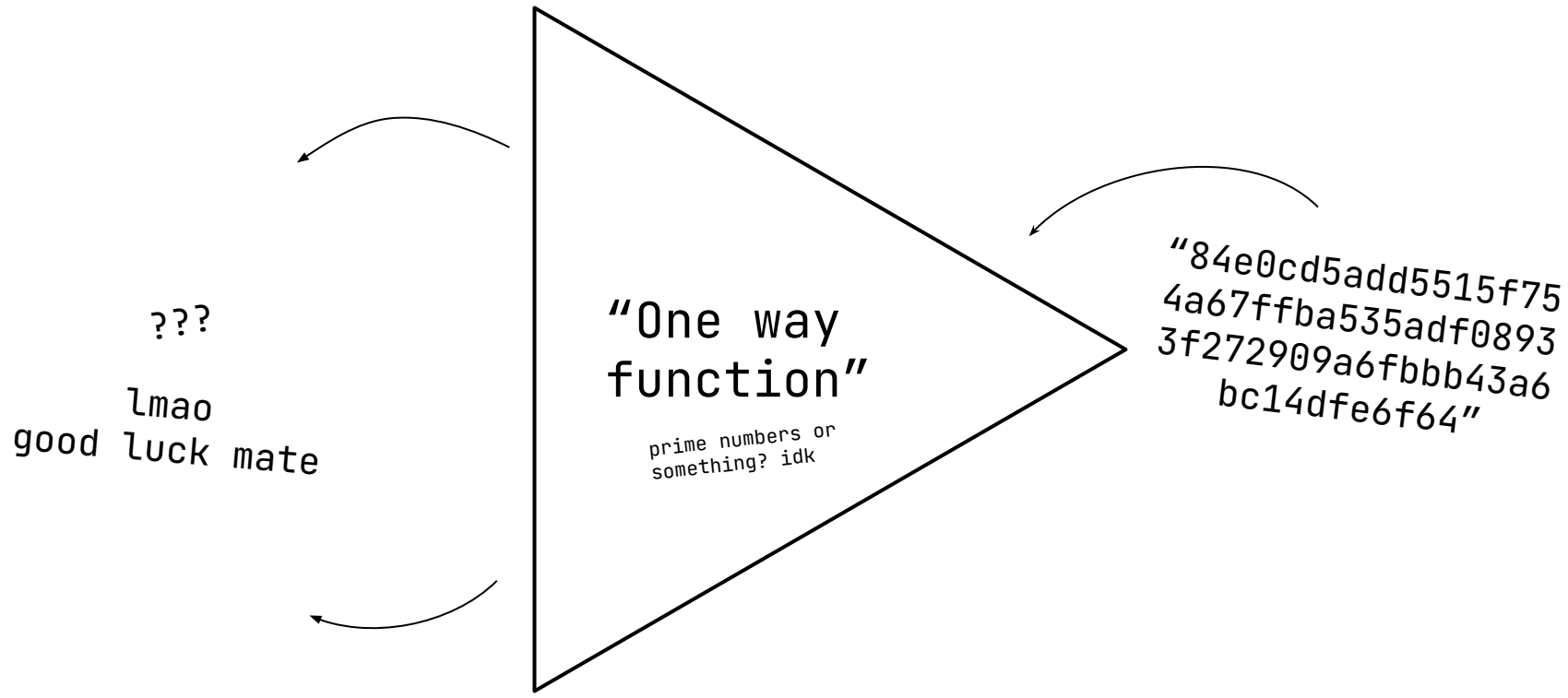




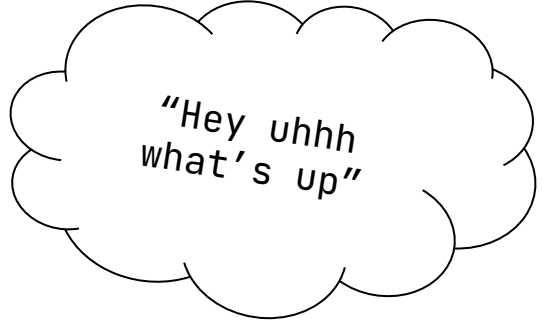
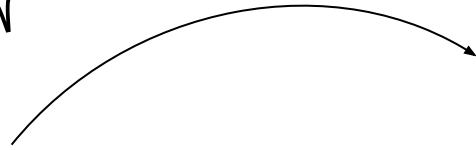
"Hey uhhh  
what's up"



"84e0cd5add5515f75  
4a67ffba535adf0893  
3f272909a6fbbb43a6  
bc14dfe6f64"

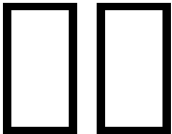


Private Key

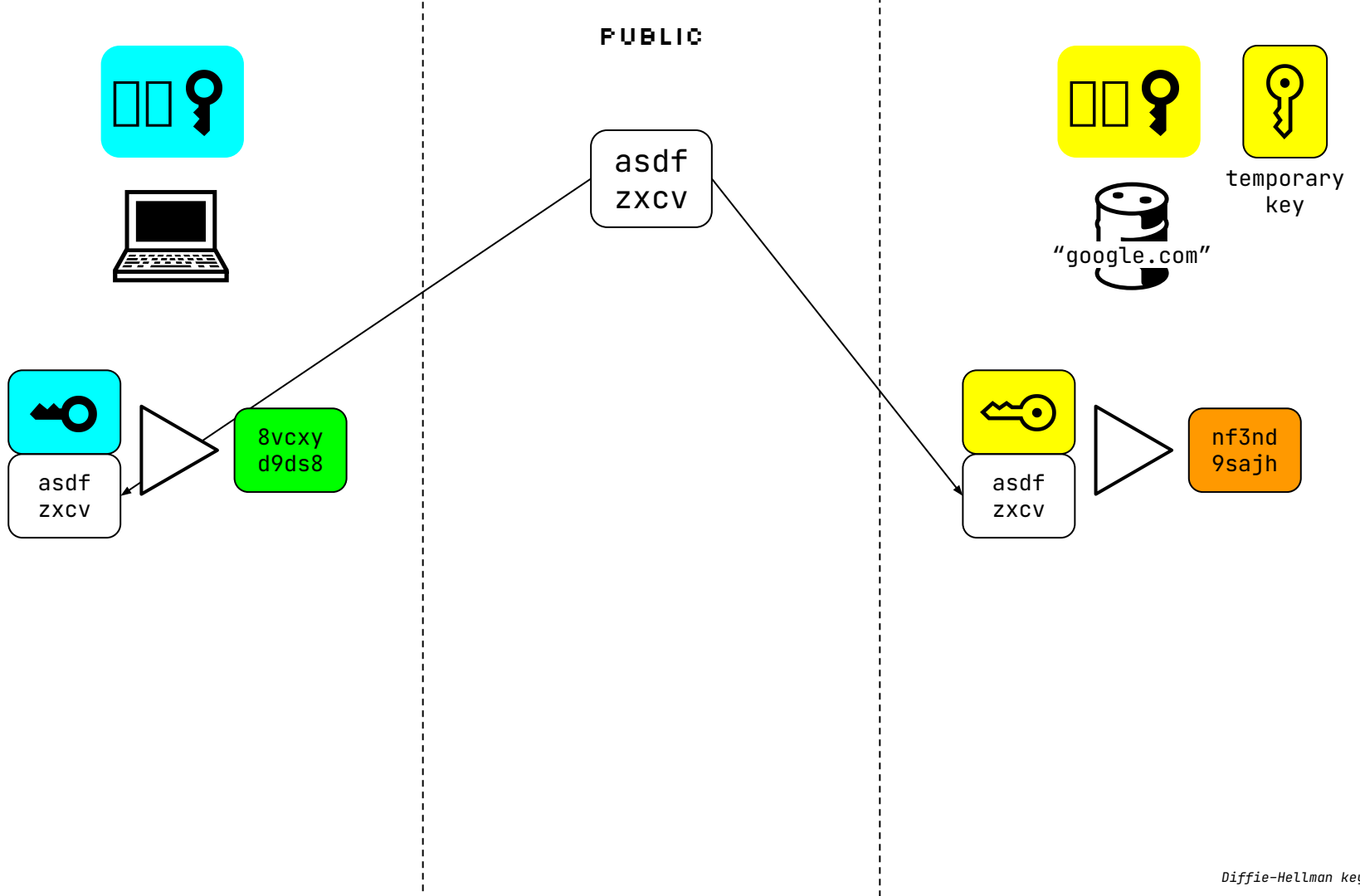


Unless ... 😊

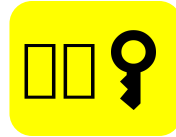
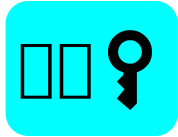
Public key



Private key



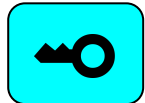
PUBLIC



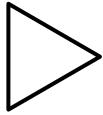
temporary key



asdf  
Zxcv



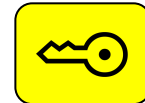
asdf  
Zxcv



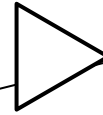
8vcxy  
d9ds8

8vcxy  
d9ds8

nf3nd  
9sajh



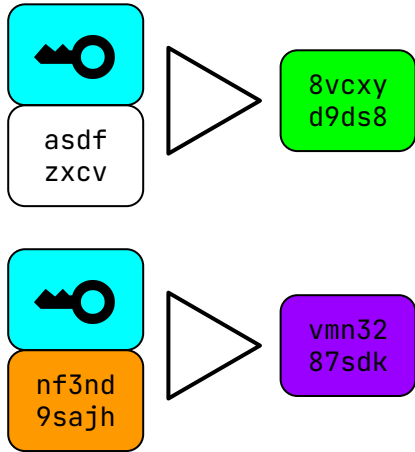
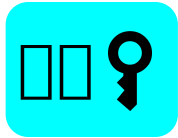
asdf  
Zxcv



nf3nd  
9sajh

nf3nd  
9sajh

8vcxy  
d9ds8

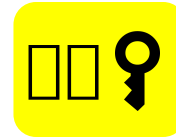


PUBLIC

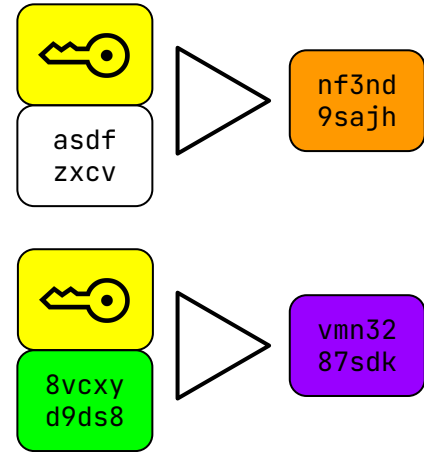
asdf  
ZXCv

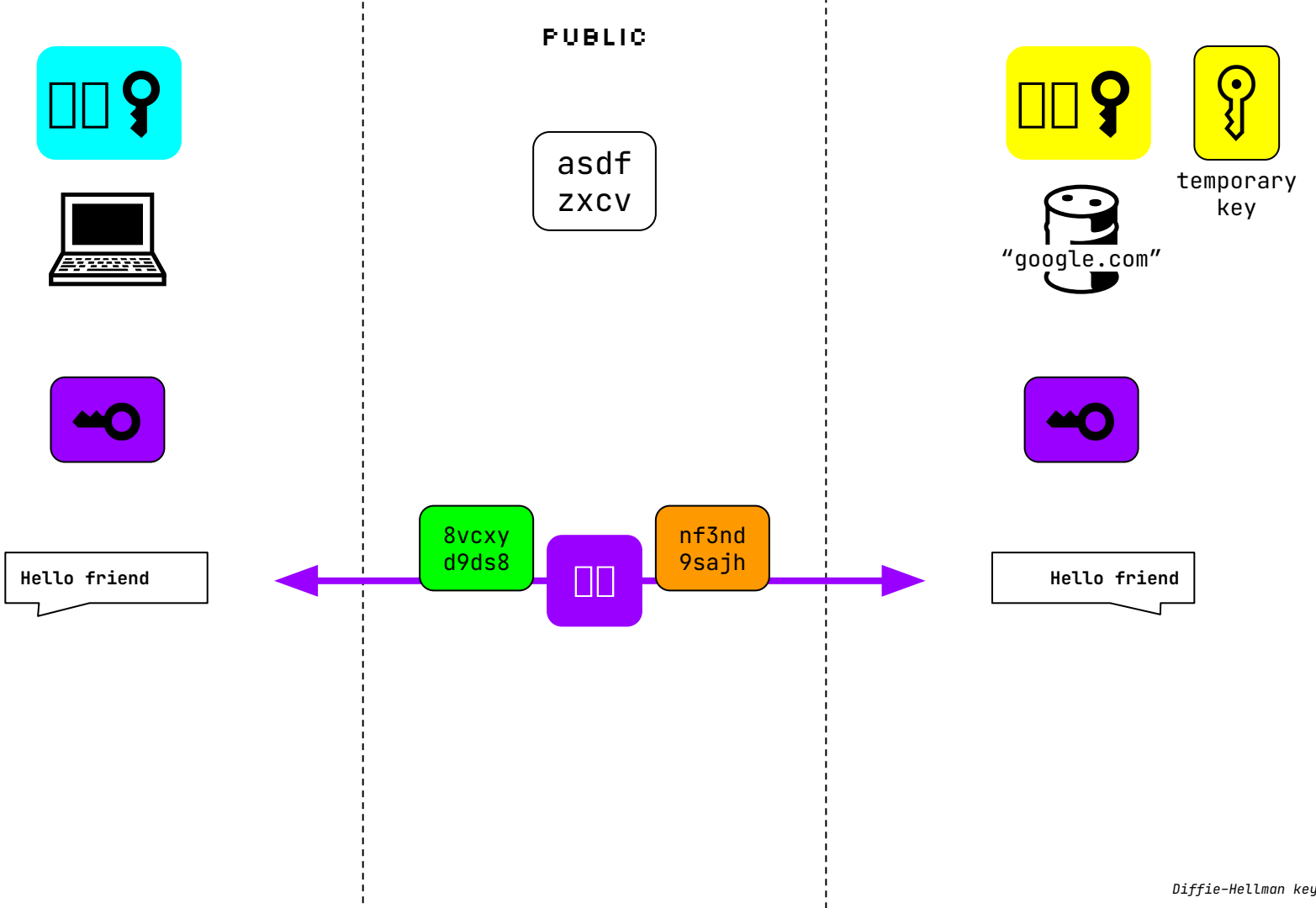
8vcxy  
d9ds8

nf3nd  
9sajh



temporary  
key





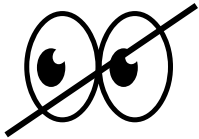


# HTTPS means 3 things:

1. Authentication

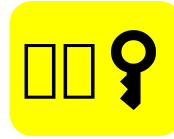
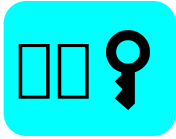


