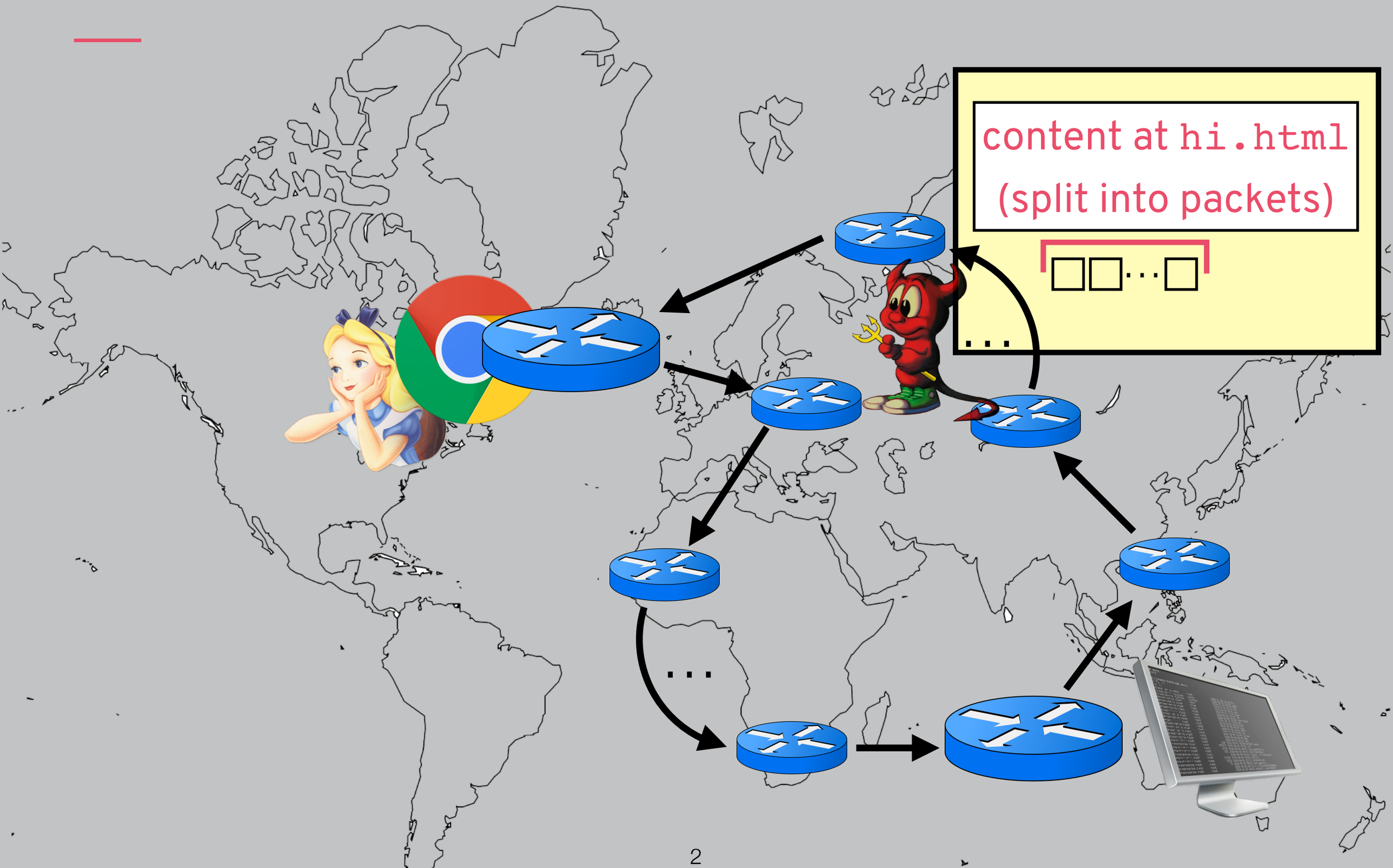
SECURITY (COMP0141):
USING ENCRYPTION

(UN)ENCRYPTED WEB TRAFFIC



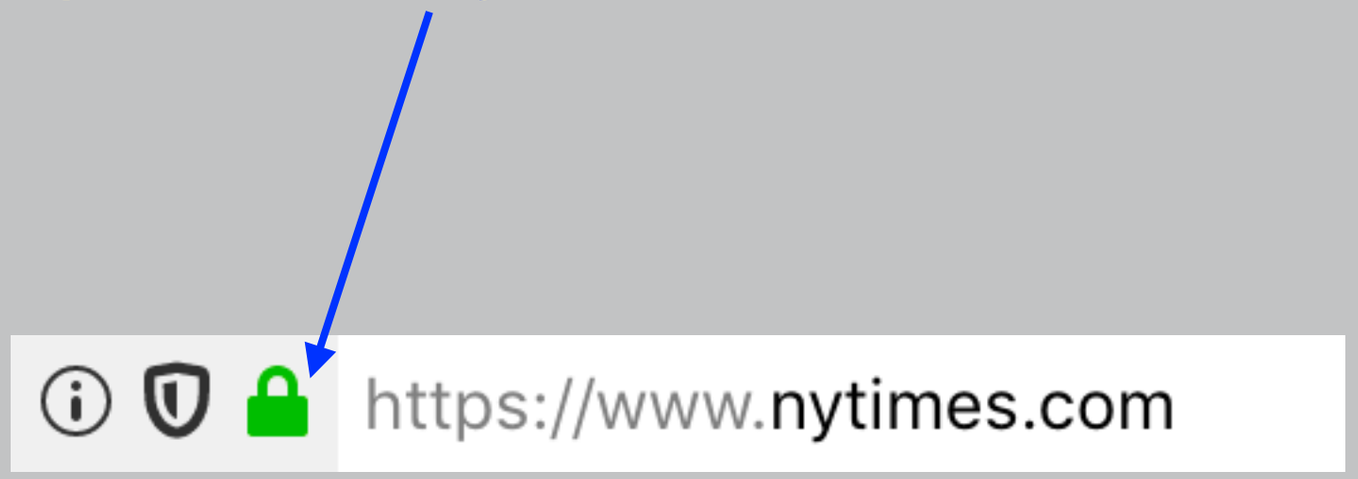
(UN)ENCRYPTED WEB TRAFFIC

1234 5678 9012 3456

How can Alice (as a human) know if her web traffic is encrypted or not?

HTTPS

the green padlock used to mean that your traffic was encrypted
(you are using secure HTTP, or **HTTPS**)



HTTPS

this is a **positive indicator**

(there is something there in the good case)

DO POSITIVE INDICATORS WORK?

"The Emperor's New Security Indicators", Schechter et al., 2007.

		Group				
Score	*First chose* not *to enter password...*	*1*	*2*	*3*	*1* ∪ *2*	*Total*
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
	Total	18	17	22	35	57

