RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART3-W09

HTTPS: Why Privacy Doesn't Equal Security

Hal Lonas
SVP & CTO, SMB and Consumer
OpenText

David Dufour
VP Cybersecurity & Engineering
OpenText

Who are these guys?

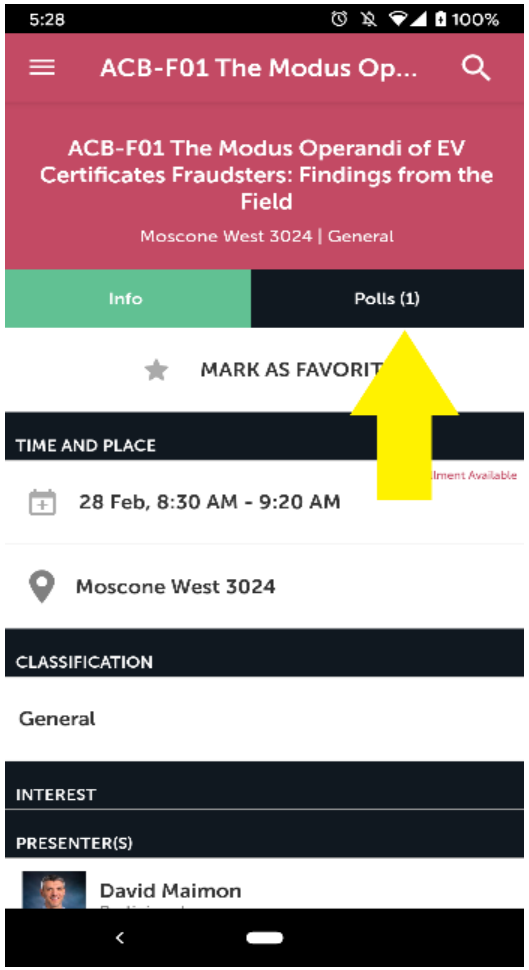
HAL LONAS
SVP and CTO

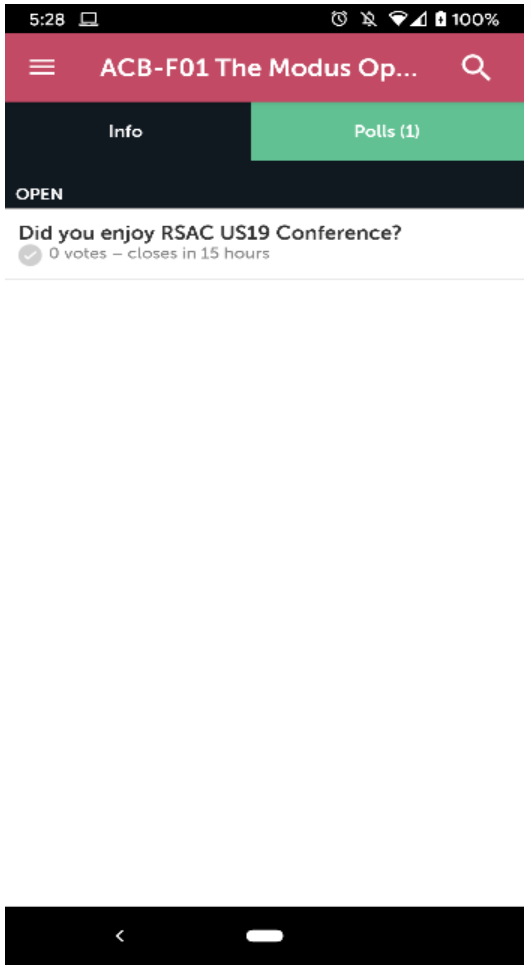
SUPERPOWERS
- Ultimate frisbee
- Machine learning /AI
- Cybersecurity since 2000

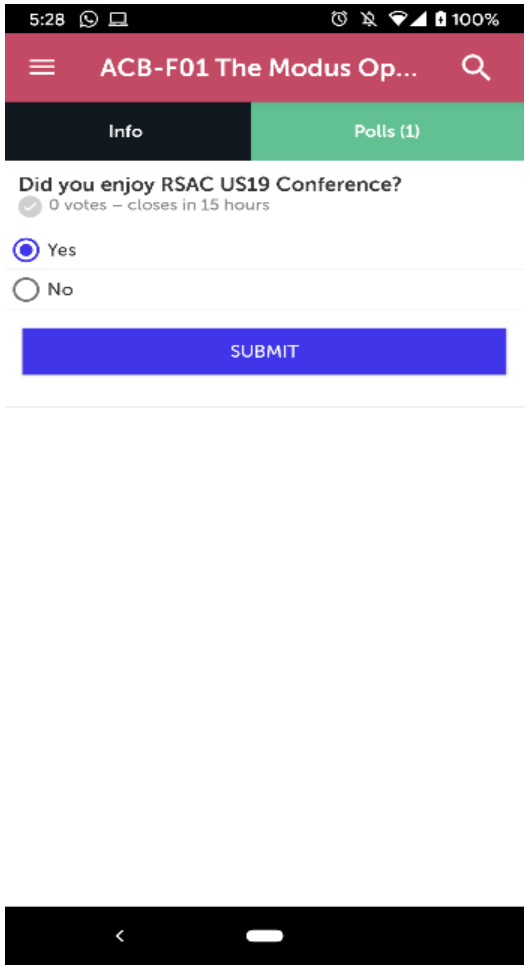
DAVID DUFOUR
VP Engineering & Cybersecurity