2. Encryption  

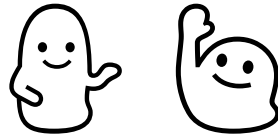


3. Data integrity  

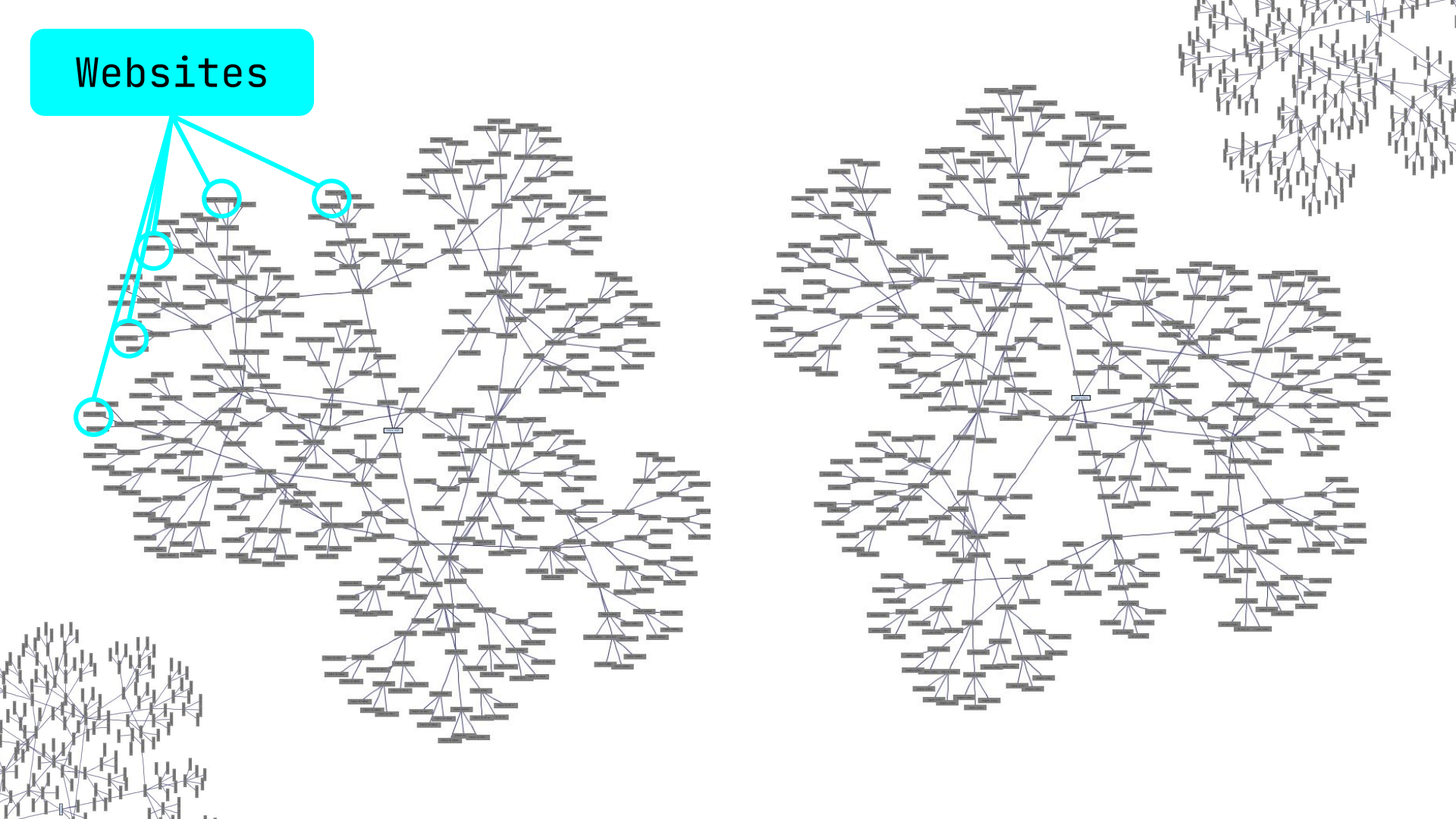




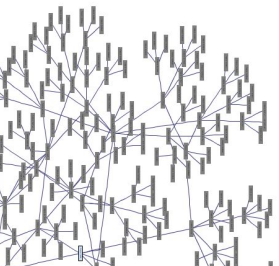
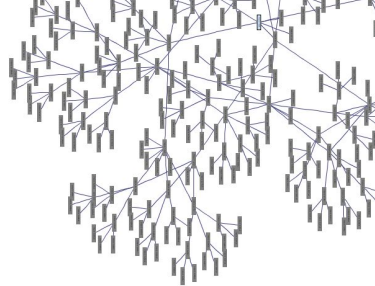
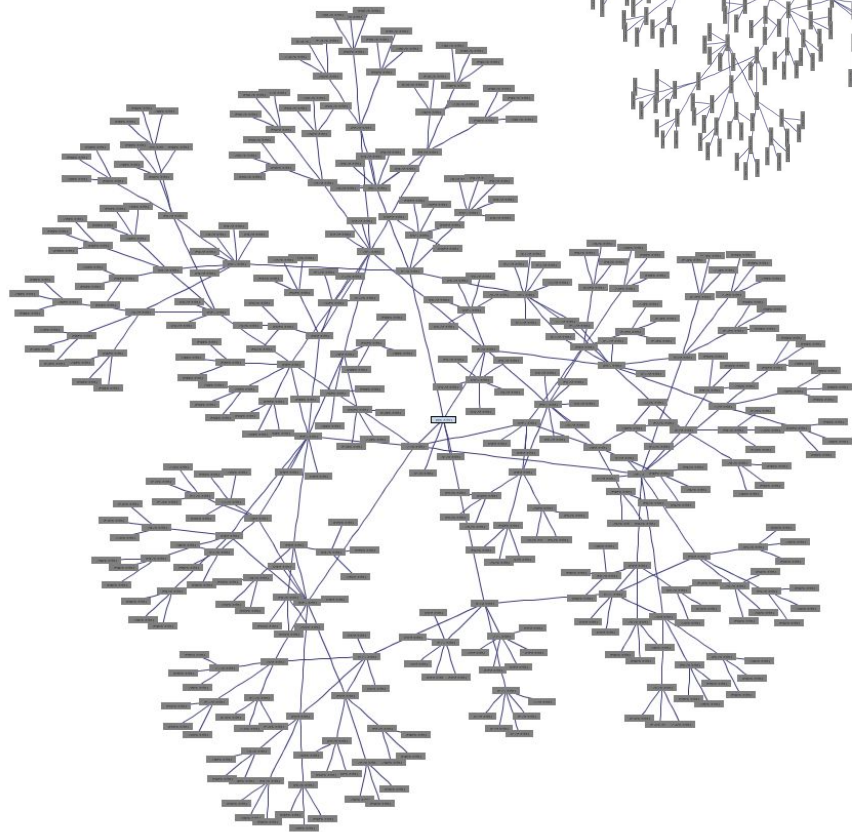
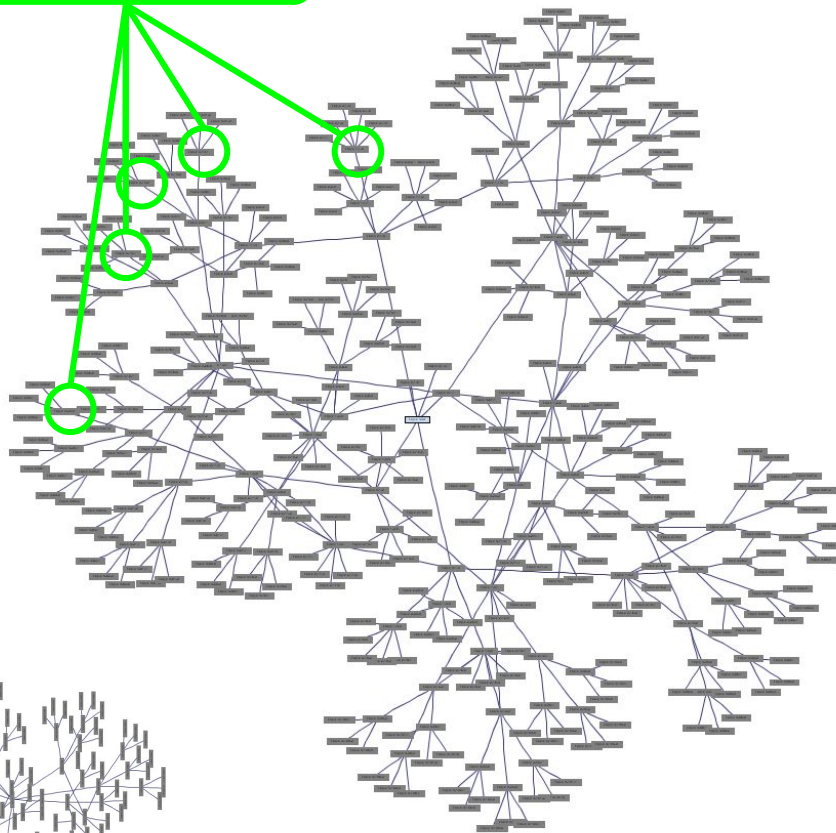
i'll vouch  
for you



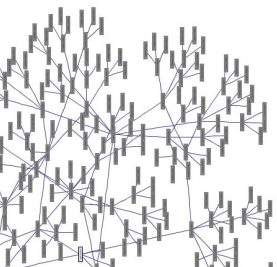
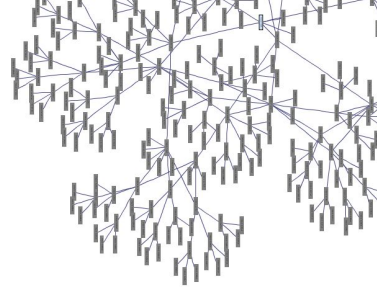
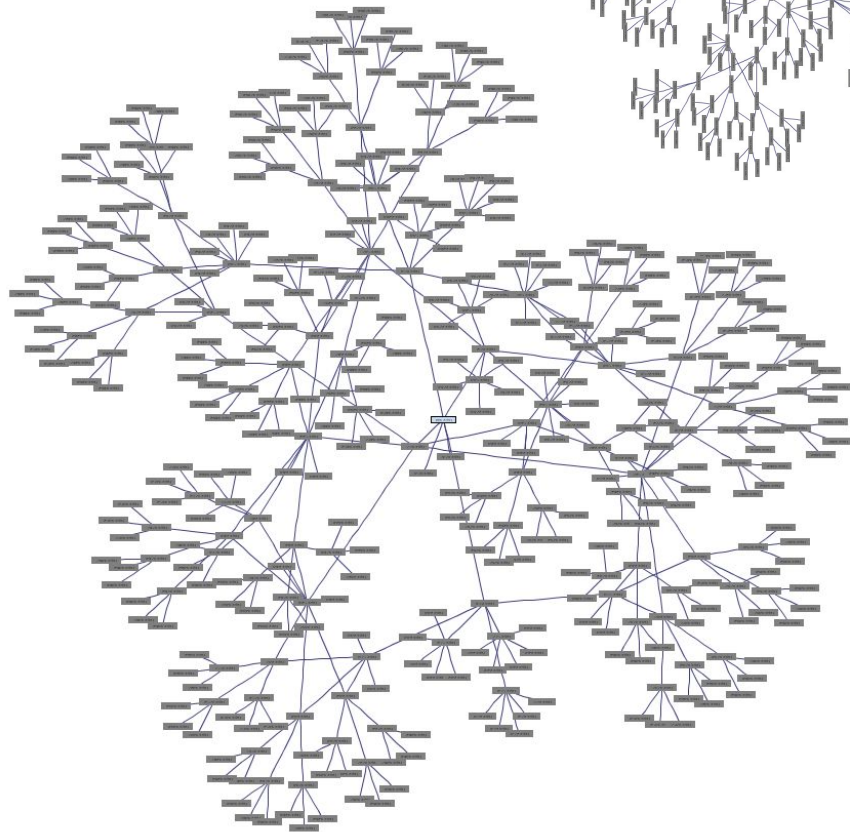
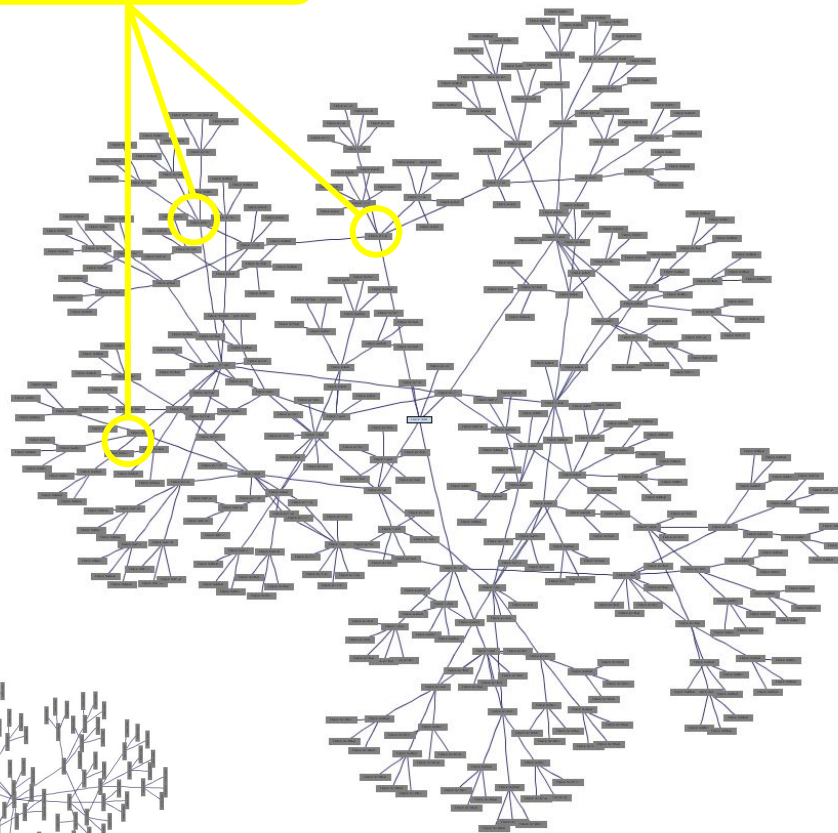
Websites



