SSL INDUSTRY TRENDS

CA DAY 2018

Dean Coclin
DigiCert

What do these mean?


STOP


PARE


Varuö


Harpa


Hello


P
Hitt Húsið


TAXI


TAXI


WC

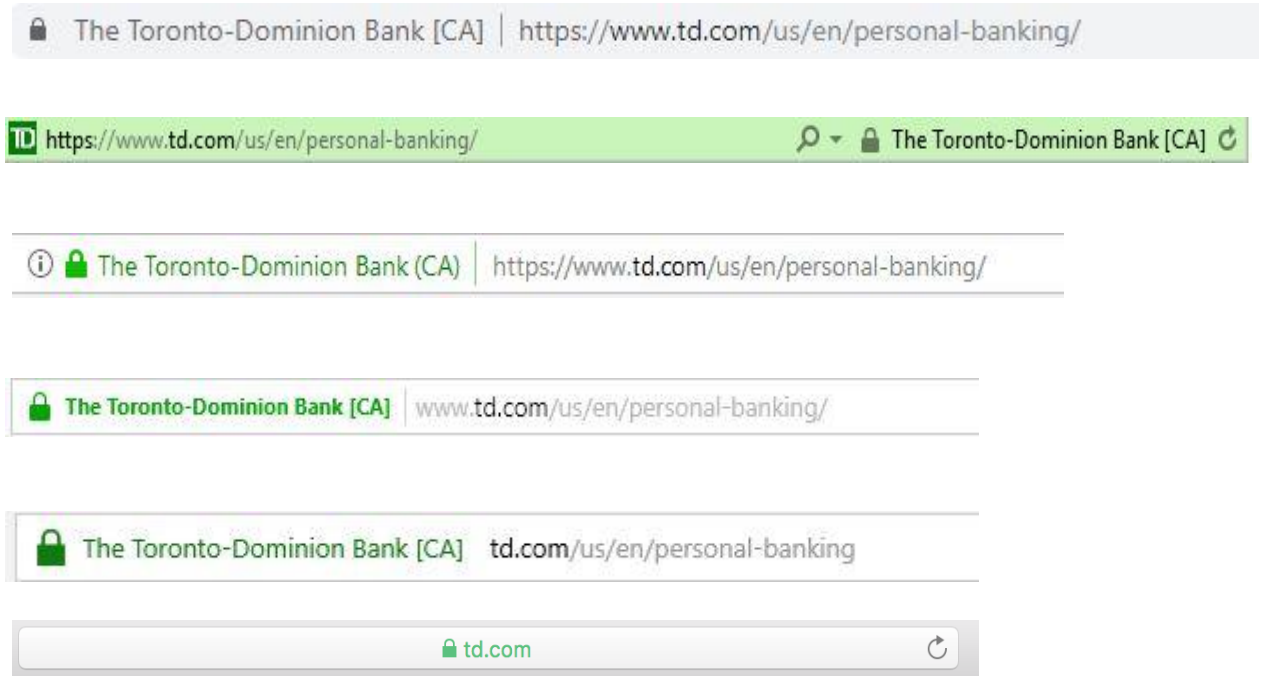

ata

Why do you know these?