SUPERPOWERS
- Skateboarding
- Cybersecurity

Get Set Up With Polling
Session ID: PART3-W09





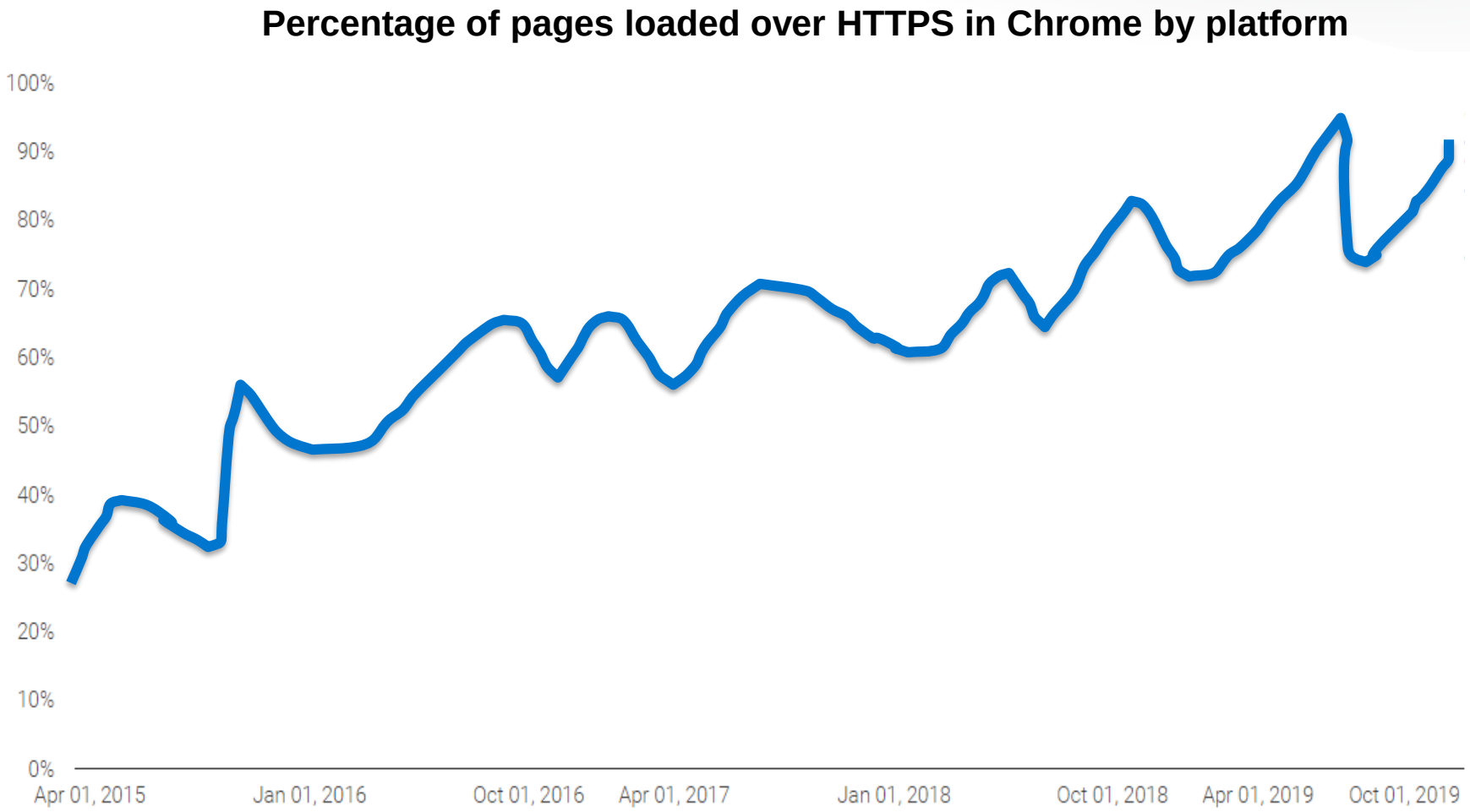


POLL: Users spend what percentage of their time on HTTPS pages?

- 22%
- 57%
- 90%
- 100%

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663

The growth of HTTPS adoption



Desktop users load **more than half** of the pages they view over HTTPS and spend **close to 90 percent** of their time on HTTPS pages.

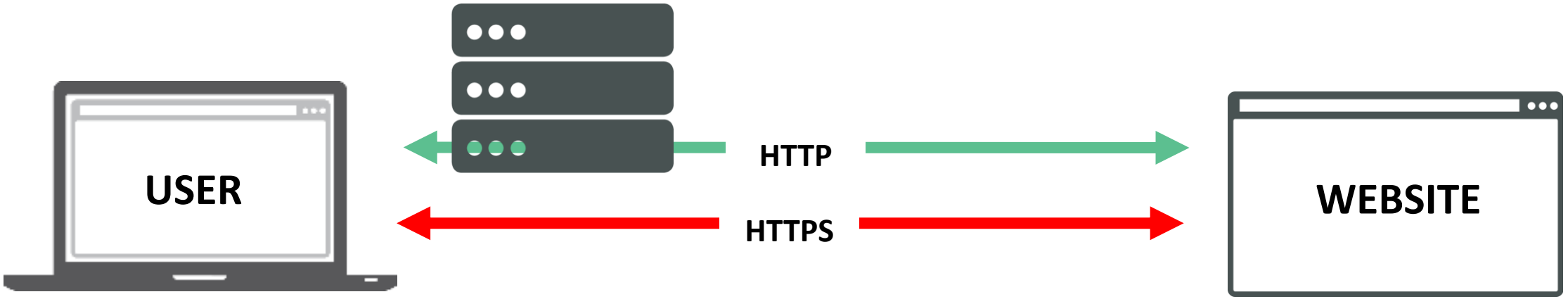
https://transparencyreport.google.com/https/overview?hl=en

Of the phishing and malware domains Webroot identified to be active in July of 2019, **54%** of them were listening on port 443.

F5 Labs "2019 Phishing and Fraud Report"

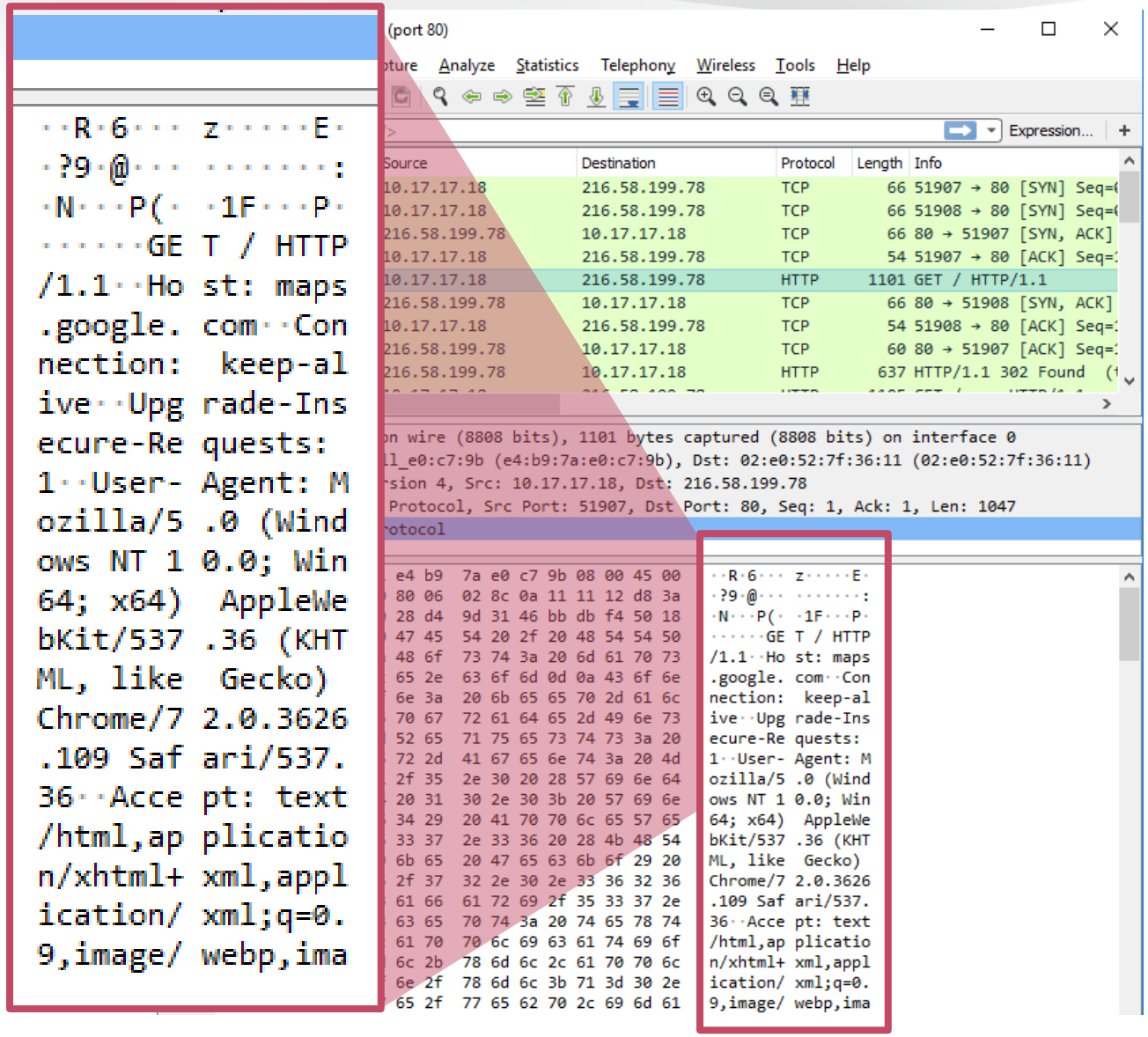
Let's discuss the privacy vs. security debate