CAs

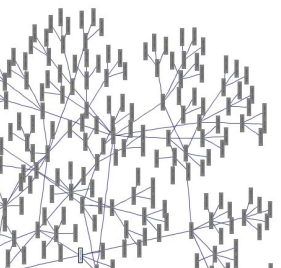
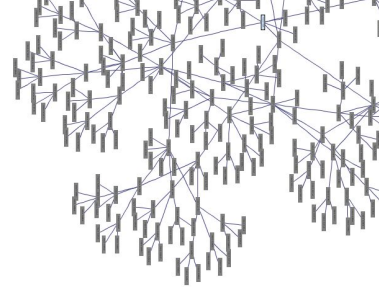
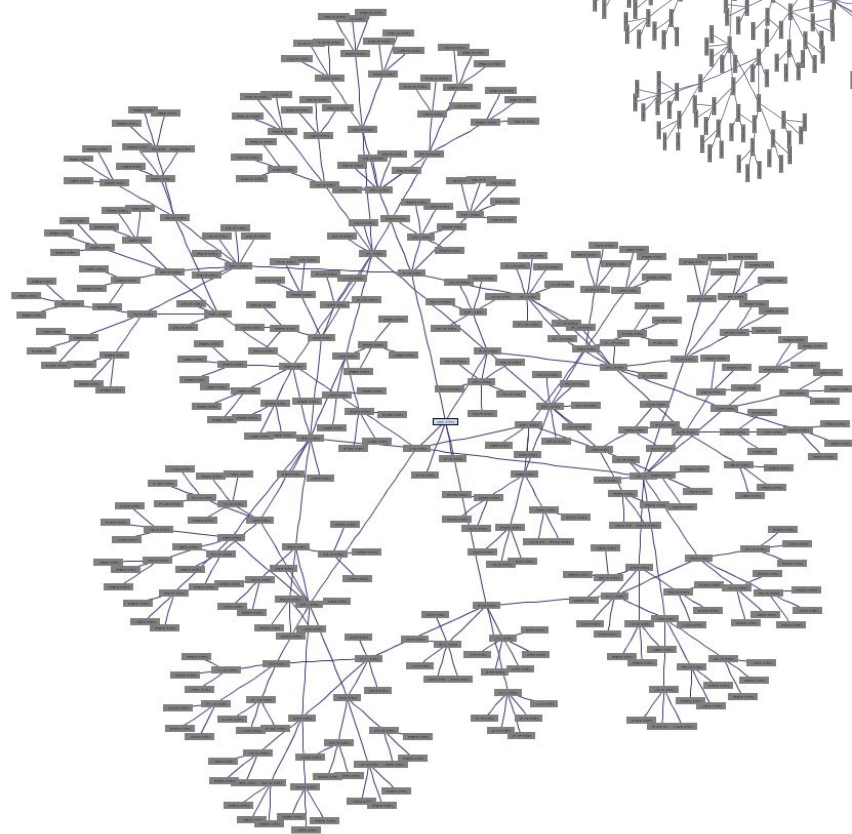
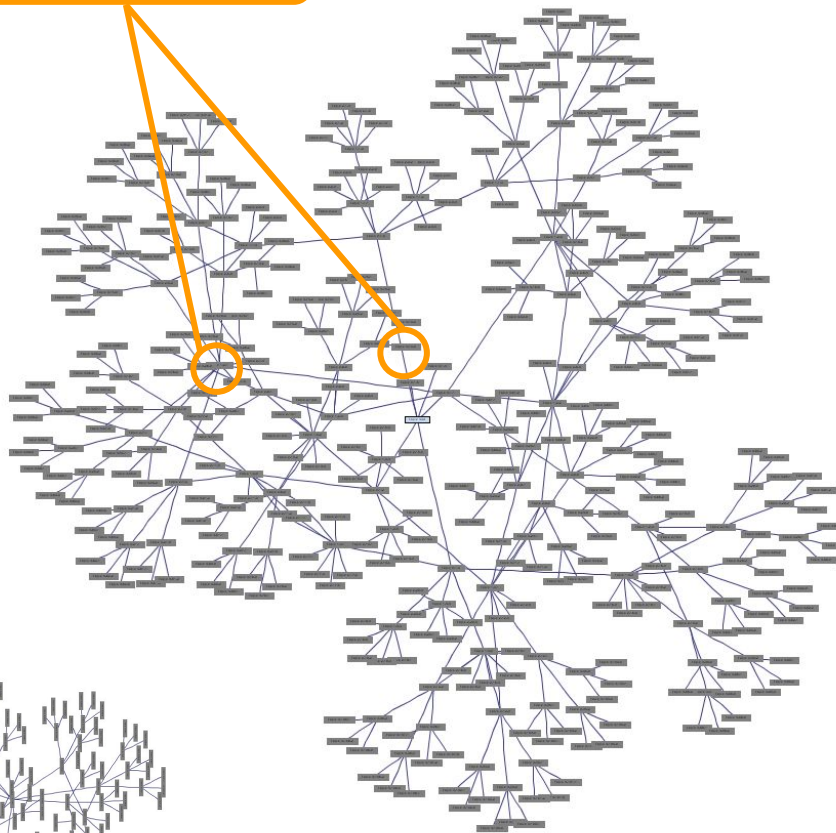


CAs



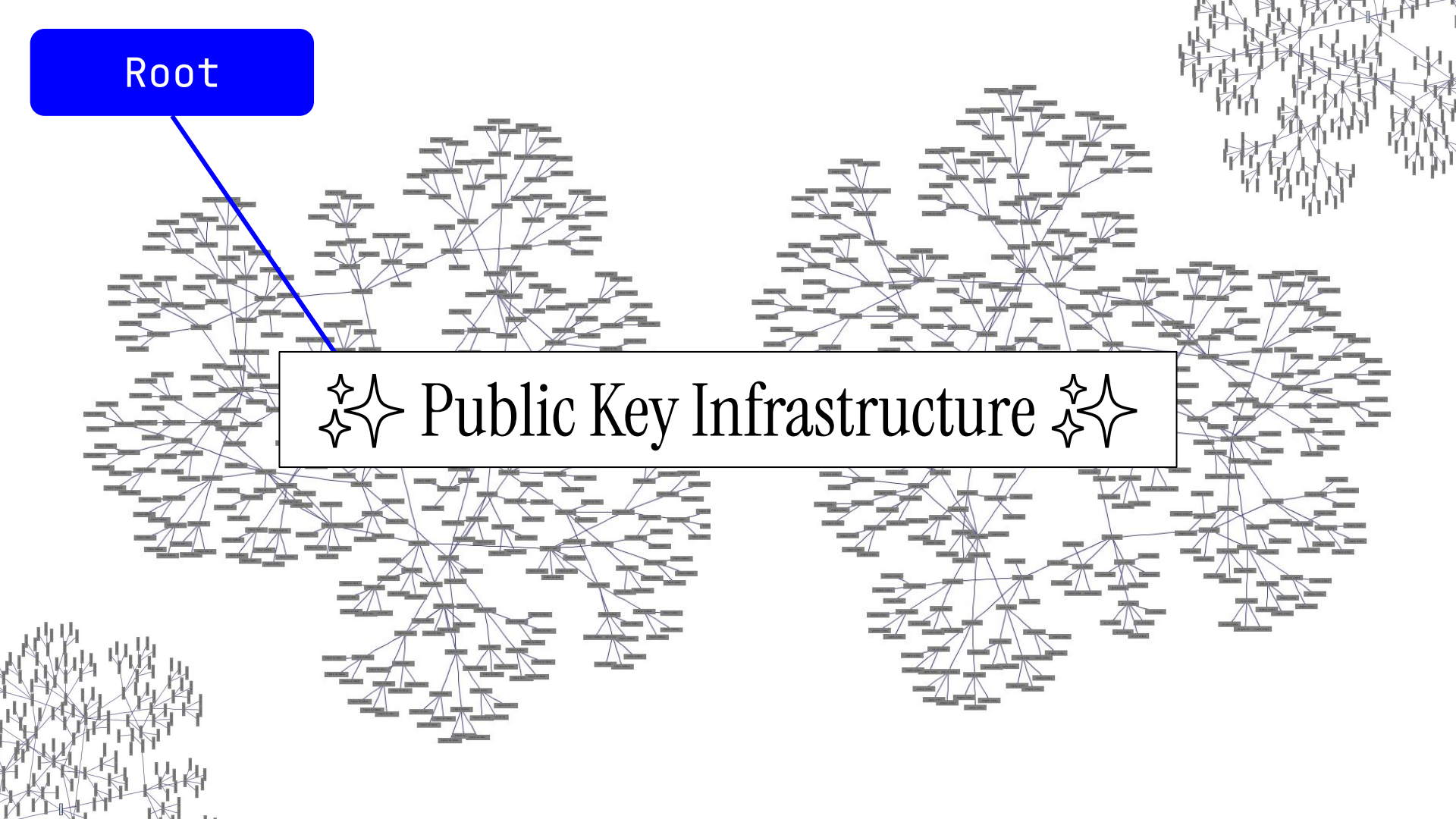


CAs



Root

✧✧ Public Key Infrastructure ✧✧



# HTTPS means 3 things:

1. Authentication ✓✓
2. Encryption ✓✓
3. Data integrity ✓✓\*



# HTTPS means 3 things:

1. Authentication ✓✓
2. Encryption ✓✓
3. Data integrity ✓✓\*

~~Trustworthiness~~

~~Good privacy policy~~

~~Phishing, malware~~



Example site



example.com

2.

SURVEY SAYS...

## “It builds trust with the customers” - Exploring User Perceptions of the Padlock Icon in Browser UI

Emanuel von Zezschwitz  
Google Inc.  
zezschwitz@chromium.org

Serena Chen  
Google Inc.  
serecena@chromium.org

Emily Stark  
Google Inc.  
estark@chromium.org

**Abstract**—We performed a large-scale online survey ( $n=1,880$ ) to study the padlock icon, an established security indicator in web browsers that denotes connection security through HTTPS. In this paper, we evaluate users’ understanding of the padlock icon, and how removing or replacing it might influence their expectations and decisions. We found that the majority of respondents (89%) had misconceptions about the padlock’s meaning. While only a minority (23%-44%) referred to the padlock icon at all when asked to evaluate trustworthiness, those padlock-aware users reported that they would be deterred from a hypothetical shopping transaction when the padlock icon was absent. These users were reassured after seeing secondary UI surfaces (i.e., Chrome Page Info) where more verbose information about connection security was present.

We conclude that the padlock icon, displayed by browsers in the address bar, is still misunderstood by many users. The padlock icon guarantees connection security, but is often perceived to indicate the general privacy, security, and trustworthiness of a website. We argue that communicating connection security precisely and clearly is likely to be more effective through secondary UI, where there is more surface area for content. We hope that this paper boosts the discussion about the benefits and drawbacks of showing passive security indicators in the browser UI.

**Index Terms**—usable security, padlock, browser, security indicators, user perception

### I. INTRODUCTION

HTTPS is the fundamental cryptographic protocol used to provide connection security on the web [1]. Over the past years, HTTPS support has proliferated<sup>1</sup> and nowadays most websites provide HTTPS to ensure data integrity and privacy between the communicating parties.

Most browsers show a padlock icon near the address bar to indicate connection security (see Figure 1, left). However, previous research has revealed that such icons are often neglected [2] and that the actual meaning of security indicators is not always obvious [3]. In fact, seeing a padlock is sometimes understood as a sign for general security and trustworthiness [4], [5]. This introduces the risk that users expect higher levels of protection that are not justified since a padlock does not guarantee that a site will behave in the user’s best interest (for example, a phishing or malware site which uses HTTPS [6]). Such misconceptions challenge the benefit of showing the padlock as a passive security indicator. Indeed, in 2018,

Google already announced plans to eventually remove secure indicators for HTTPS pages in Chrome<sup>2</sup>.

To quantify the impact of modifying such established browser UI, we conducted the first large-scale online survey ( $n = 1,880$ ) to systematically evaluate user perceptions of the padlock and modified iconography in a simulated encounter with an unfamiliar online shop. We designed different variations (see Figure 1) based on the most popular browser (i.e., Chrome) and tested the effects of replacing or removing the padlock icon. Our user study confirmed that the majority of users have misconceptions about the padlock’s meaning, since only 11% of the respondents had exclusive expectations on connection security and it revealed opportunities to optimize browsers for better discoverability of secondary UI.

In this paper, we present the results of the online survey and discuss implications for the design of modern web browsers. Our results may not generalize to real-world browsing, since, for example, users may be more likely to contemplate the padlock icon when prompted to make a trust decision in a survey than in a naturalistic scenario. However, we believe that our results provide important up-to-date insights into users’ perceptions and beliefs regarding the padlock icon. We hope that this paper provokes discussion about the benefits and drawbacks of showing passive security indicators in a HTTPS-enabled ecosystem, as it highlights the limitations of communicating fine-grained security information via simple iconography.

### II. RELATED WORK

In 2002, Friedman et al. [3] claimed that the padlock icon is a suboptimal choice to communicate connection security since it rather conveys “the idea of a ‘place’ that can be made secure” than data protection in transit. They concluded that the design of web browsers needs to be optimized in a way that helps users to better understand the accurate meaning of connection security.