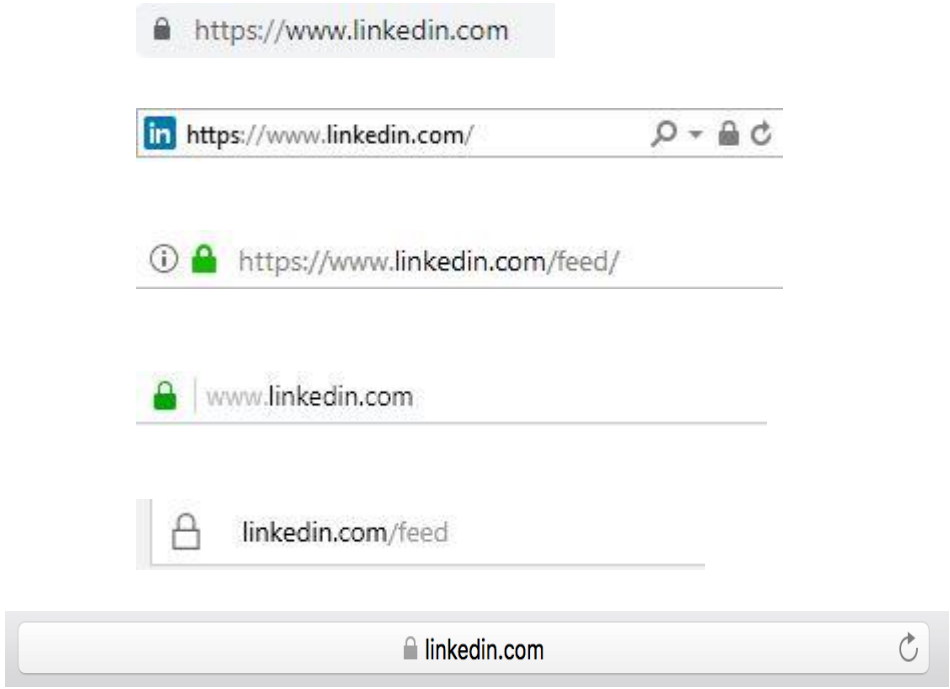
- You've had formal training
- Easy to understand
- Frequent repitition
- Universal, Global

→Large swath of the population knows what to do when they see these signs!

Now, how about these?



And these?



What do these tell us?

Green, Gray, Full name, domain name?

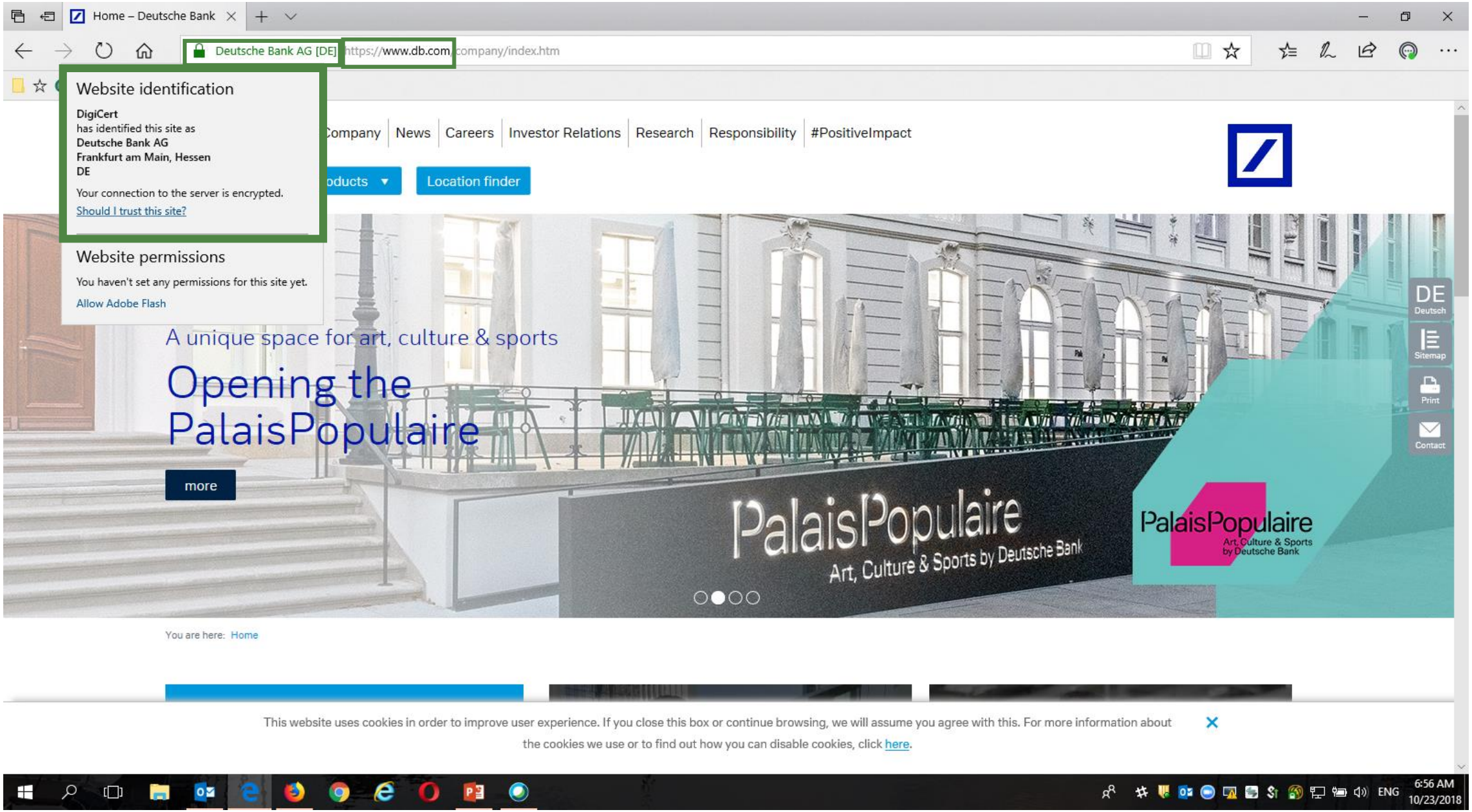
Green locks, Gray locks, Hollow locks?