Architecture

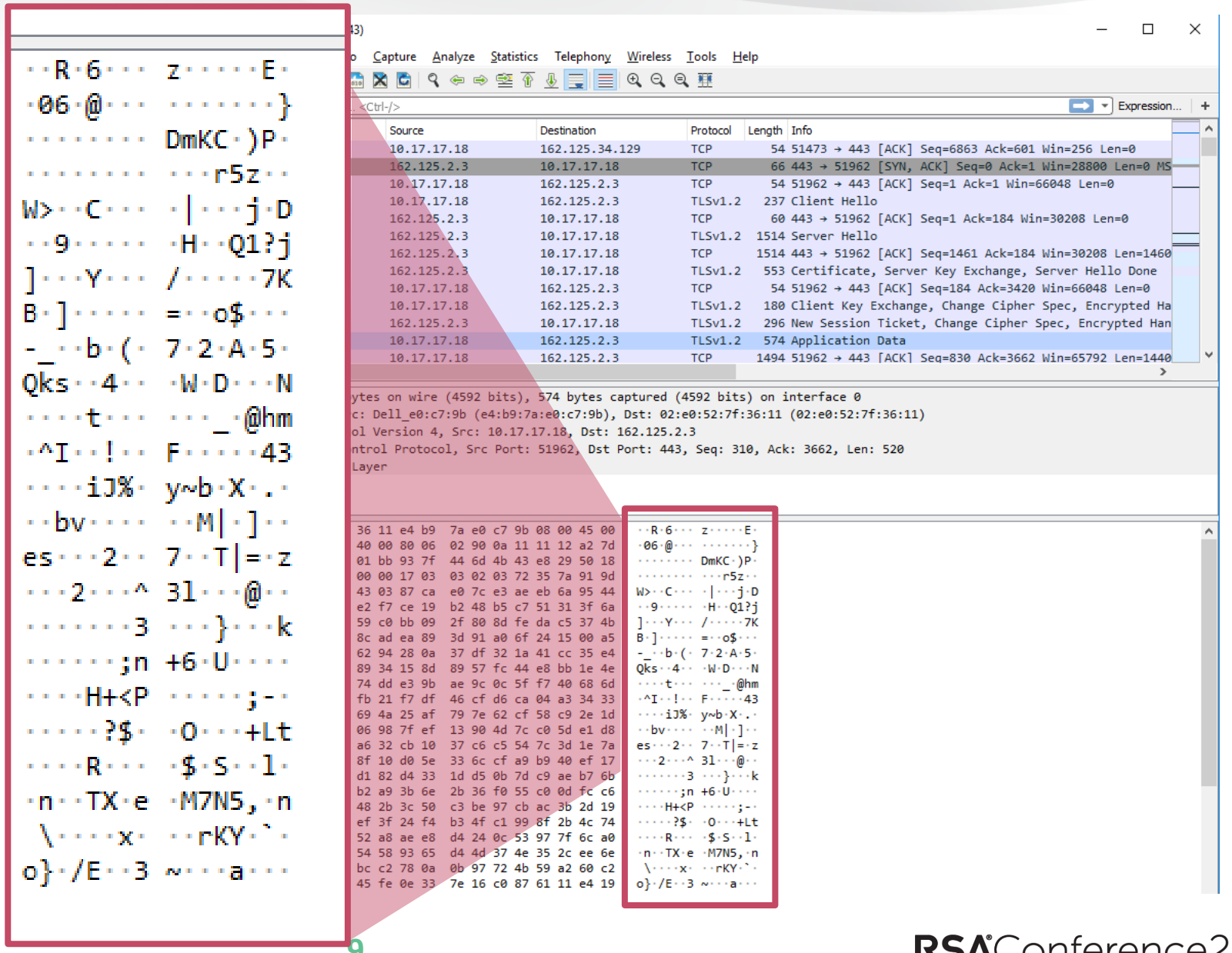


Don’t have full visibility with HTTPS

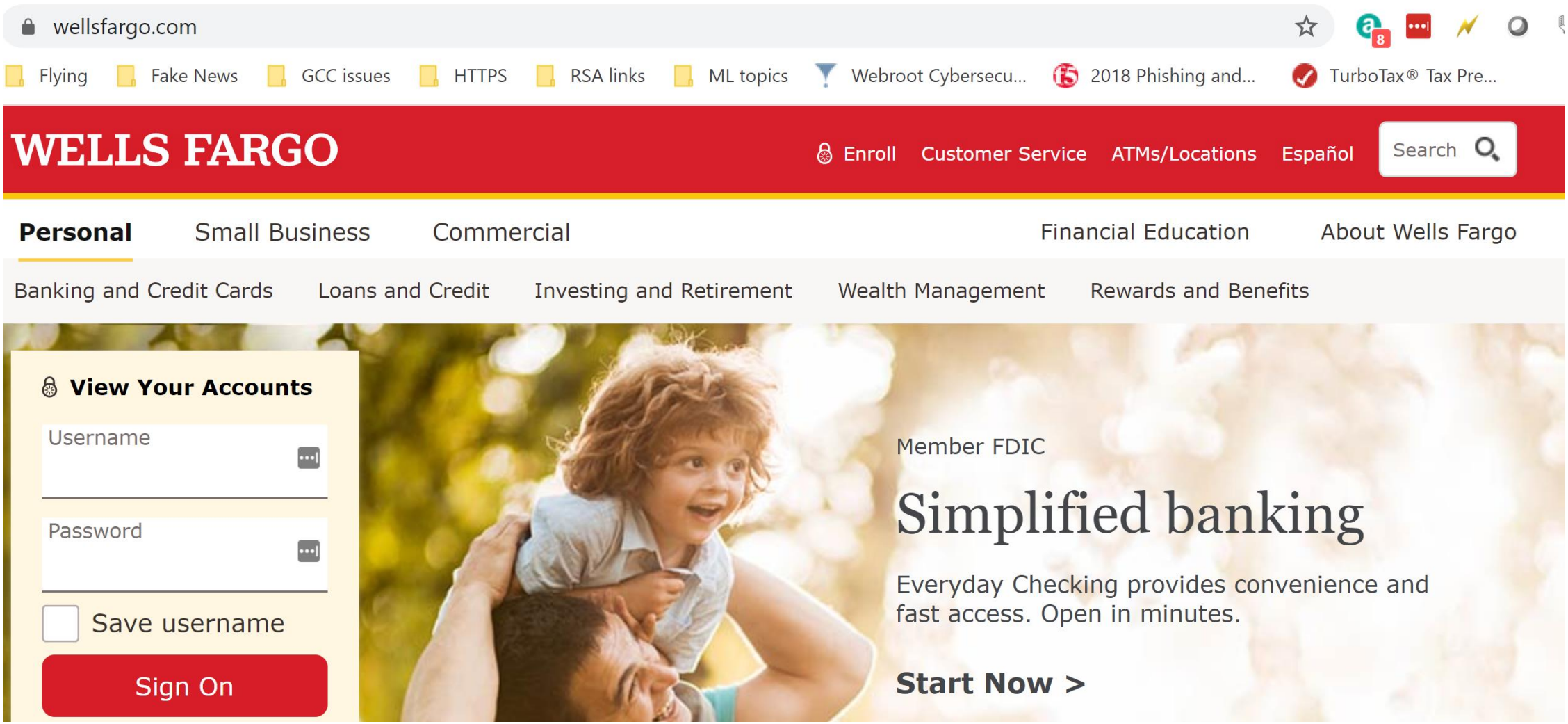
HTTP vs. HTTPS