Indeed, various studies [4]–[10] have indicated that users often misunderstand the meaning of the padlock icon. Ruoti et al. [8] performed an interview study and found that such misconceptions can foster insecure behavior (e.g., ignoring TLS warnings). Based on the observation that the padlock

<sup>1</sup>blog.chromium.org/2018/05/evolving-chromes-security-indicators.html accessed: 2022/02/28

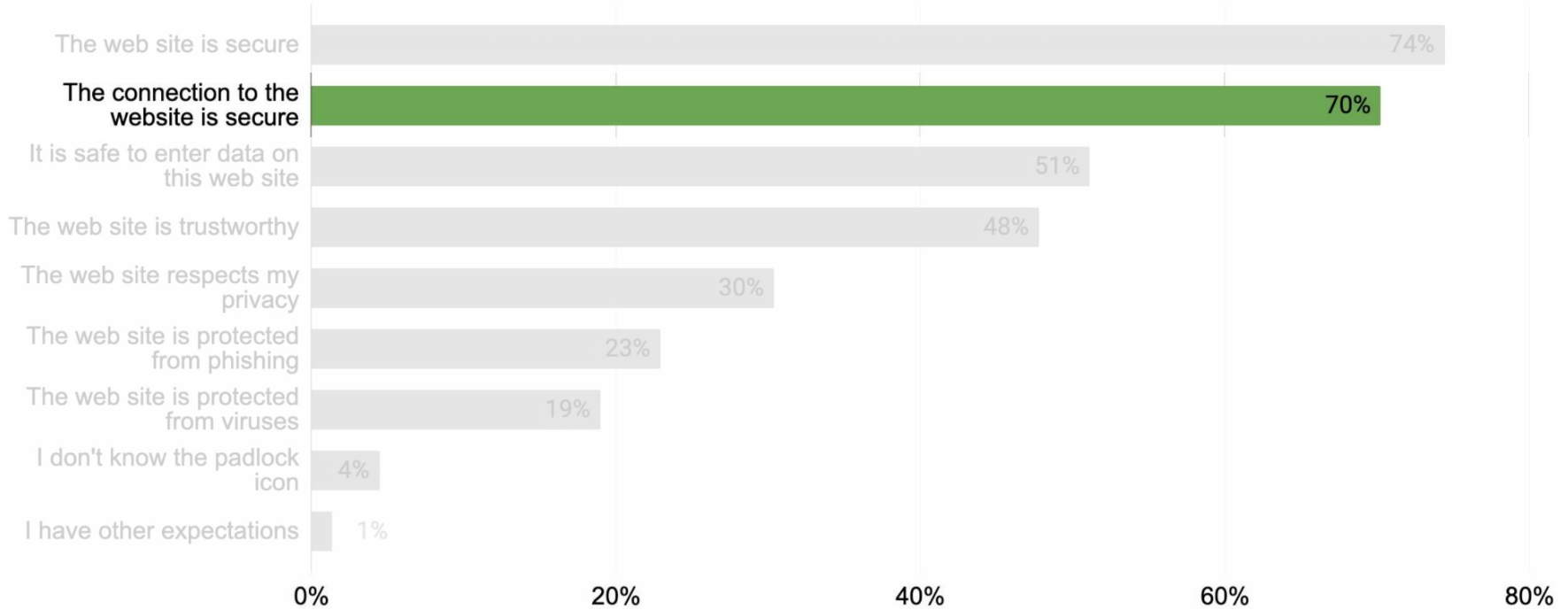
<sup>2</sup>transparencyreport.google.com/https/overview accessed: 2022/02/28

Dear 1,880 people

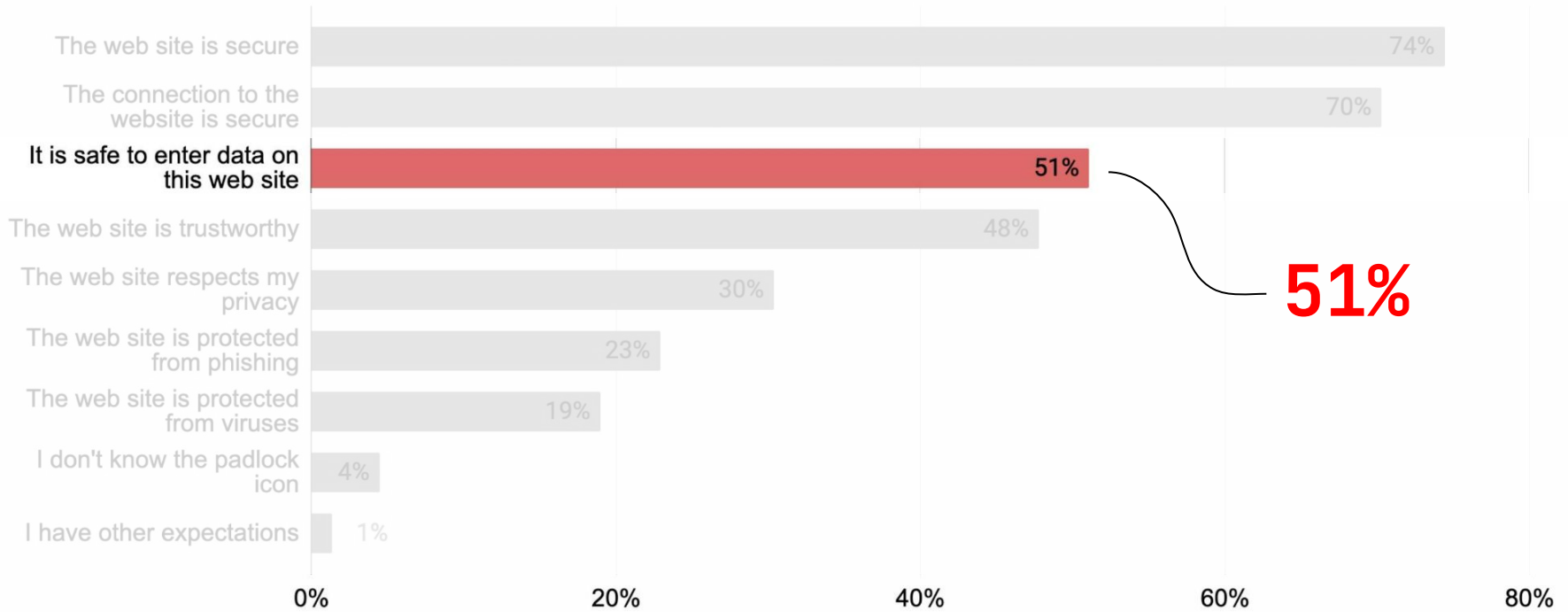
What does  mean?

wait who are you

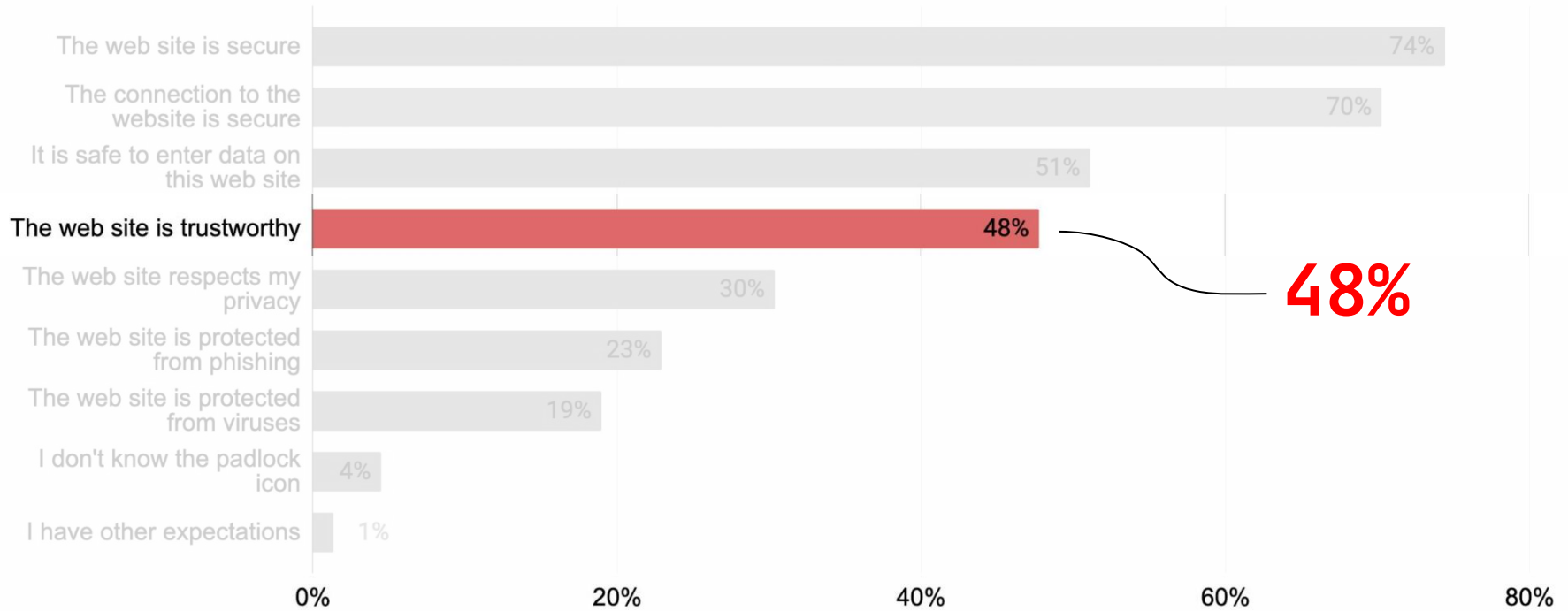
(multiple choice results)



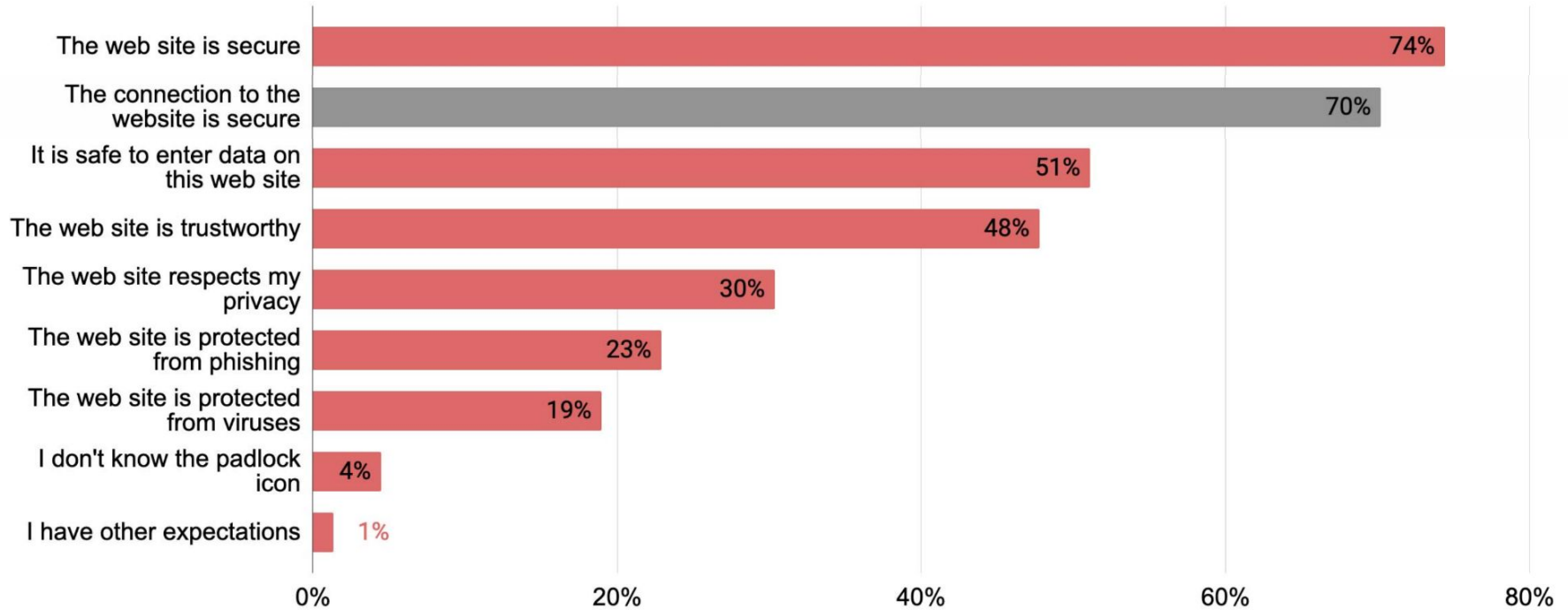
(multiple choice results)



(multiple choice results)



(multiple choice results)





89% of participants  
*overestimated* the  
security guarantees


ceptibility. Secure email transport had minimal effect, while **HTTPS increased the click-through rate of email phishing links (72.0% HTTPS, 60.0% HTTP)** and the credential-entry rate of phishing sites (58.0% HTTPS, 55.6% HTTP). How-

Q. Is this a problem?

A. Yes

Sign in - chase.com

secure.03b-chase.com/web/auth/dashboard#/dashboard/overviewAccounts/overview/index