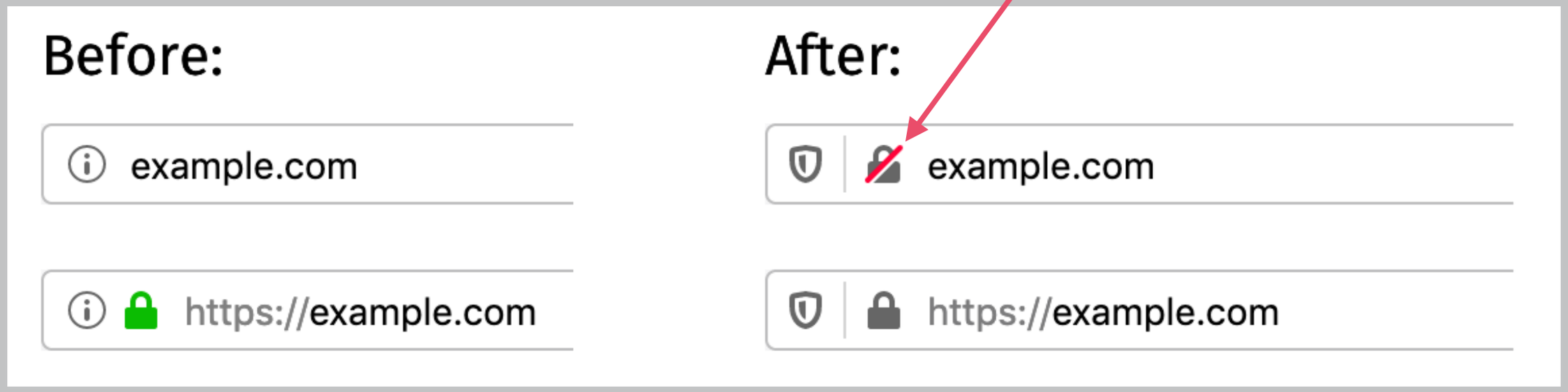
significant increase when presented with a **negative indicator** (warning page)

BEFORE...

absence of positive indicator

positive indicator

BEFORE... AND AFTER



HTTPS INDICATORS IN 2018

Status	Chrome	Firefox	Edge	Safari	Opera	Notes
HTTP						No indicator shown.
Mixed HTTPS (active content)						Some browsers warn against mixed active content.
Mixed HTTPS (passive content)						All browsers show a positive indicator. Most commonly a lock icon.
HTTPS (DV)						All browsers show a positive indicator.
HTTPS (OV)						All browsers show a positive indicator.
HTTPS (EV)						All browsers show a positive indicator, but most browsers show the verified name of the organization in a green color.

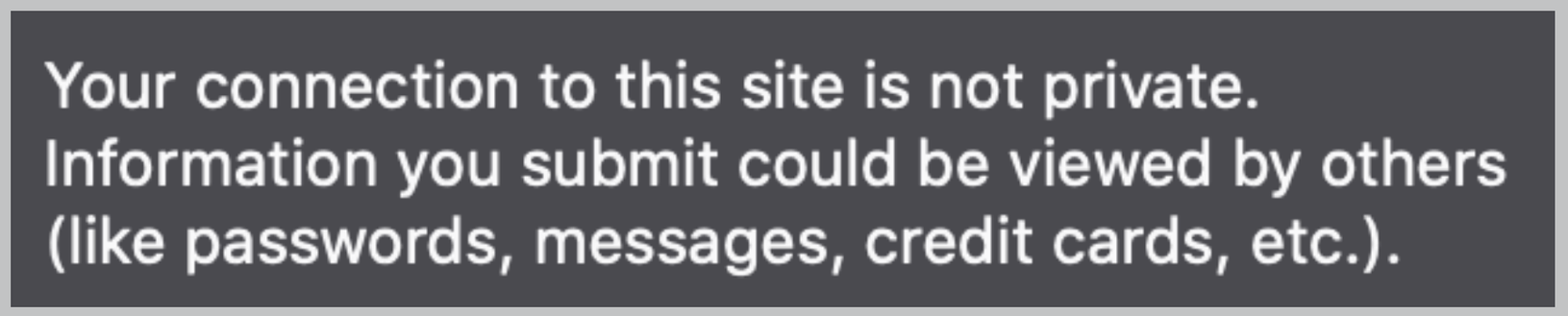
HTTPS INDICATORS TODAY: DEMO

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

secure
(encrypted)

insecure
(unencrypted)