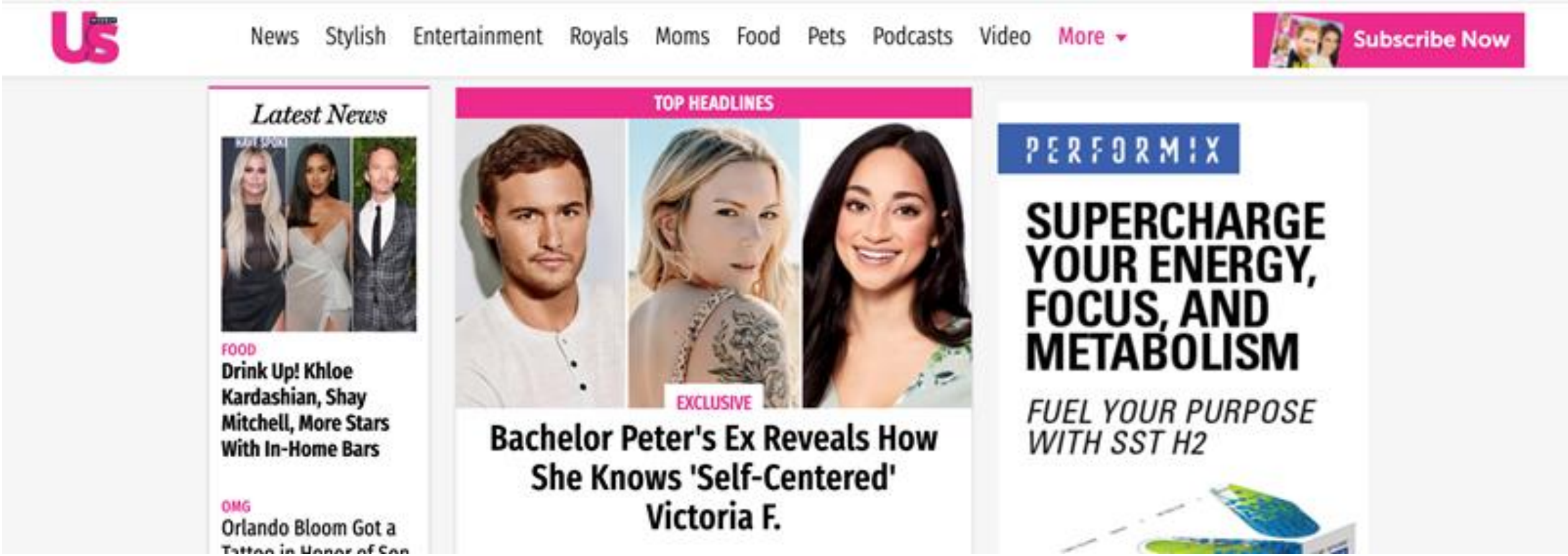
HTTP vs. HTTPS



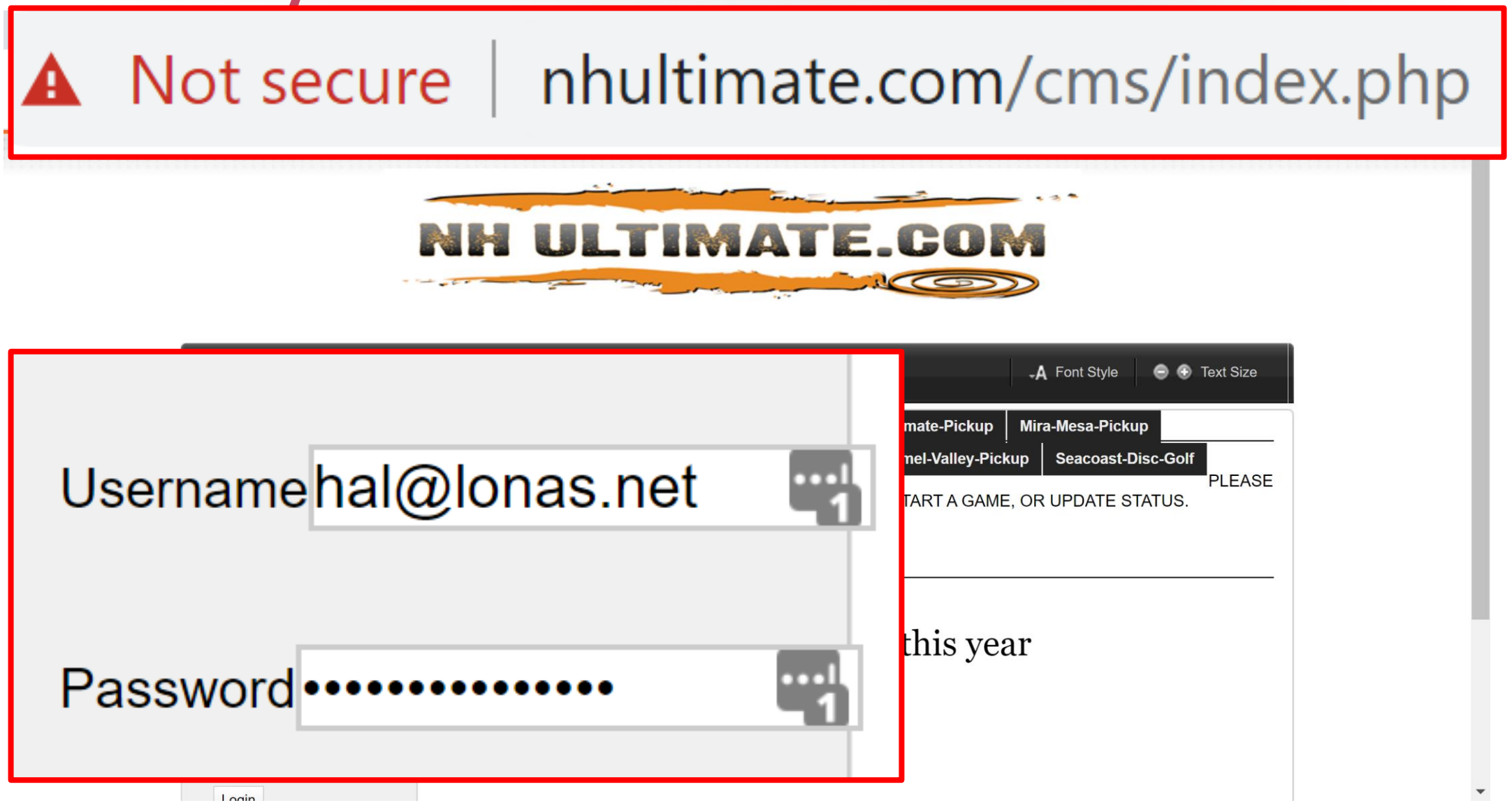
Does every website need to be HTTPS?