# BTW THIS IS A PHISHING ATTACK

**Username**

---

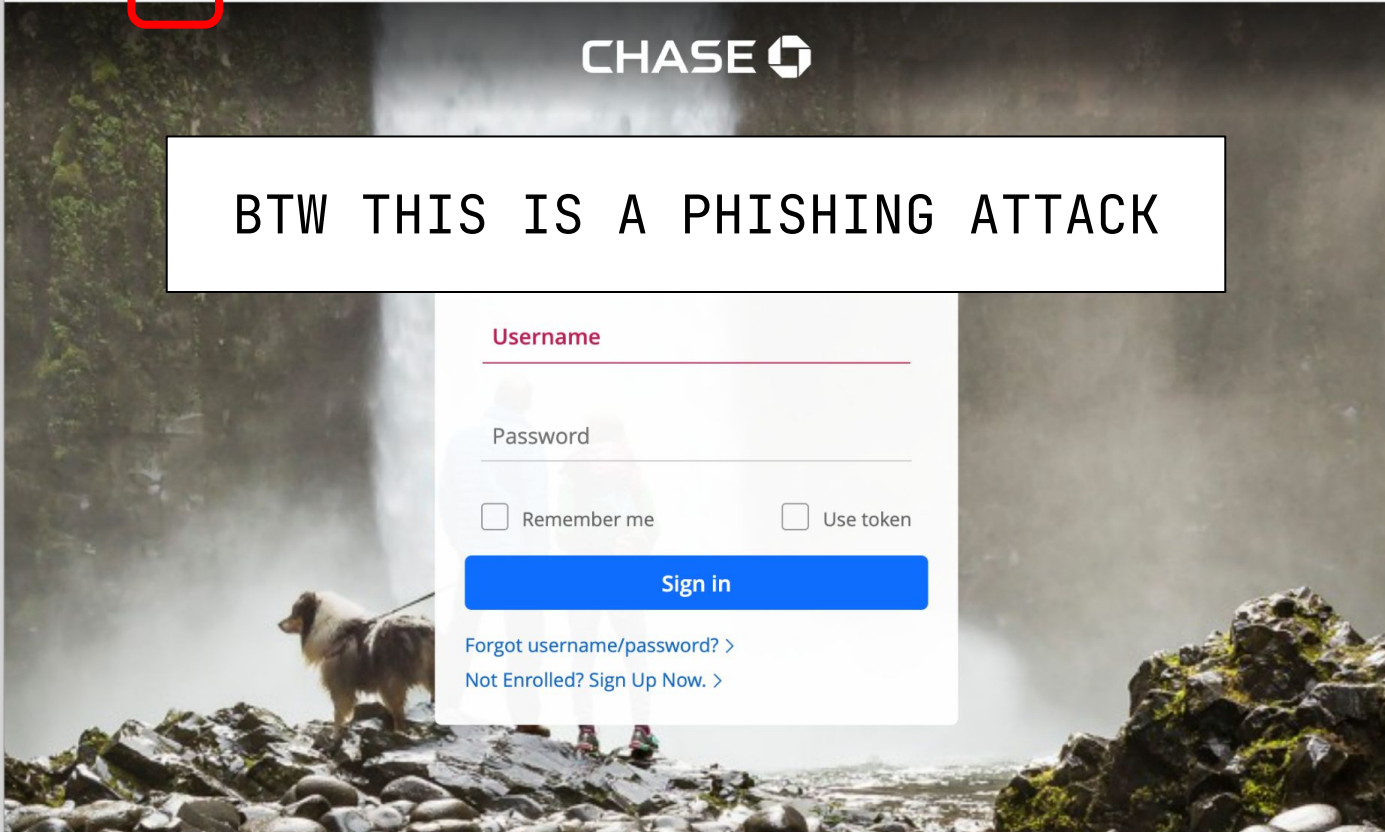
Password

---

Remember me  Use token

**Sign in**

[Forgot username/password? >](#)  
[Not Enrolled? Sign Up Now. >](#)





## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



June 10, 2019

Alert Number  
I-061019-PSA

Questions regarding this  
PSA should be directed to  
your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

### Cyber Actors Exploit 'Secure' Websites In Phishing Campaigns

Websites with addresses that start with "https" are supposed to provide privacy and security to visitors. After all, the "s" stands for "secure" in HTTPS: Hypertext Transfer Protocol Secure. In fact, cyber security training has focused on encouraging people to look for the lock icon that appears in the web browser address bar on these secure sites. The presence of "https" and the lock icon are supposed to indicate the web traffic is encrypted and that visitors can share data safely. Unfortunately, cyber criminals are banking on the public's trust of "https" and the lock icon. They are more frequently incorporating website certificates—third-party verification that a site is secure—when they send potential victims emails that imitate

- **Do not trust a website just because it has a lock icon or "https" in the browser address bar.**

- Do not simply trust the name on an email: question the intent of the email content.
- If you receive a suspicious email with a link from a known contact, confirm the email is legitimate by calling or emailing the contact; do not reply directly to a suspicious email.
- Check for misspellings or wrong domains within a link (e.g., if an address that should end in ".gov" ends in ".com" instead).
- Do not trust a website just because it has a lock icon or "https" in the browser address bar.

#### VICTIM REPORTING

The FBI encourages victims to report information concerning suspicious or criminal activity to their local FBI field office, and file a complaint with the IC3 at [www.ic3.gov](http://www.ic3.gov). If your complaint pertains to this particular scheme, please note "HTTPS phishing" in the body of the complaint.

What does  mean?

I trust website!

*NO—*

3.

UN-MIS-COMMUNICATE

09

Gmail is  
HTTPS by default

JAN  
2010

JUL  
20



JAN  
2010

EFF & Tor Project  
releases HTTPS  
Everywhere extension

JUN  
2010

20

Google Search defaults  
to HTTPS for all  
signed-in users

11

MAR  
2012

20

HTTPS



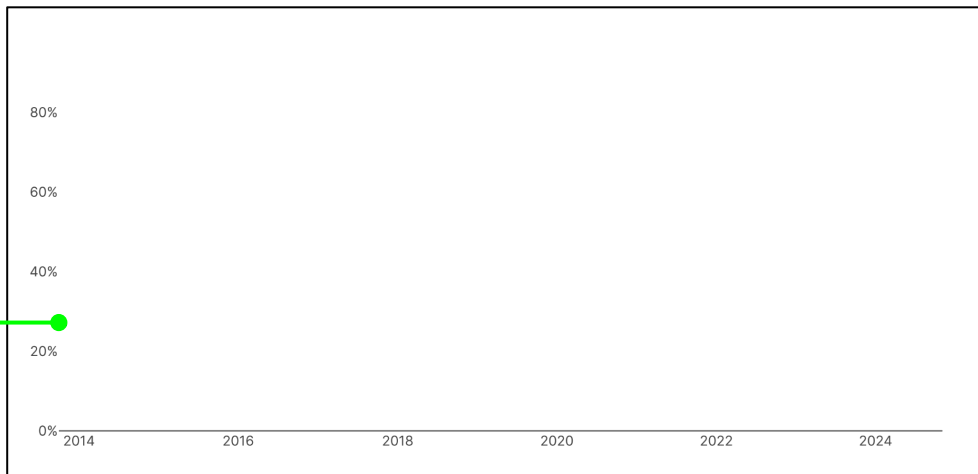
HTTP



**~27%**

Oct 2013

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

12

2013

20

HTTPS



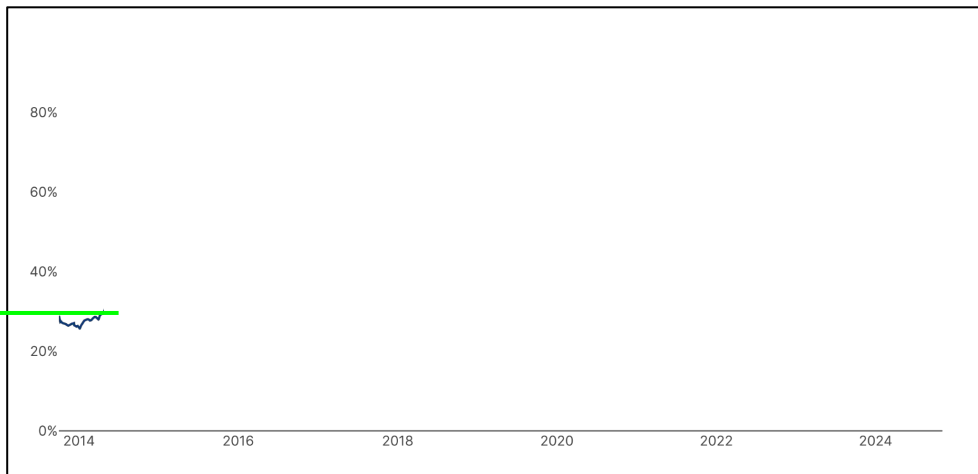
HTTP



**~30%**

May 2014

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

“HTTPS Everywhere” at  
Google I/O

13

MAY  
2014

20

HTTPS



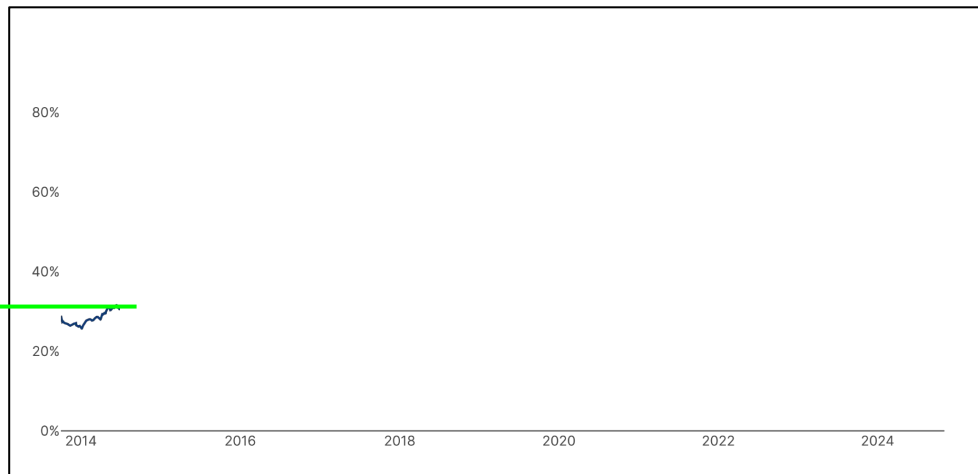
HTTP



**~31%**

Aug 2014

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

Google Search starts  
using HTTPS as signal  
for search ranking

13

AUG  
2014

20

HTTPS



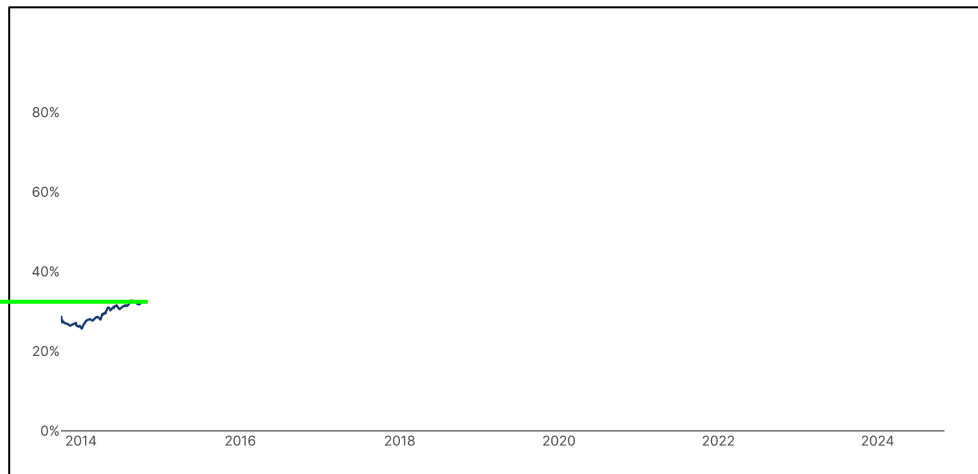
HTTP



**~32%**

Nov 2014

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

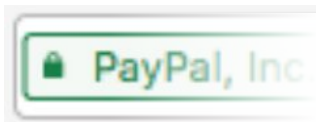
Let's Encrypt  
announces  
free certificates