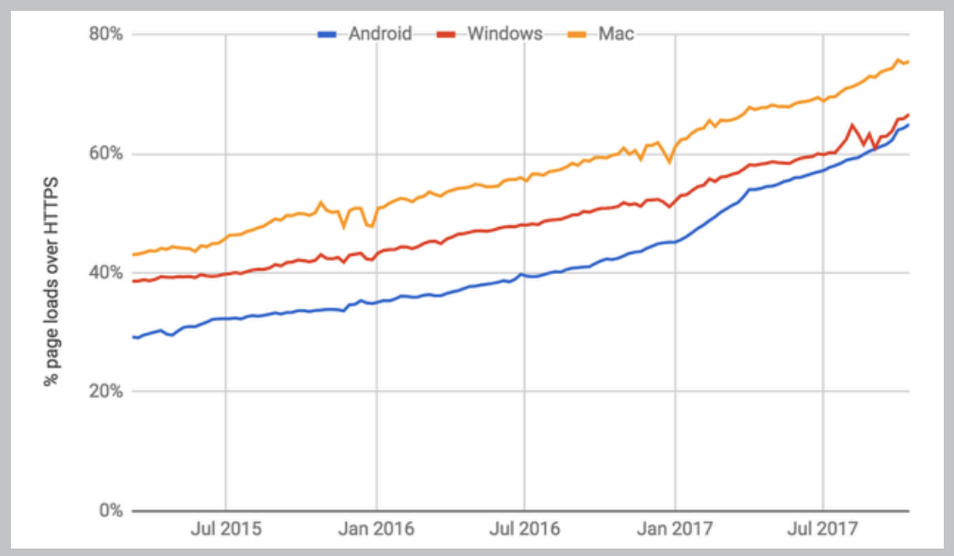


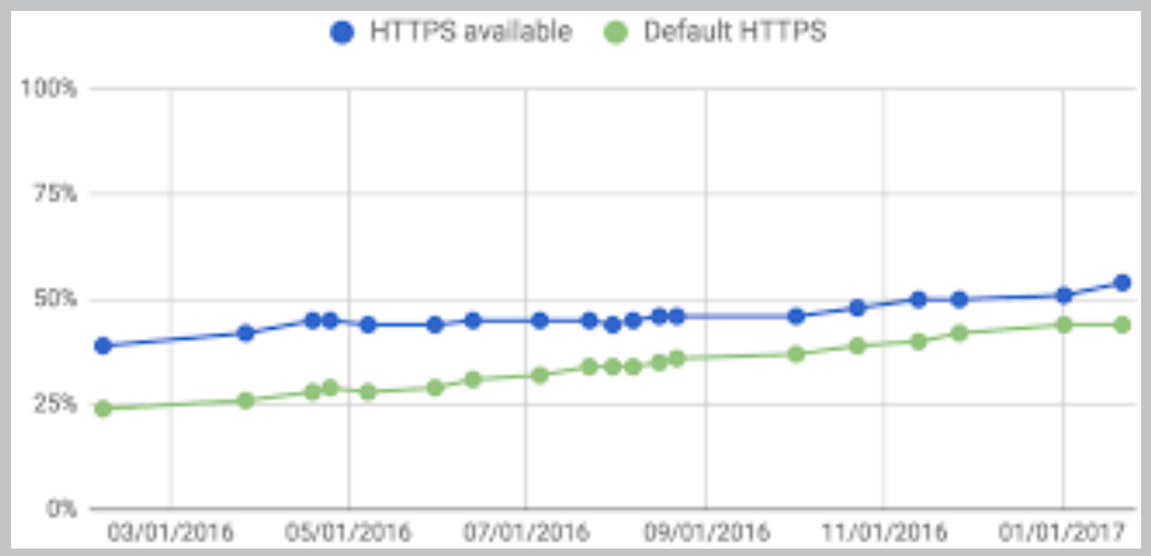
USABLE ENCRYPTION

Success story for usable security!

- Studies showed that old (positive) indicators were not usable and thus did not protect users
- As a result, browsers moved or are moving towards negative indicators instead

This was enabled by technological advances (which we'll see next week) that also made HTTPS much more widespread





QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2746845`

to take this week's quiz!