Does every website need to be HTTPS?



Does every website need to be HTTPS?



POLL: If you were forced to pick, what is most important to you and your organization?

- **Privacy**
- **Security**

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663

RSAConference2020

The Problems HTTPS Creates

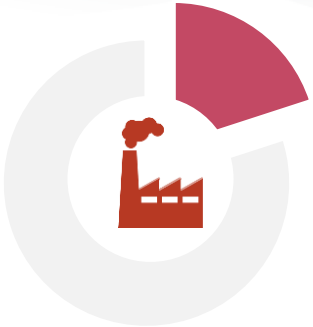
POLL: What percentage of malicious sites are found on benign domains?

- 2%
- 24%
- 64%
- 82%

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663

The HTTPS Security and Policy Gap

1 in 4 (24%) malicious URLs is hosted on an otherwise non-malicious sites



20% Non-malicious sites hosting bad URL: Manufacturing

27% of phishing sites used HTTPS to trick users into thinking the site was safe

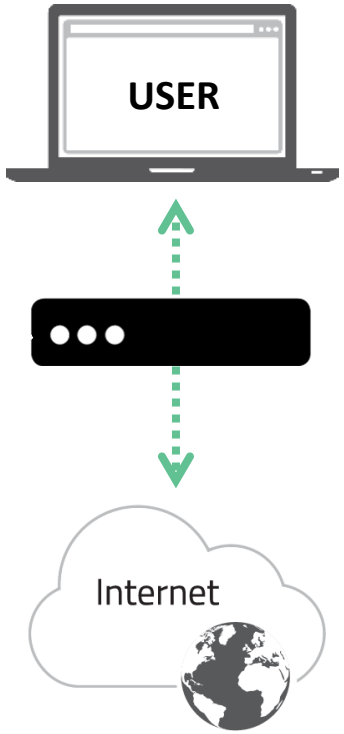
Based on Webroot URL categorization data from January to November 2019.

Privacy vs. Security: What does it mean for network devices?

http://docs.google.com/hacker/sketchyfile/page.html

domain

path



http://www.docs.google.com/hacker/sketchyfile/page.html

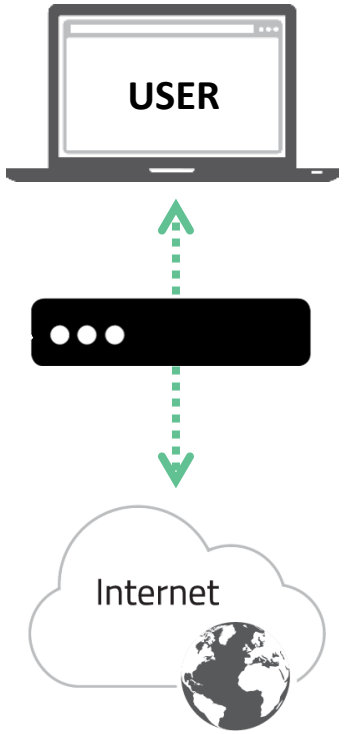
http://www.docs.google.com/hacker/sketchyfile/page.html

Privacy vs. Security: What does it mean for network devices?