13

NOV  
2014

20

HTTPS



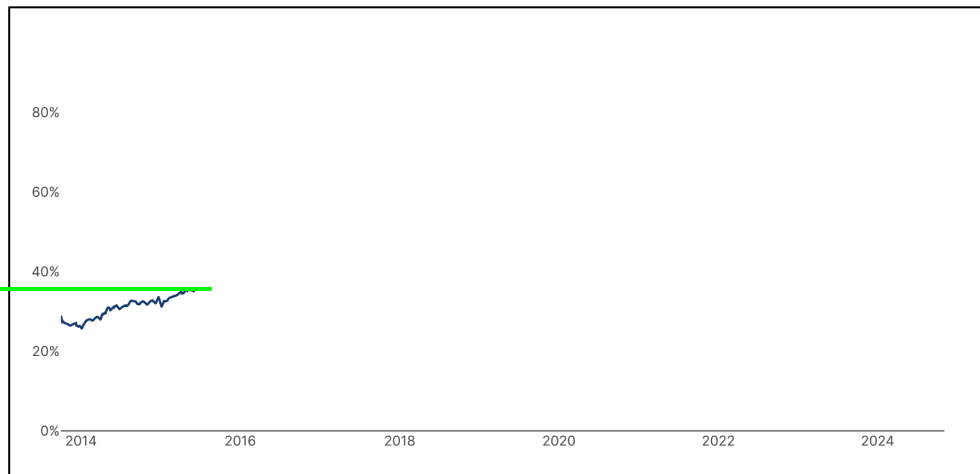
HTTP



**~35%**

Jun 2015

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

Chrome experiments with  
security indicators

14

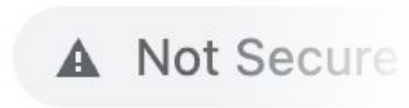
2015

20

HTTPS



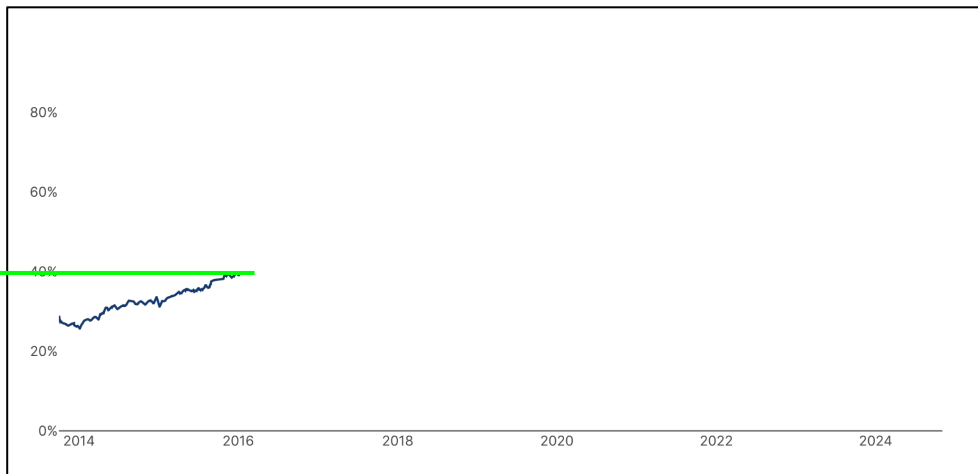
HTTP



**~40%**

Jan 2016

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

Chrome updates security indicators

15

2016

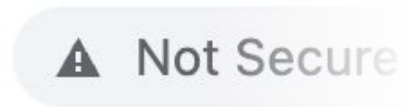
20



HTTPS

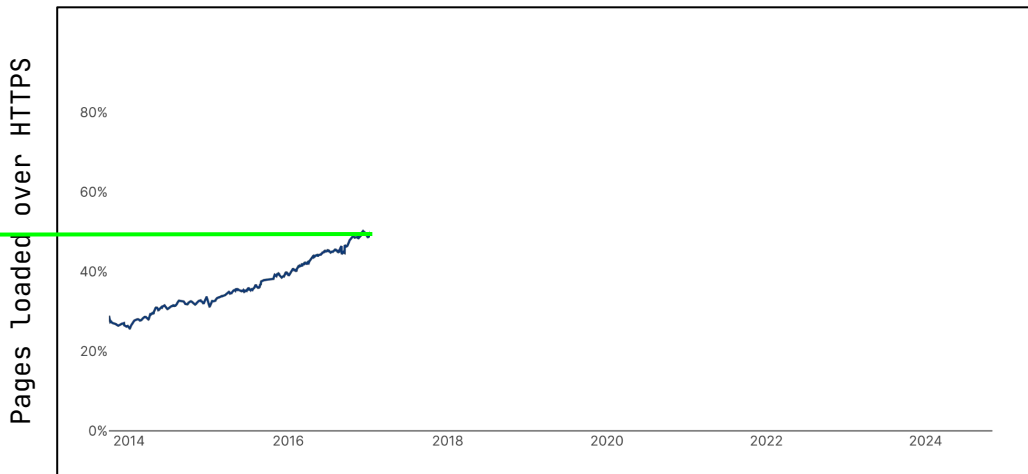


HTTP



**~50%**

Jan 2017



[LetsEncrypt stats](#)

More aggressive warnings for  
credit cards & passwords submitted  
over HTTP in Chrome and Firefox

16

JAN  
2017

20

HTTPS



example.co

HTTP

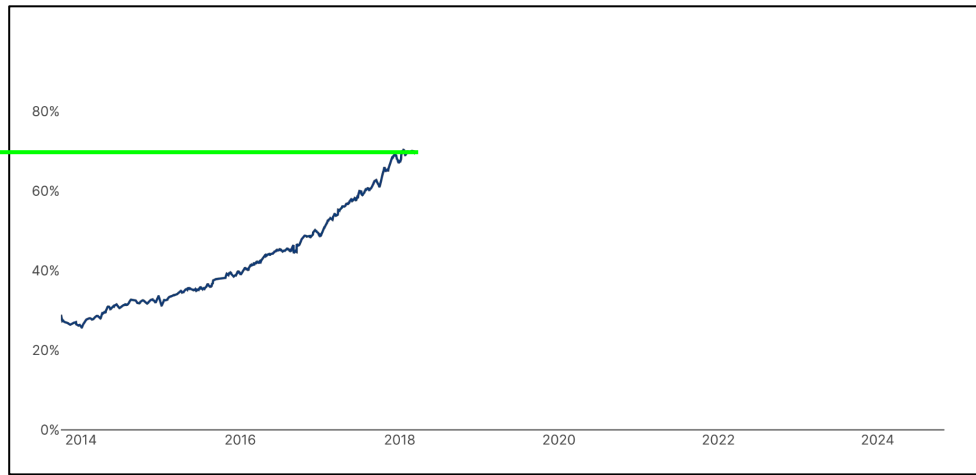


Not Secure

~70%

Feb 2018

Pages Loaded over HTTPS



[LetsEncrypt stats](#)

Chrome starts marking  
all HTTP connections as  
"Not Secure"

17

FEB  
2018

20

HTTPS



example.co

HTTP

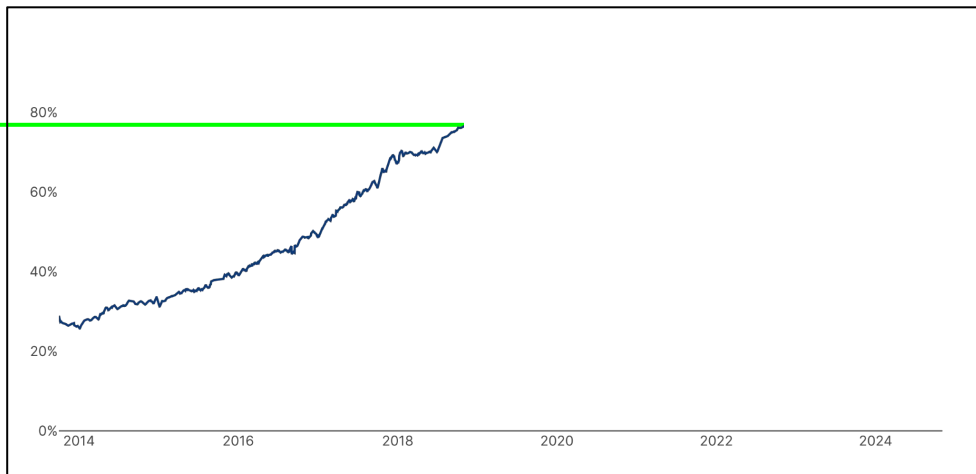


Not Secure

~77%

Jan 2019

Pages Loaded over HTTPS



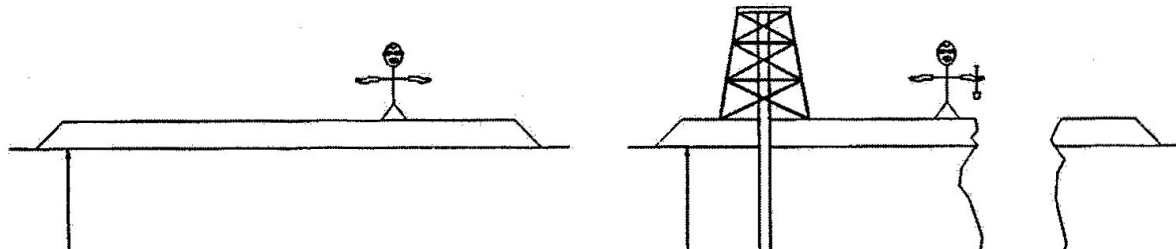
[LetsEncrypt stats](#)

17

2019

20

Communication  
requires context.

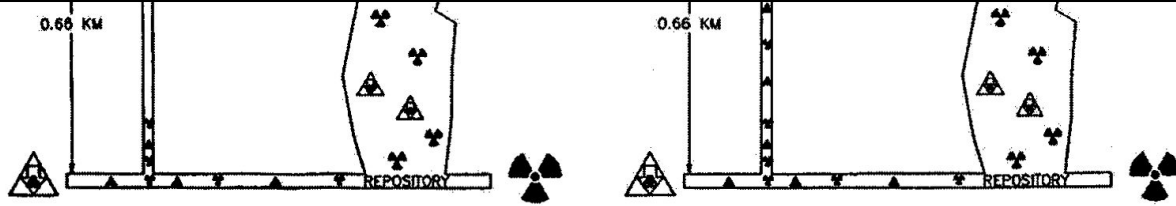


*This place is a message... and part of a system of messages... pay attention to it!*

*This place is not a place of honor... nothing valued is here*



*The danger is still present, in your time, as it was in ours.*





2008

2010

2012

2015

2016

2018

now?

https://www.android.com

PayPal, Inc. [US] https://www.paypal.com

Secure | example.com

example.com

2008

2010

2012

2015

2016

2018

now?



http://www.google.com

www.softpedia.com

www.softpedia.com

www.cnn.com

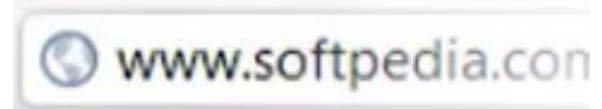
Not Secure | http://www.cnn.com

Not Secure | https://www.cnn.com

2008



2010



2012



2015



2016



2018



now?

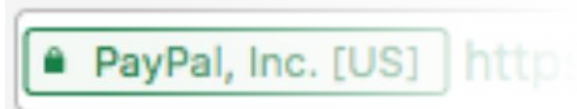
HTTP indicators  
become *louder*

2008

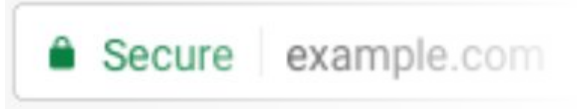
2010



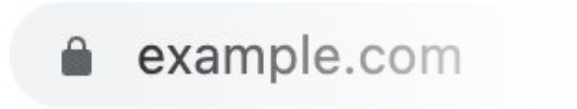
2012



2015



2016



2018



HTTPS indicators  
become *quieter*

now?

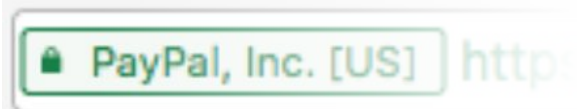


2008

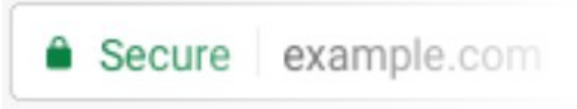
2010



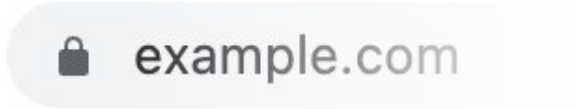
2012



2015



2016



2018



now?



4.

GOODBYE LOCK

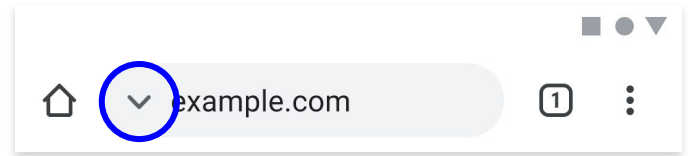
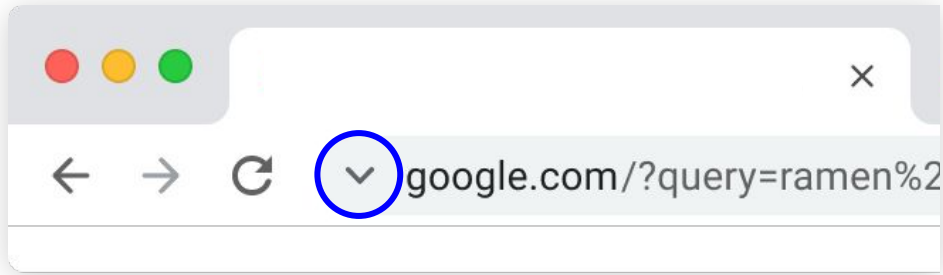
Hi! We want to remove  
the lock icon!

Don't people depend on it  
for reassurance? 🙄

.. rats

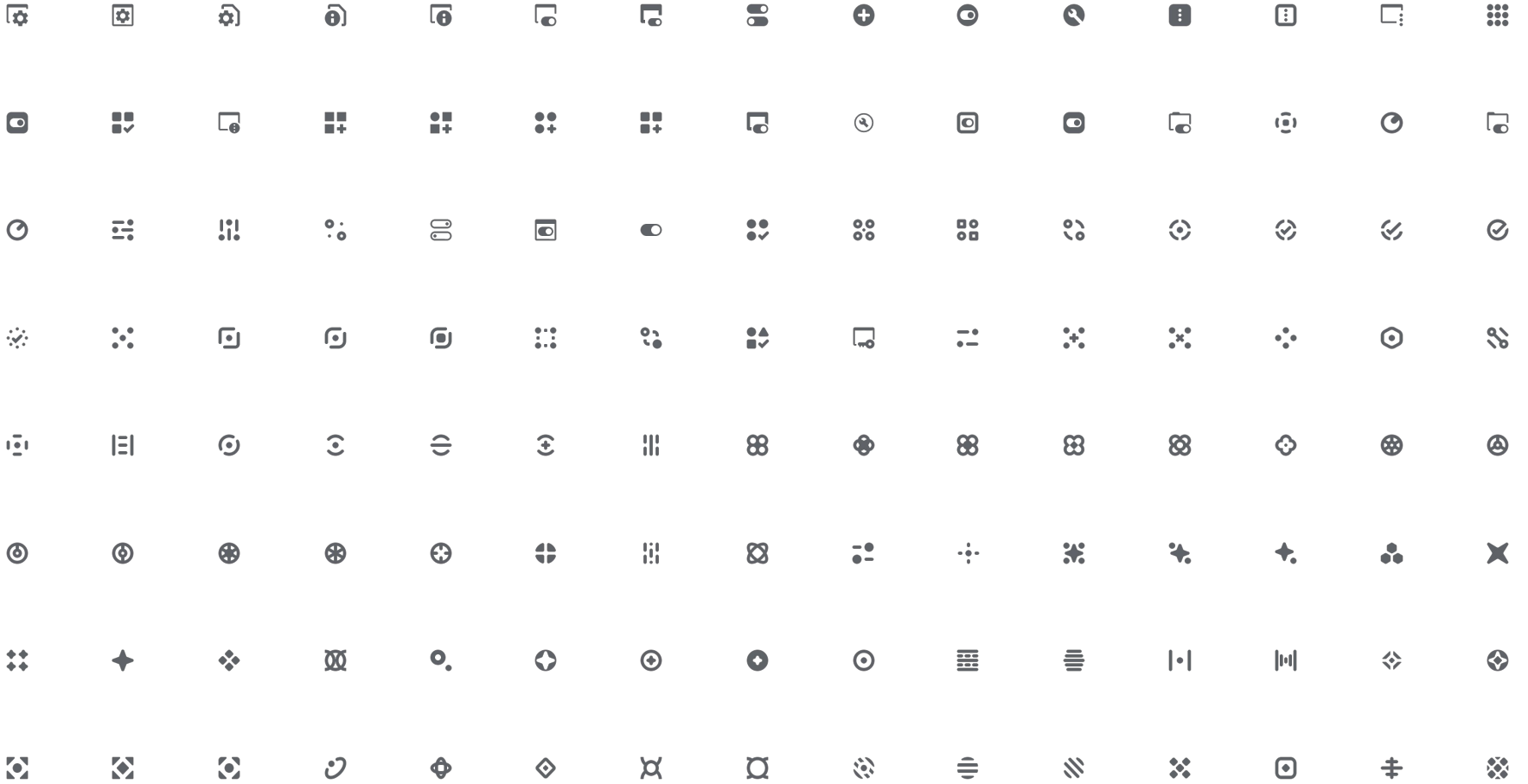
Will

“1% experiment”



# Results

- **People noticed the change**
  - Significant increase in opening site controls (~83%/36% on Windows/Android)
- **They did not freak out**
  - No regressions on time spent on HTTPS pages
  - No regressions on forms submitted over HTTPS



Hey so it looks like  
removing the lock is fine

We are still worried people  
will feel bad!