Why are they hard to comprehend?

- Security indicators are hard to implement and get right!
- User education is needed
- Inconsistency makes it harder
- Evolve, but share consistency!

Security in Money – It's there when you need it

Security in EV – there when you need it



Why EV?

Extended Validation

- Anti-Counterfeiting – EV is distinguished, examinable, provides strong identity proof
- QWACs rely on EV
- Corporate security – control of domains, easier to spot fraud sites
- Use cases outside the browser – EV data can be consumed by a variety of *things*:
  - Managed Security Services
  - Internal Audit teams
  - Compliance groups
  - Firewalls
  - Automated Security Systems
  - AI security assistants

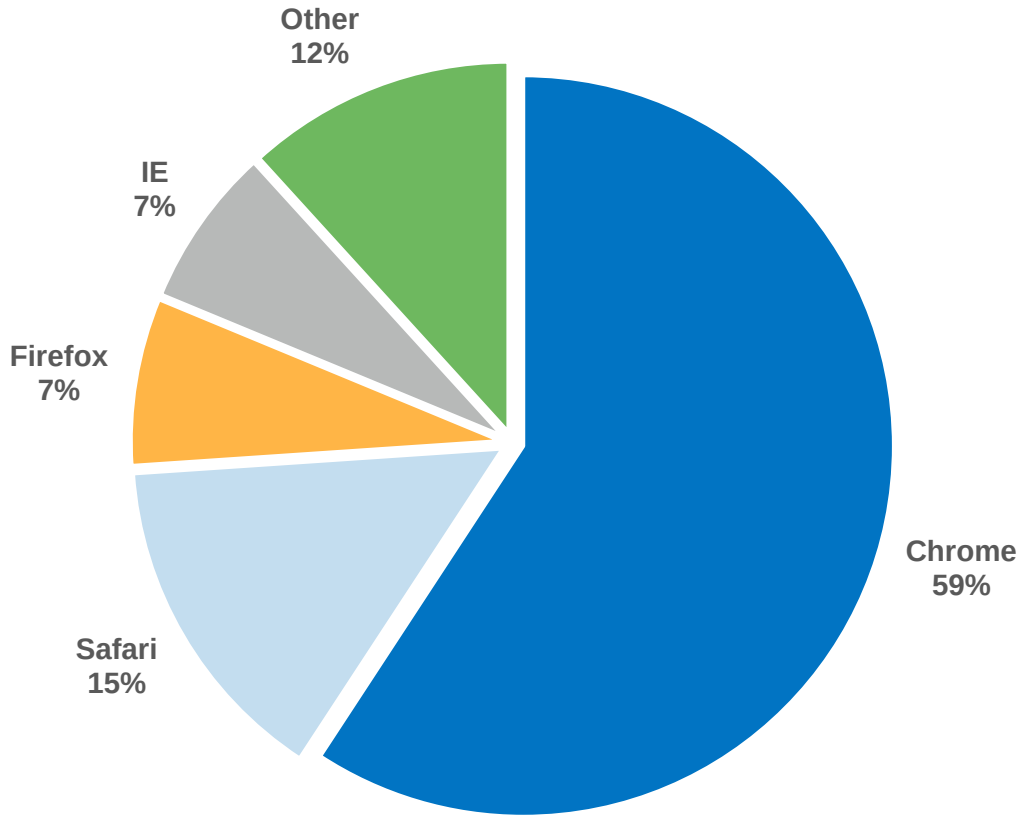
Identity is important, so what can we do to improve EV?