https://docs.google.com/hacker/sketchyfile/page.html

domain

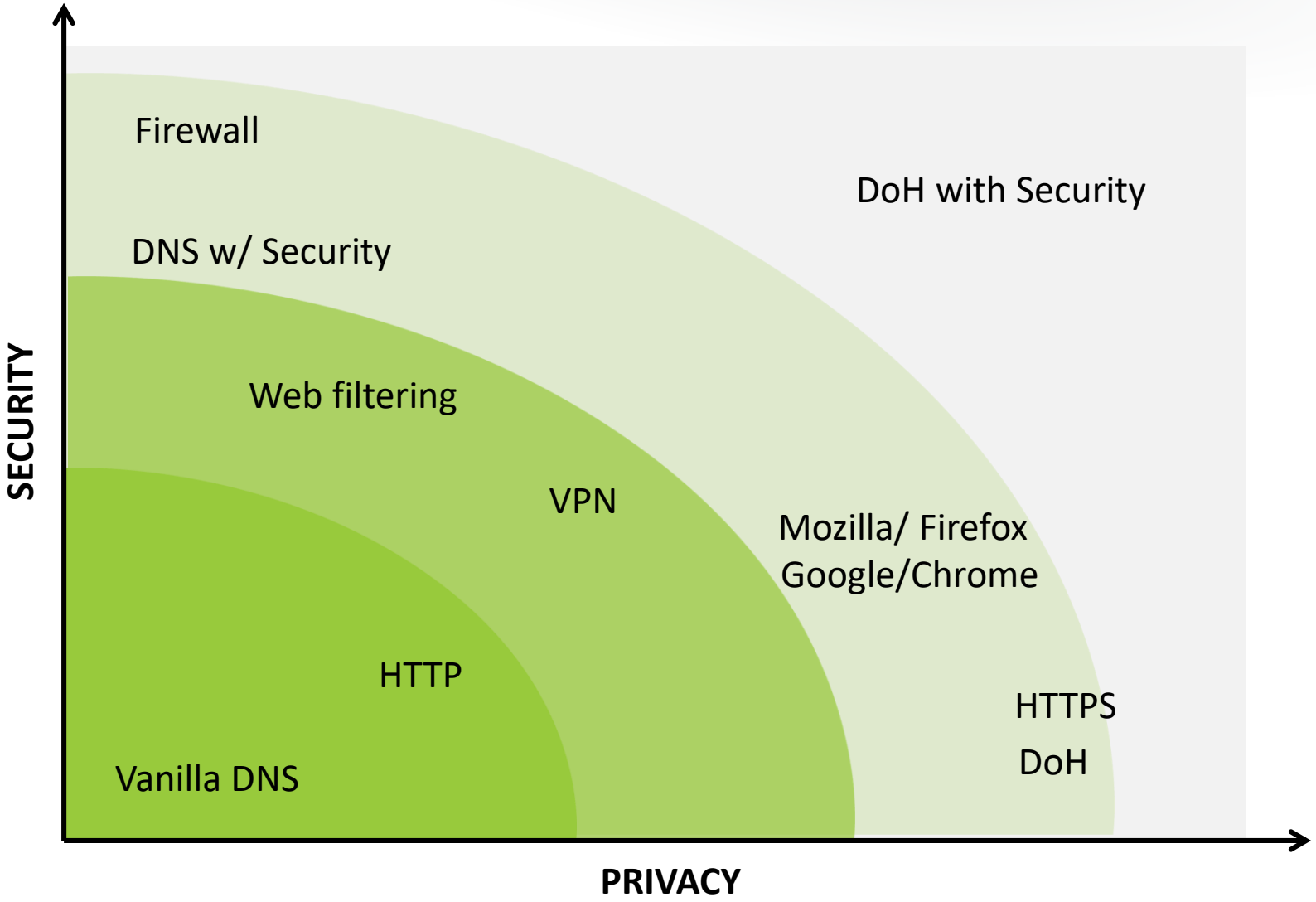
path



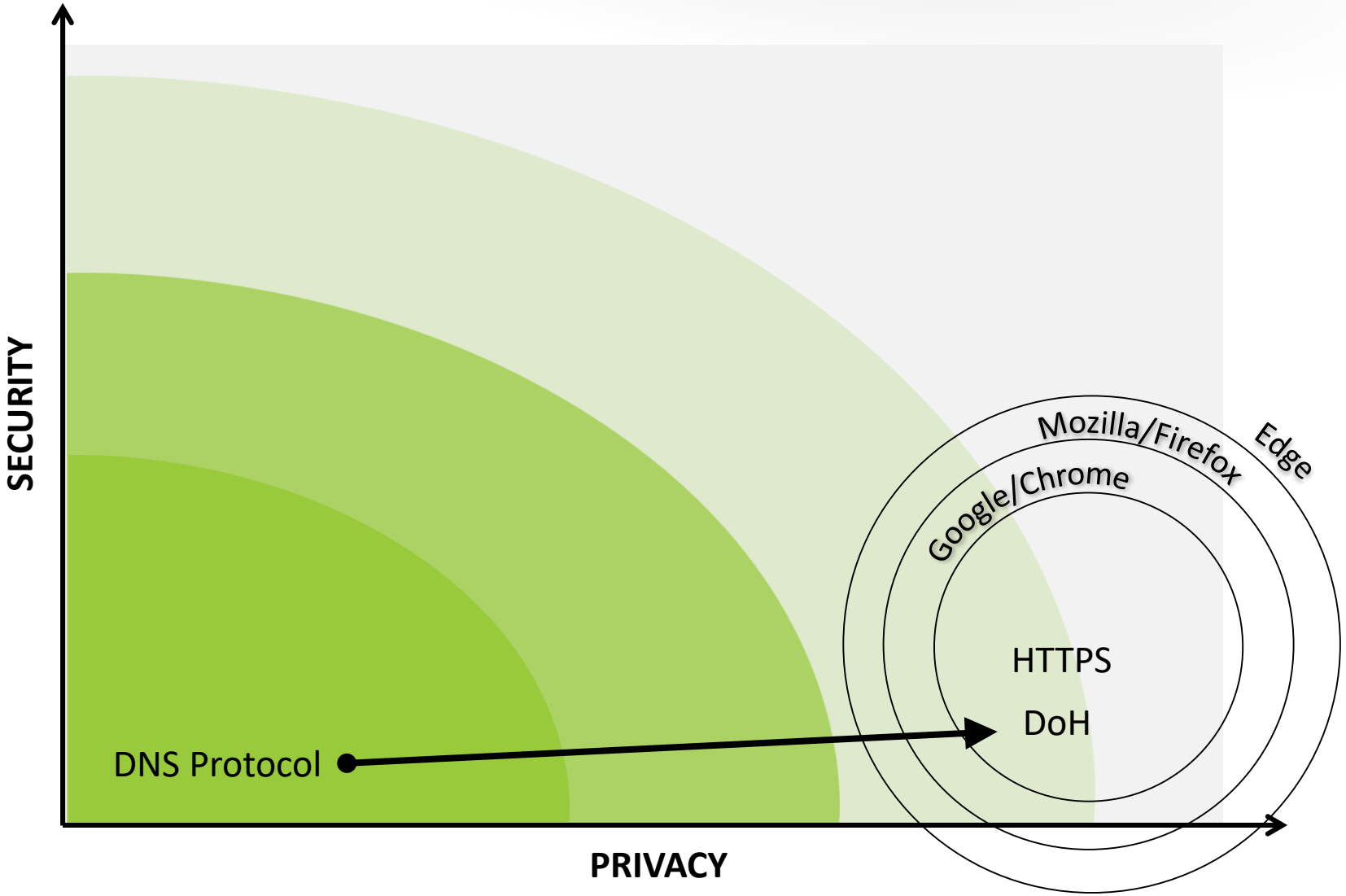
https://www.docs.google.com/hacker/sketchyfile/page.html

https://www.docs.google.com/4fd9bfc48f6728bd636f9418c29851a5

Spectrum of choices



When DNS meets HTTPS



Godlua – The first malware to leverage DoH

Godlua, a Linux DDoS bot, is the first-ever malware strain seen using DoH to hide its DNS traffic.