But lock icon danger bad!! 😞 😞

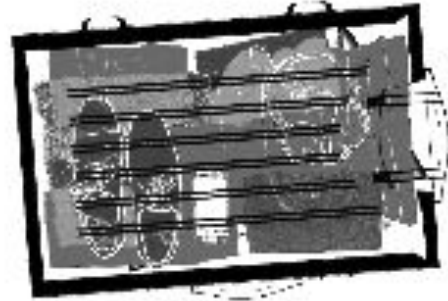
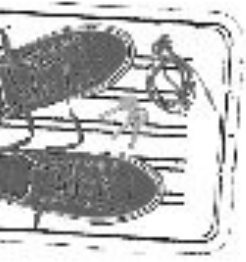
Read 11:28 AM



5.

THE ALLURE OF  
SECURITY THEATRE

# *“Security Theatre”*

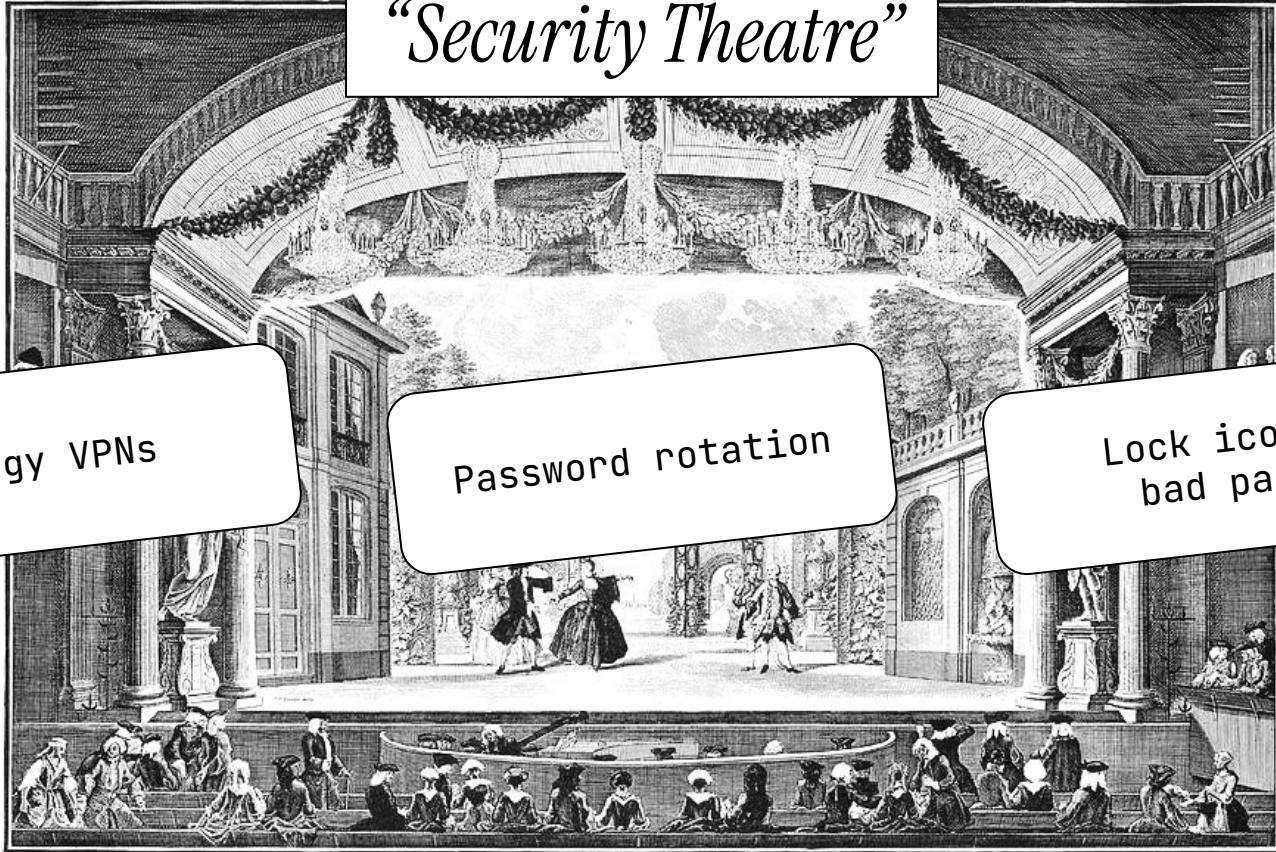


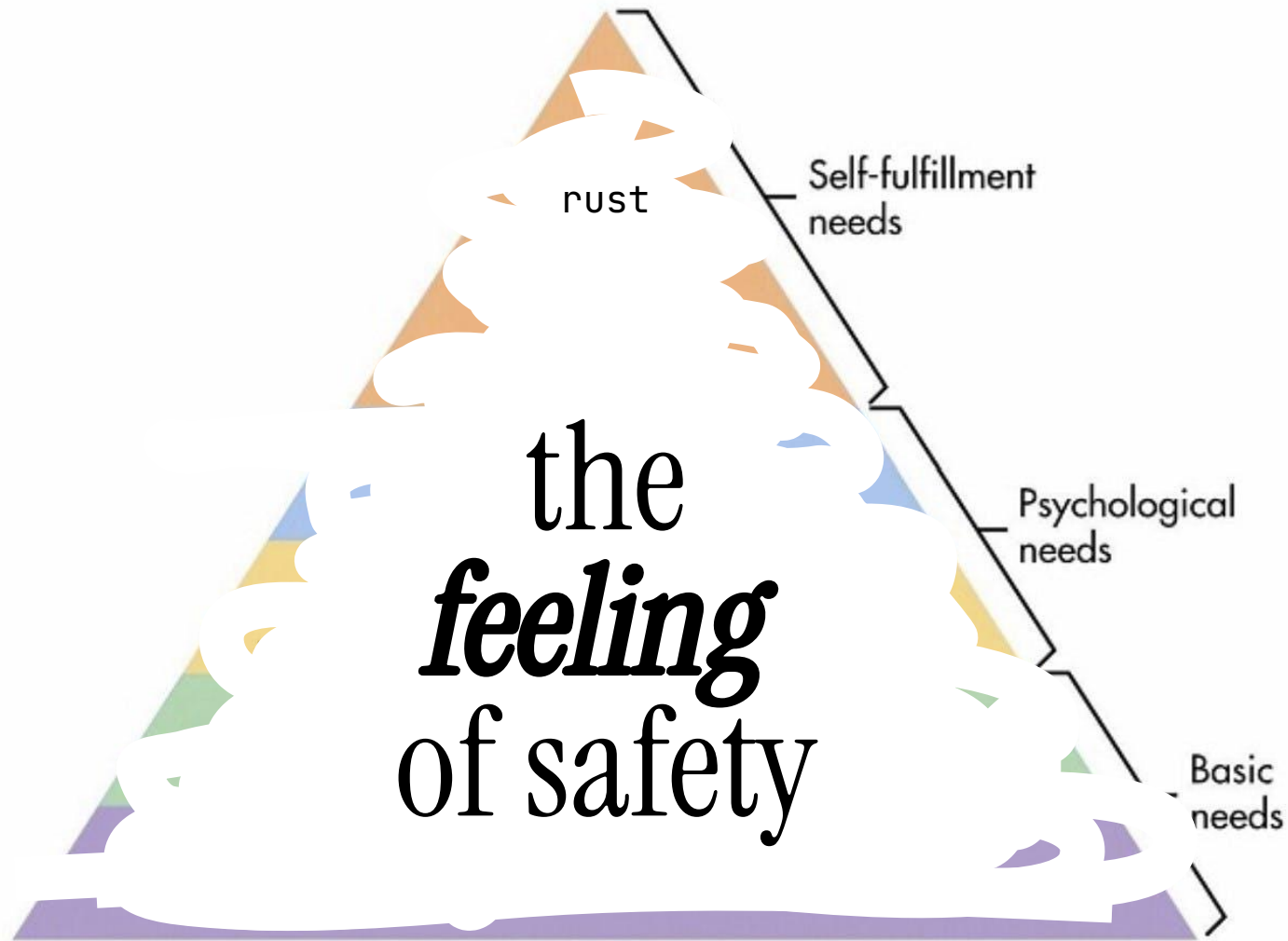
# *“Security Theatre”*

Dodgy VPNs

Password rotation

Lock icon on  
bad pages







*reassurance is important*



Reassurance



Theatre?

# Look to user behaviour

- Does lack of reassurance lead people *away* from safety?
  - **No.** No regression on HTTPS pages / form submissions
- Does the presence of reassurance lure people *towards* danger?
  - **Yes.** Slight increase in phishing click-through rates



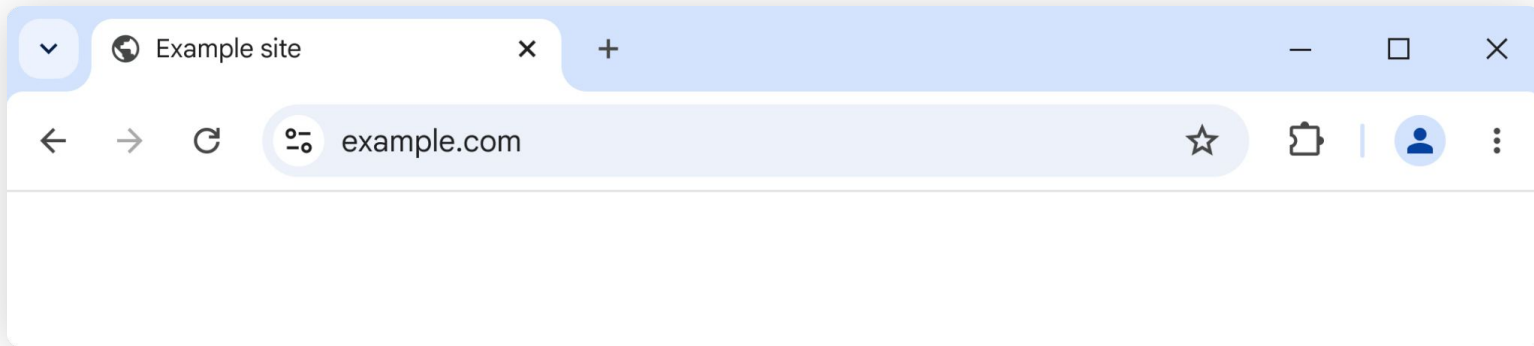
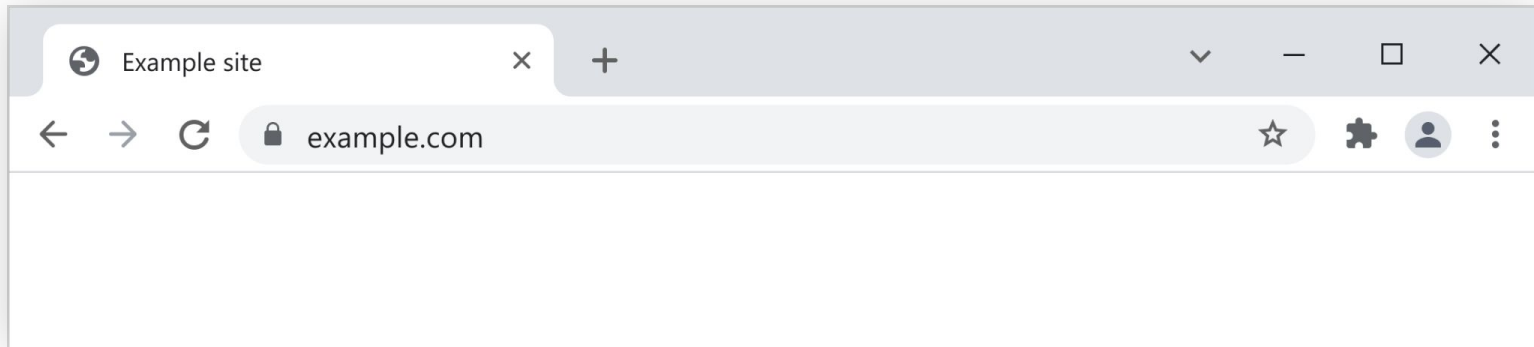
Reassurance