1. Require EV certificates to specify the method of domain validation used as information in the certificate
2. Require CAs to verify a registered trademark before issuing an EV certificate
3. Include trademark and brand information in a certificate
4. Provide a face-to-face verification with the certificate requester
5. Only issue EV certificates if certain security parameters (e.g., proper Transport Layer Security (TLS) version) are met
6. Require a valid CAA record prior to issuance
7. Require that the CA check the certificate type in the CAA record or respect a CAA policy regarding validation processes prior to issuing
8. Require CAs to log the identity with an identity blockchain
9. Include LEIs in certificates

- Discuss in CA/B Forum Validation Working Group and add these to EV Guidelines

https://www.digicert.com/blog/ev-certificates-digicert/

Browser Market Share



Source: WSJ Feb 2018

Since browser UI changes in treatment of http went into effect…

>78%

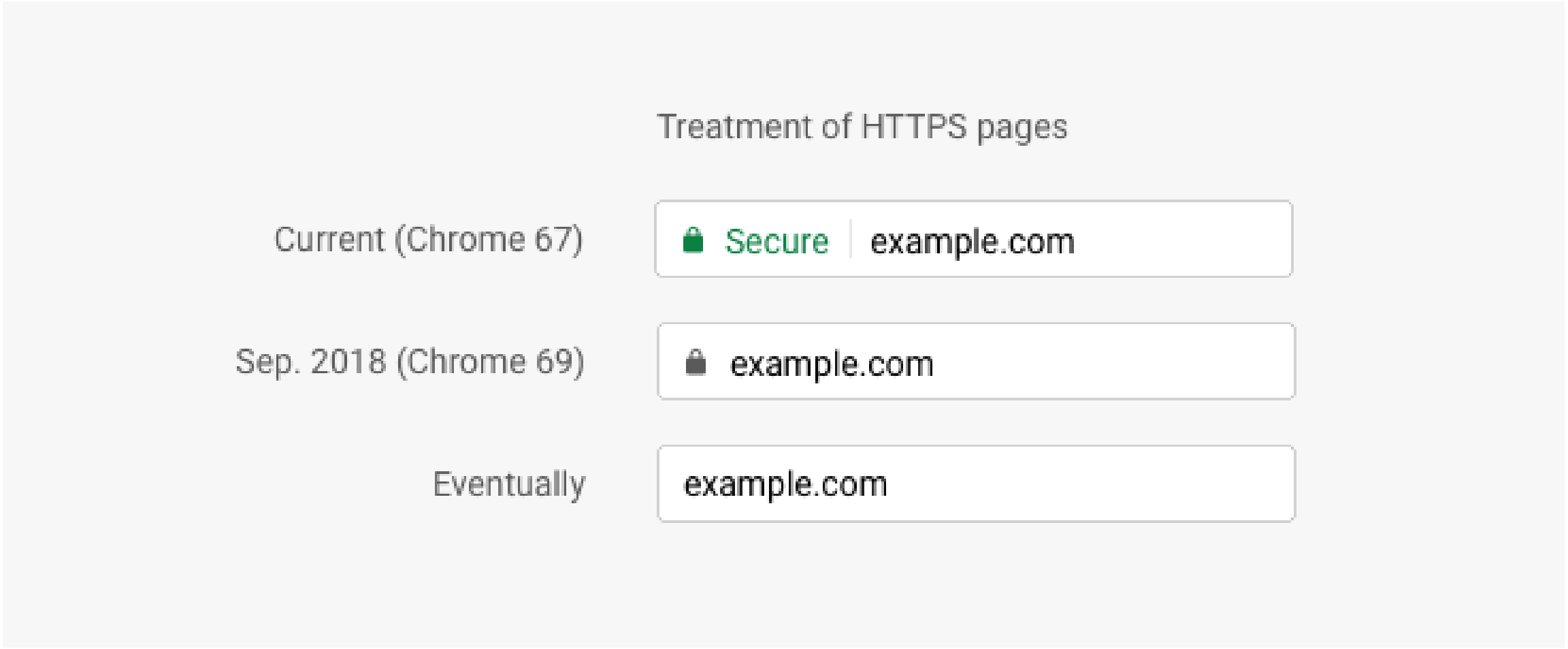
of page loads in Chrome over https

>68%

of page loads in Android over https

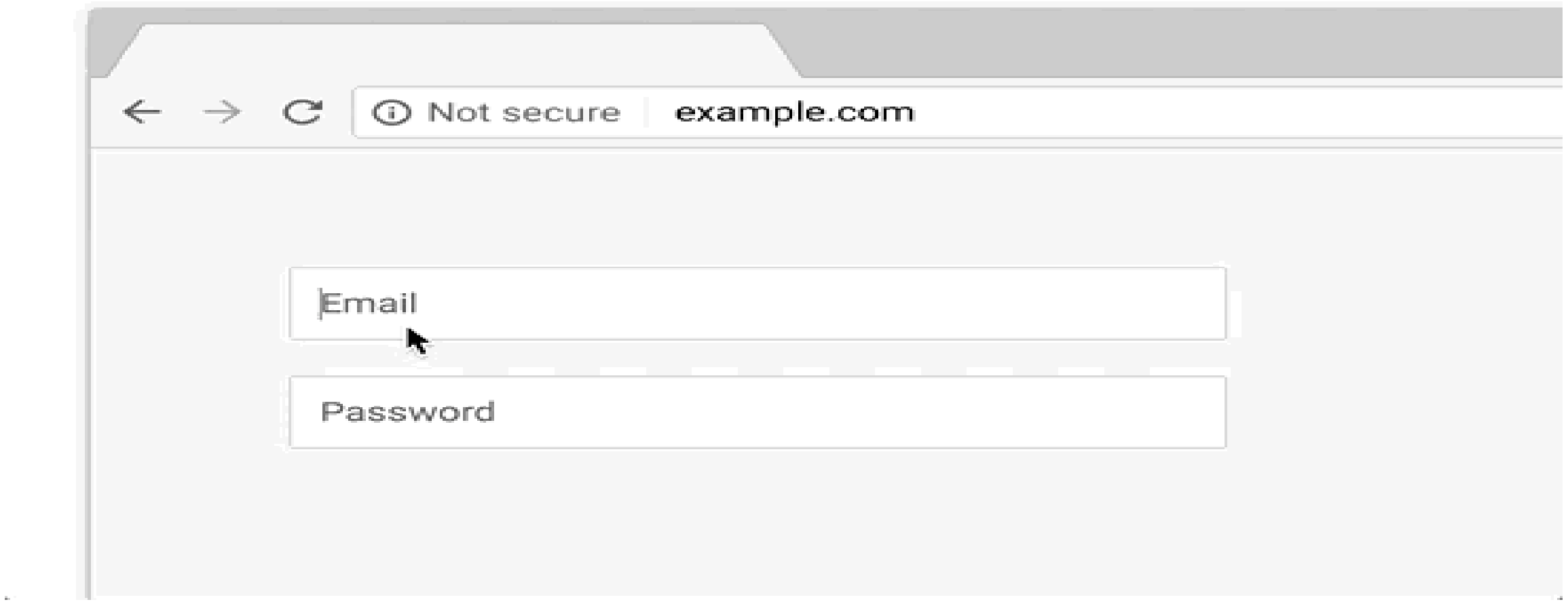
https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