RSAConference2020

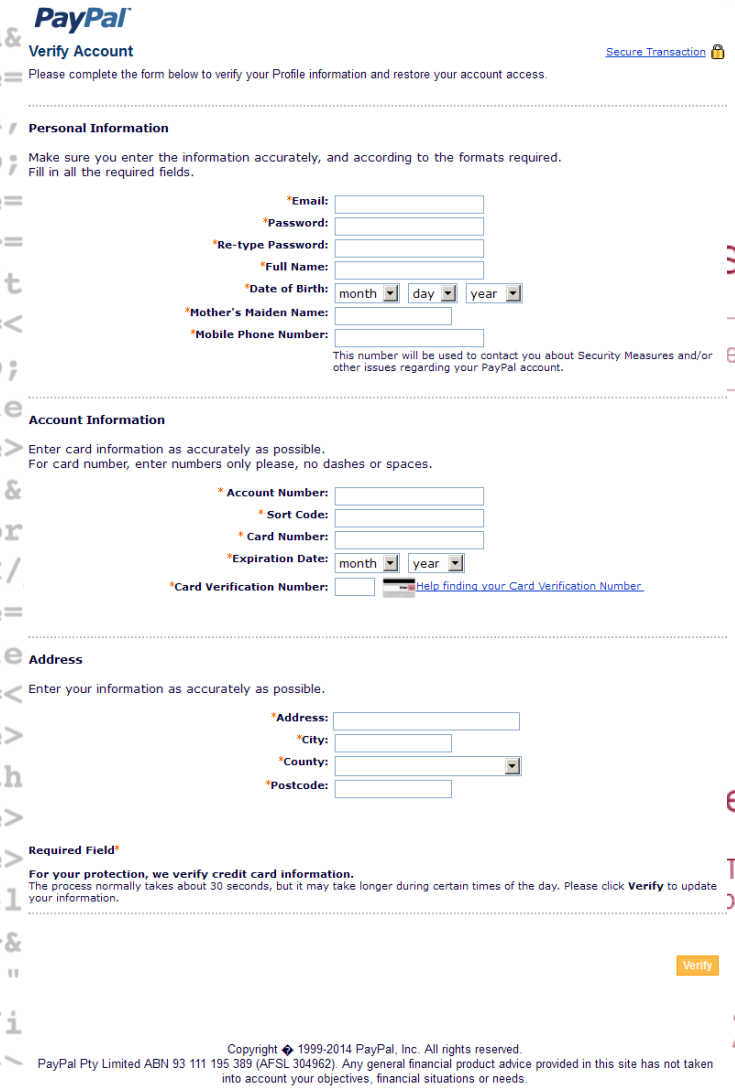
Cybercriminals & HTTPS

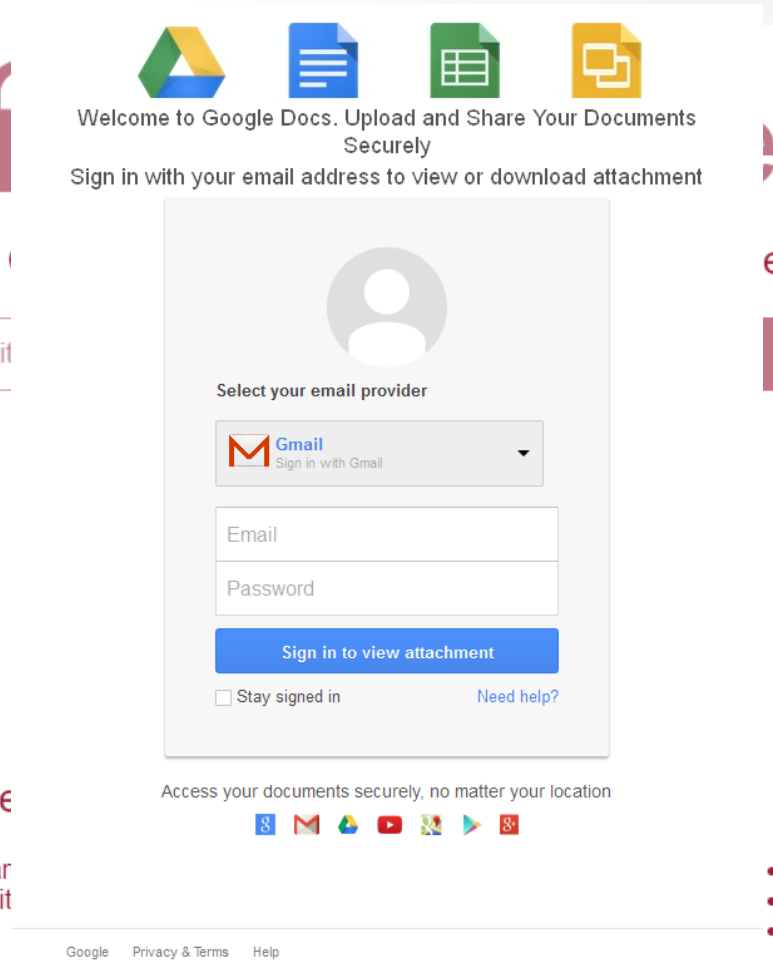
POLL: Did your last malware attack come over HTTPS?

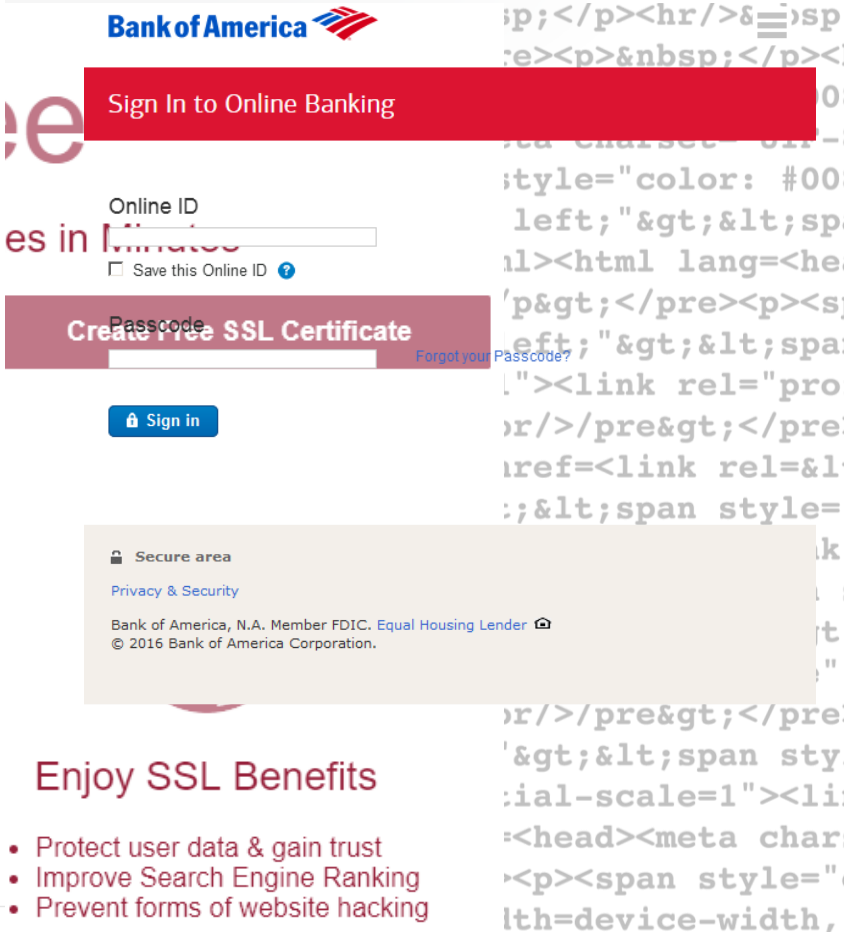
- Yes
- No
- I don't know

https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663

What are the ingredients to make the bomb?