Theatre



People





Chrome shows neutral  
icon for HTTPS

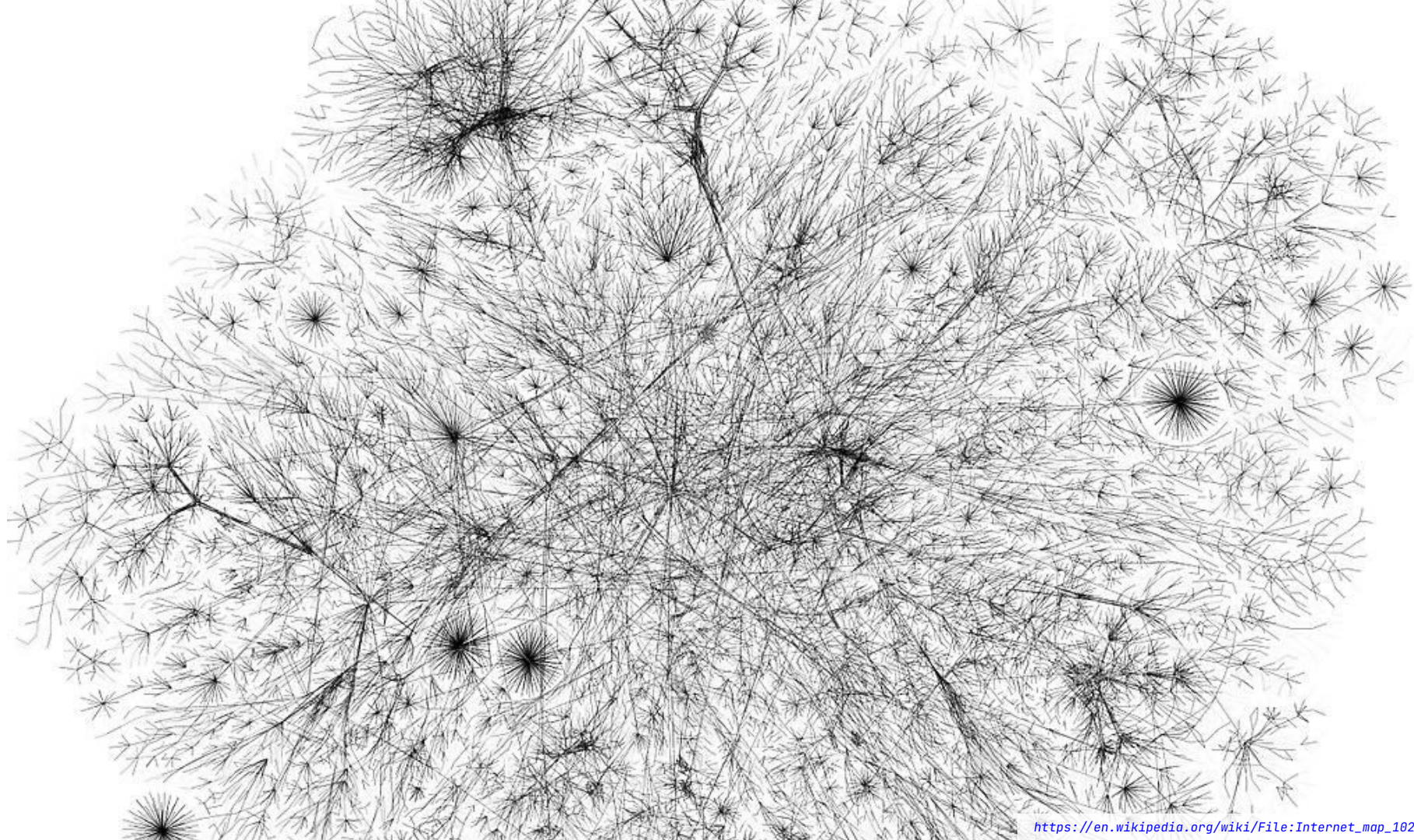
22

SEP  
2023

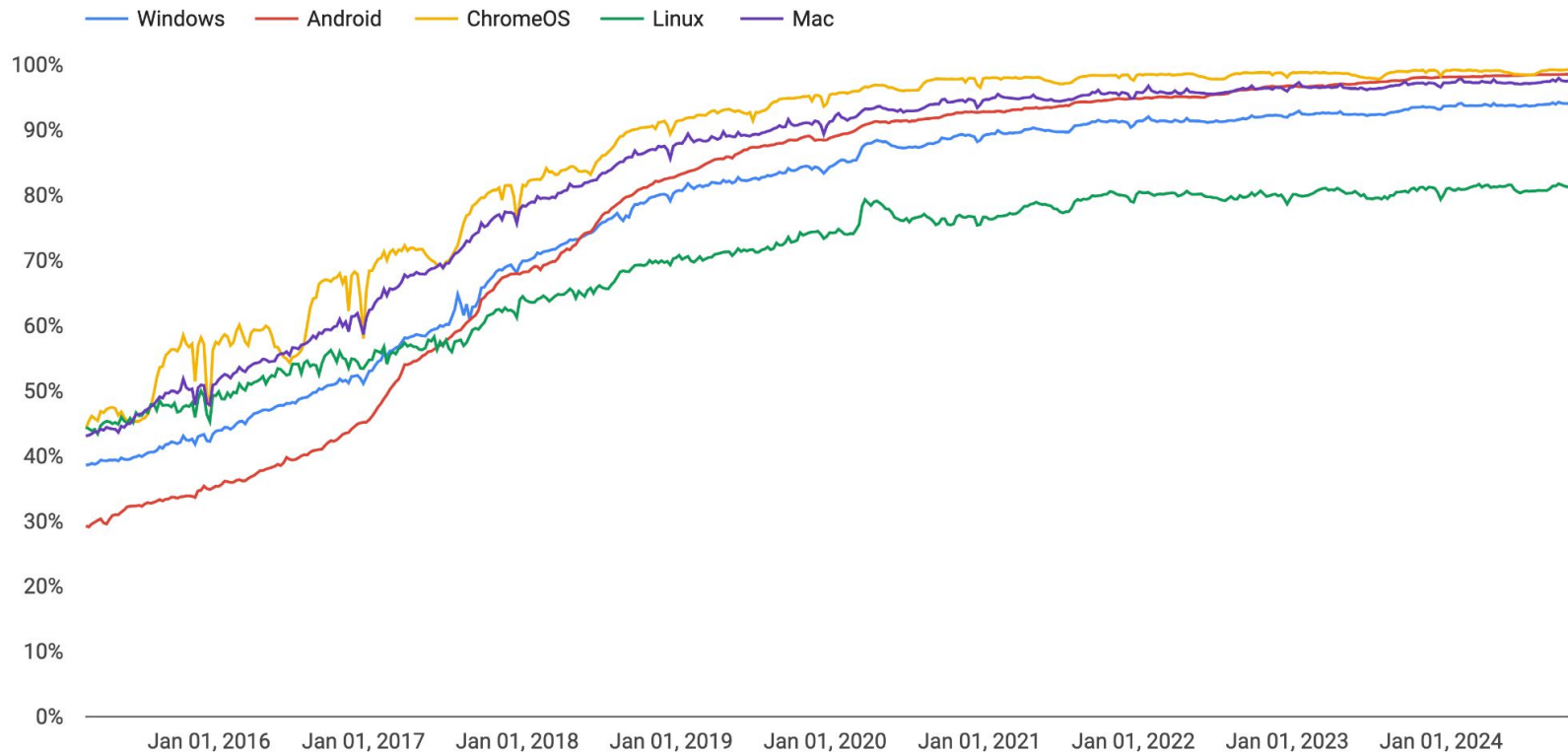
20

6.

# ECOSYSTEM CHANGE



# Pages Loaded over HTTPS in Chrome

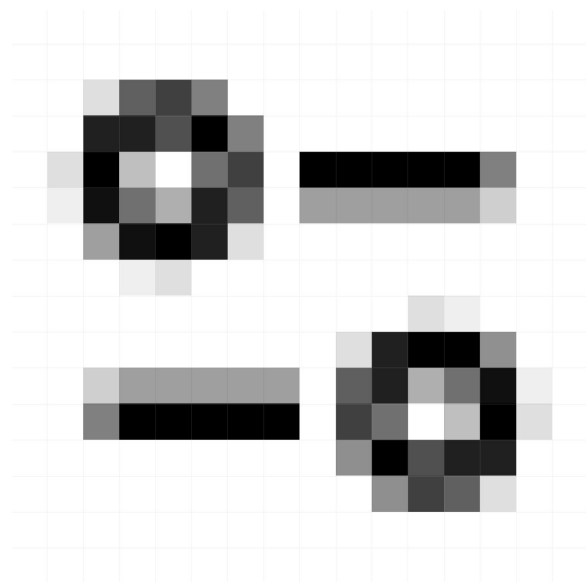
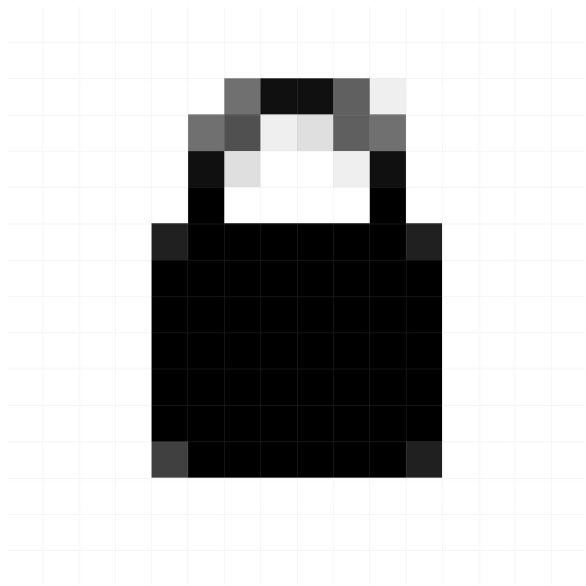


...but it's *worth it*

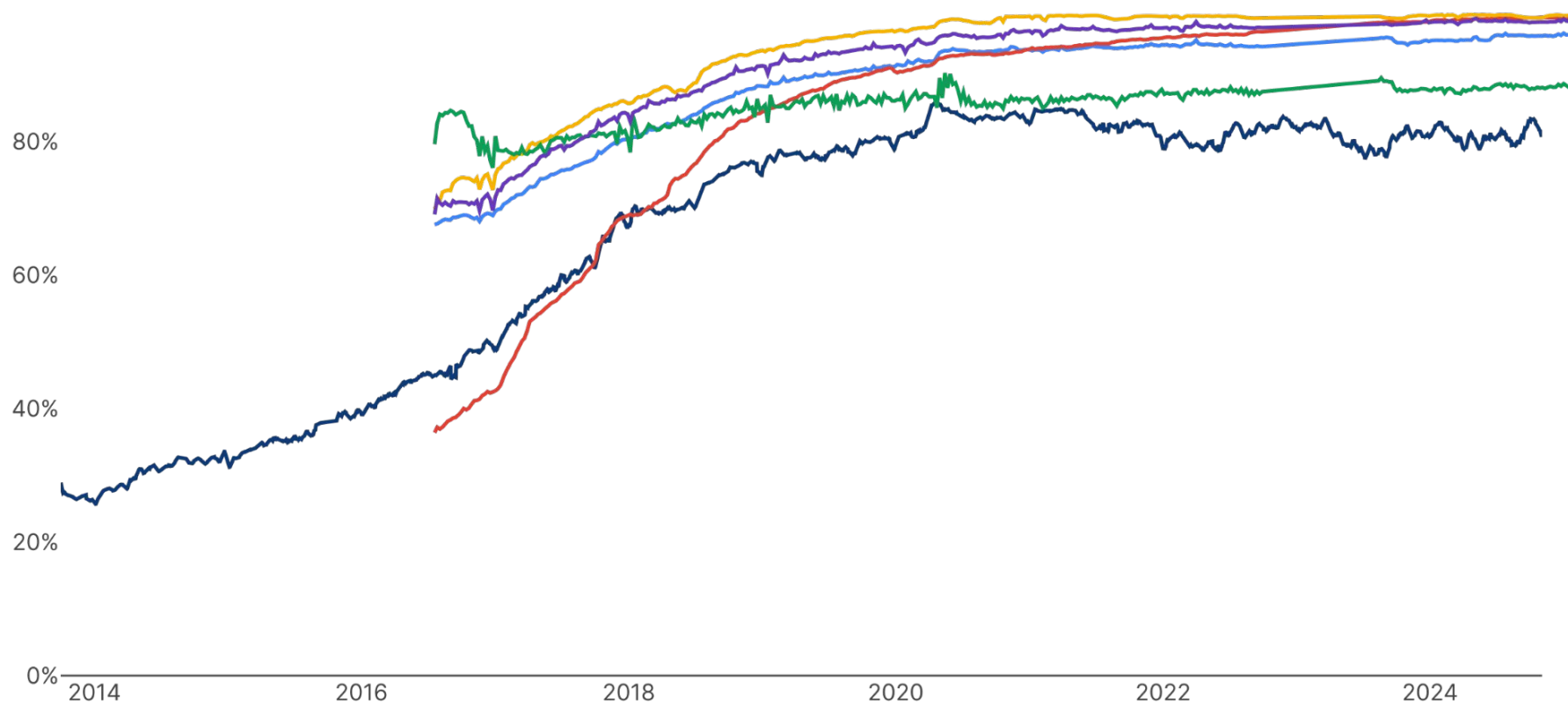


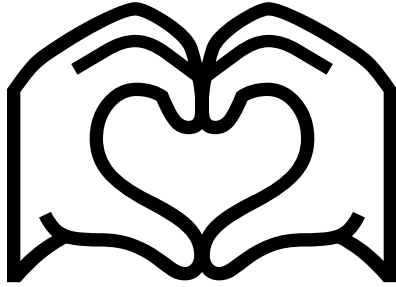


https://



# Pages Loaded over HTTPS in Firefox & Chrome







### *further reading–*

- E. Zezschwitz, S. Chen, E. Stark, ["It builds trust with the customers" - Exploring User Perceptions of the Padlock Icon in Browser UI](#), *IEEE Security and Privacy Workshops 2022*
- A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, ["Rethinking Connection Security Indicators"](#), *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*
- [Timeline of HTTPS Adoption](#)
- [Diffie-Hellman key exchange](#)
- J. Katz, Y Lindell, [Introduction to Modern Cryptography, Second Edition](#), Chapman & Hall
  - This one is if you really love math & number theory

### *greetz–*

- Those who worked tirelessly on removing the lock throughout the past 3 years: Emily Stark, Joe DeBlasio, Emanuel von Zezschwitz, Mustafa Emre Acer, Carlos Joan Rafael Ibarra Lopez, Chris Thompson, David Adrian, Alex Ainslie, Shweta Panditrao, Eric Mill
- Special shoutout to Emily Stark, a long-standing legend in this space. TY also for reviewing this talk and fact-checking my TLS handshake diagrams!
- Adriana P. Felt for her impactful prior research that I constantly refer back to, and for reviewing this talk