Changes to Chrome



https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

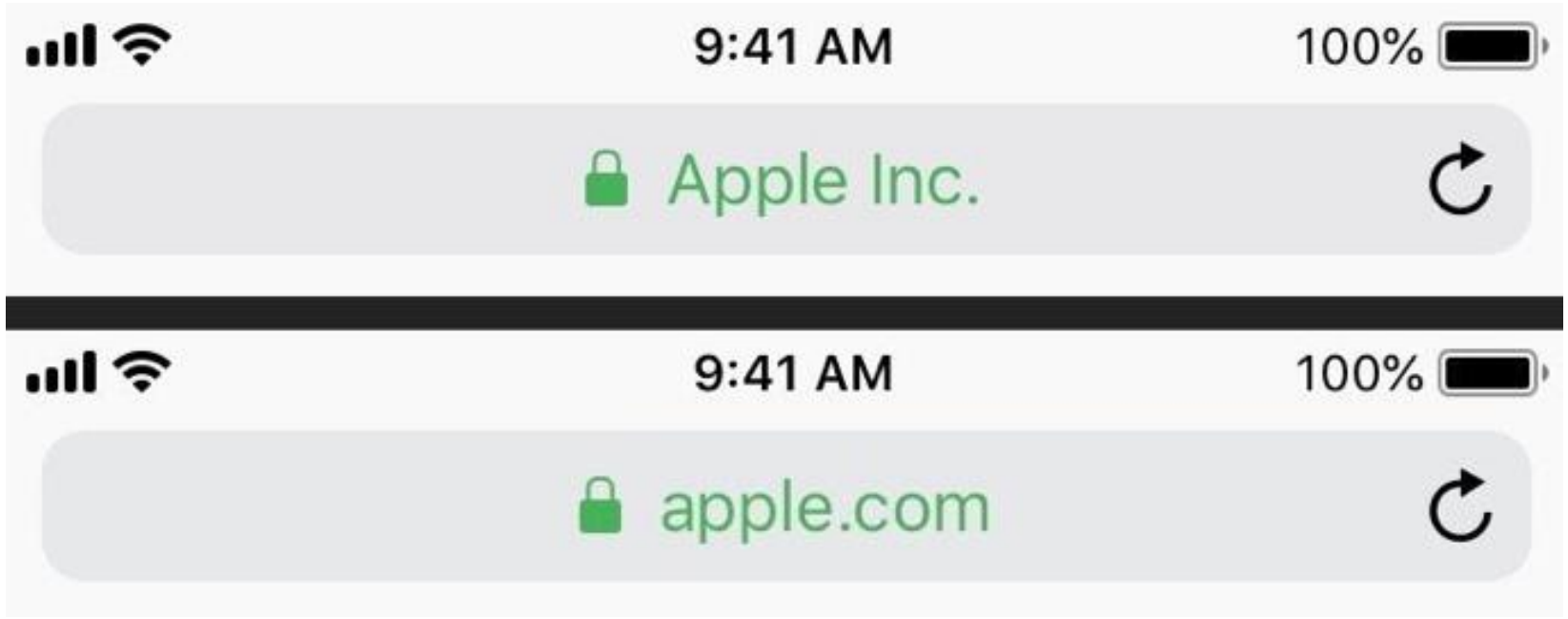
Treatment of http pages in Chrome 70 (October)



https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

Apple changes to Safari EV UI

- Changing from Apple Inc. (Company name) to apple.com (Domain name)
- Will maintain green lock next to the name