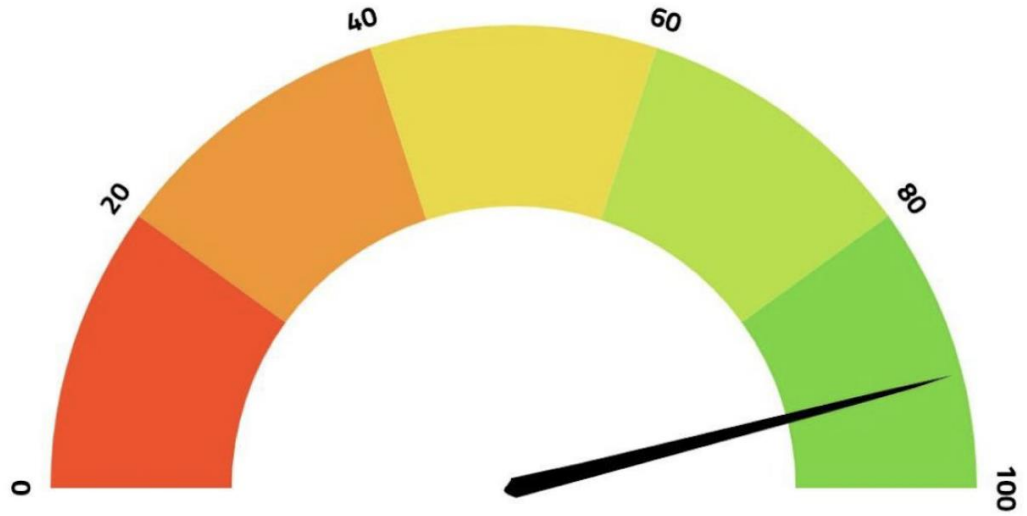




2,000,000+ Free SSL Certificates Created

We put security certificates to the test

https://webroot.com



Score: 92

Score Summary

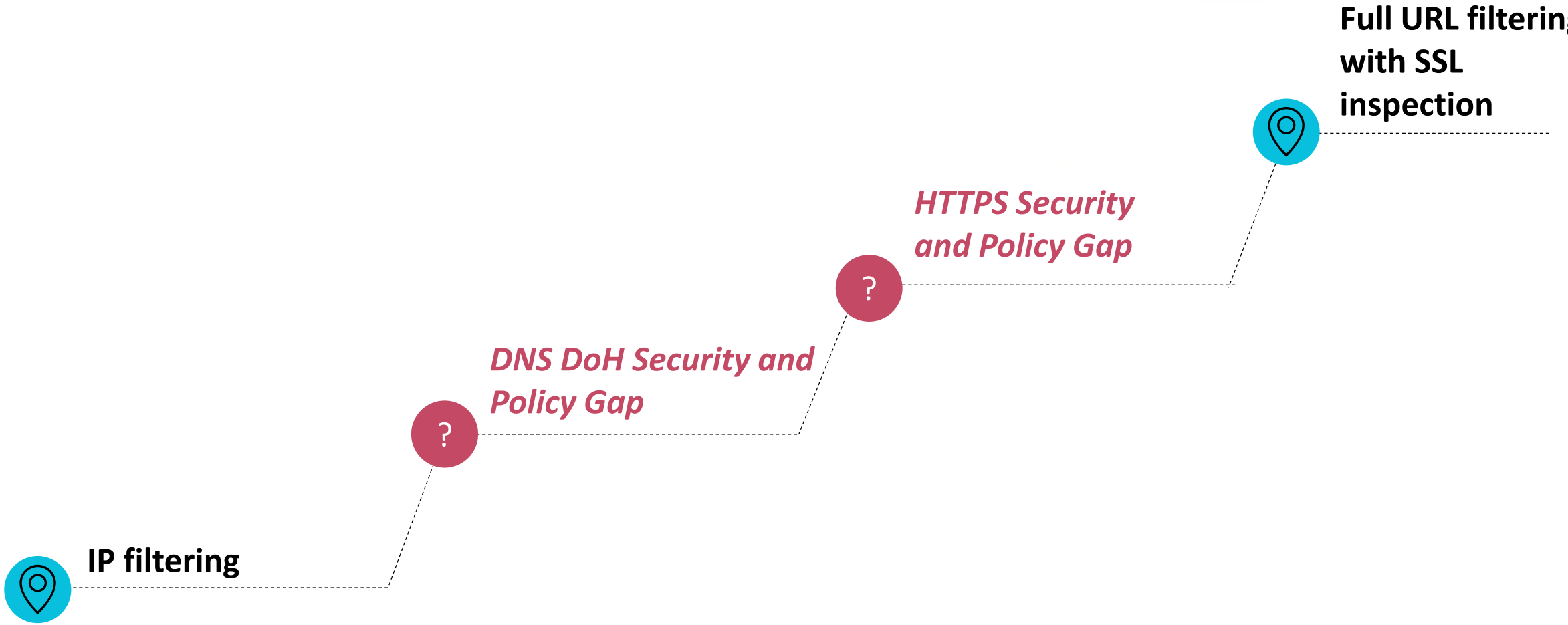
These are safe certificates that have not been tied to phishing. There is a very low predictive risk that your infrastructure and endpoints will be exposed to attack.

HARVEY MUDD COLLEGE

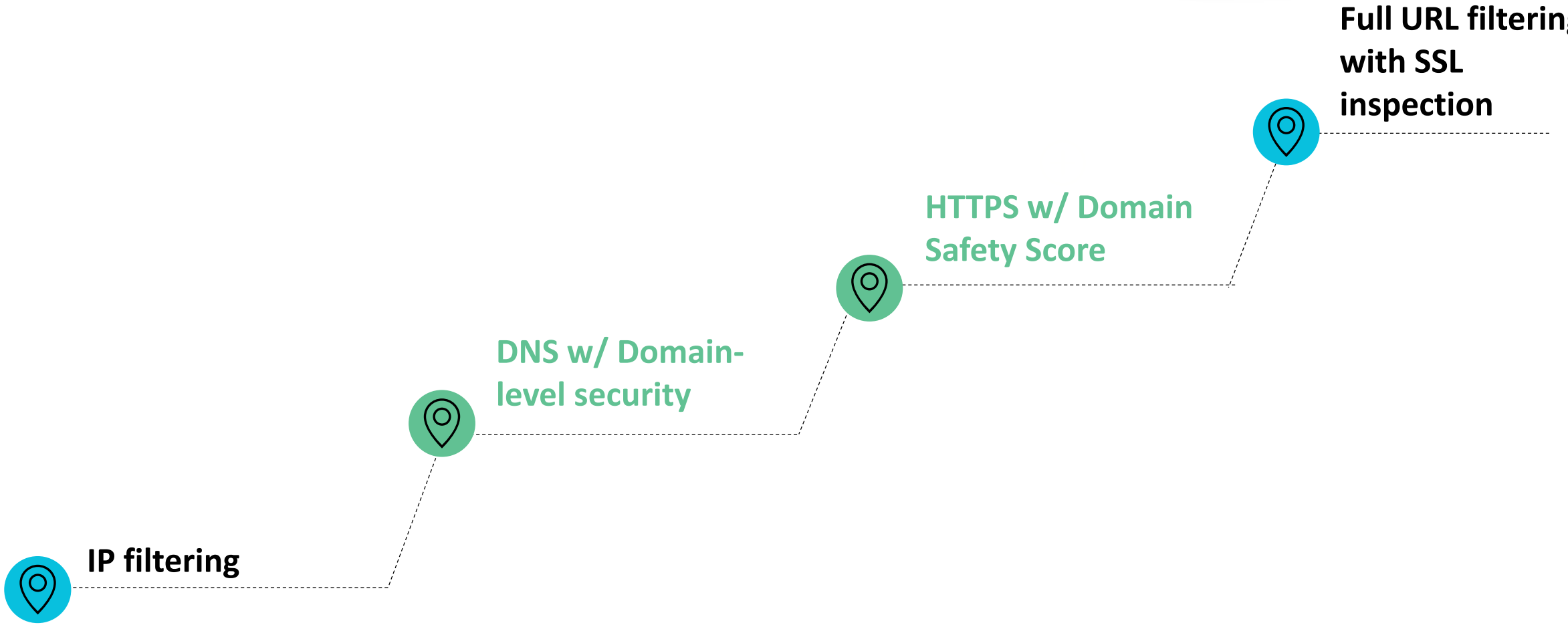
RSAConference2020

What the Future Holds

Current Solutions for Filtering on HTTPS Traffic



Filling the Gap: Classifying at the Domain Level



Recommendations to Security Professionals

		Domain level filtering
	Web filtering	Endpoint Security
Passwords	DNS / DoH	Patching
Training	HTTPs	EDR / MDR
Phishing Simulations	Firewall	MFA
Outsourcing / leaning on the experts	VPN	Backup
USER	NETWORK	DEVICE

RSAConference2020

Thank you!
Questions?

RSAConference2020

Continue the Discussion…
Visit booth S-635 for a conversation