Publicly Trusted, Observable TLS Certificates

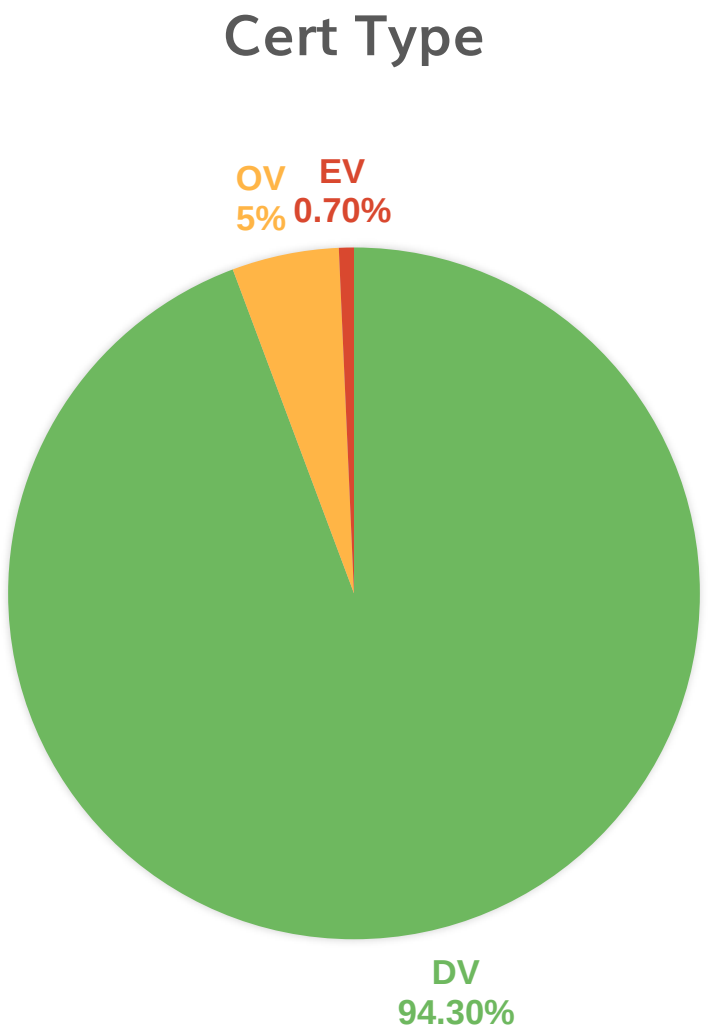
43.7M

Oct

- 3[illegible]6 Million certificates in J[illegible]e 2018 Netcraft report
  - +13.2 million from June 2017 (+68%)
  - +27.2 million from June 2016 (+500%)
- Most of the growth comes from Let's Encrypt and cPanel offerings
  - >24.8M certs
  - 81% of DV, 76% of all
- EV market up 21.1% since June 2017

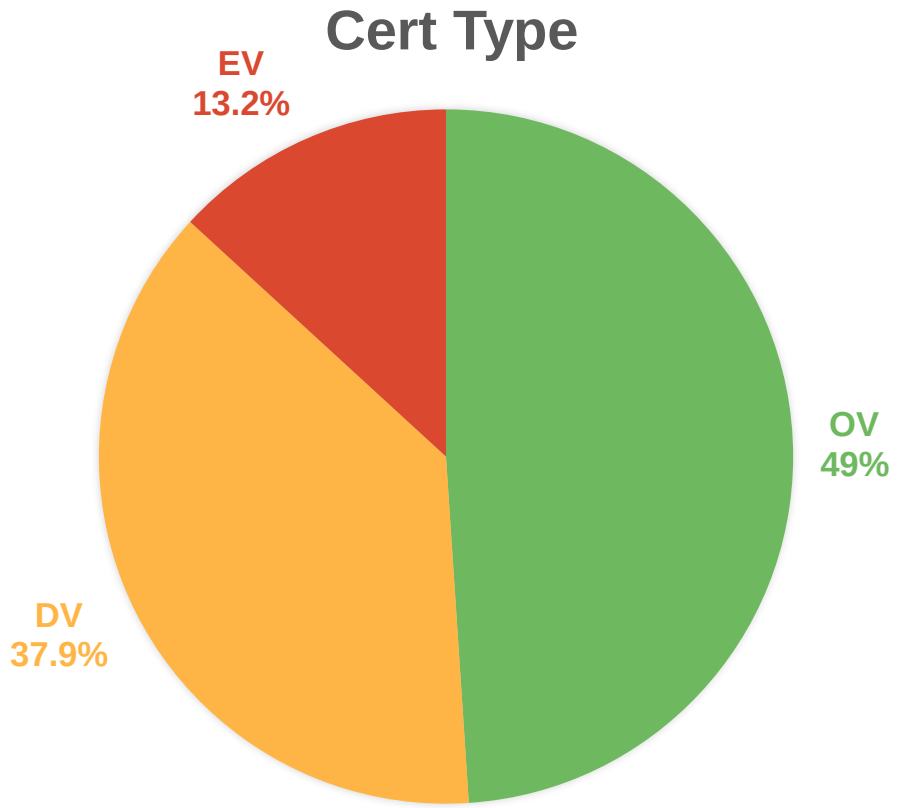
Source: Netcraft Data

Breakdown of Certificate Types



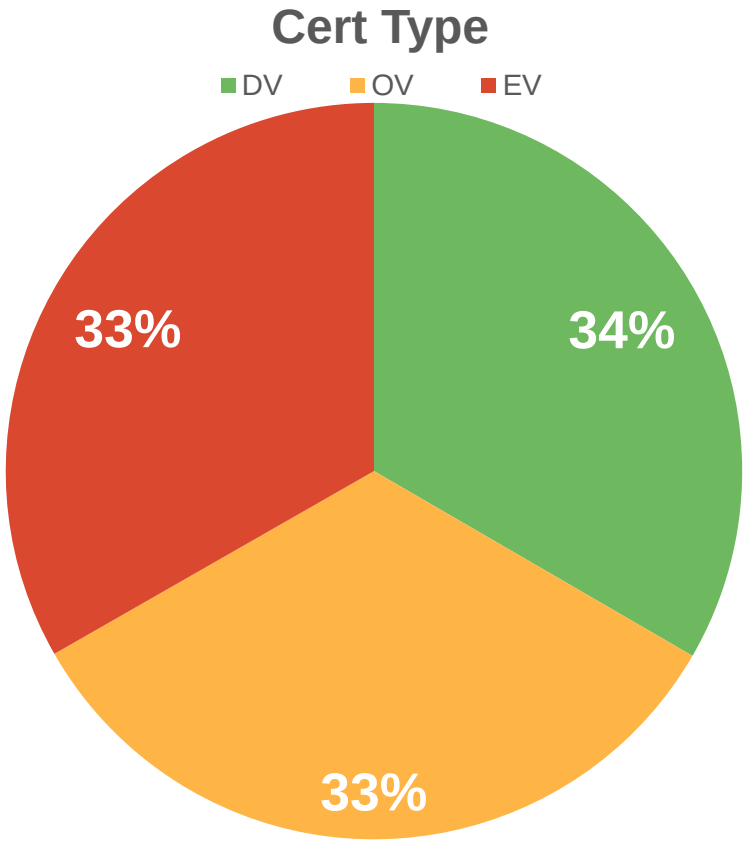
Source: Netcraft Data

Share of Traffic by Product Type



Source: Comscore and Netcraft Data, analyzed by DigiCert

Share of E-Commerce Transactions by Cert Type



Source: Comscore and Netcraft Data, analyzed by DigiCert

Qualified Website Authentication Certificates

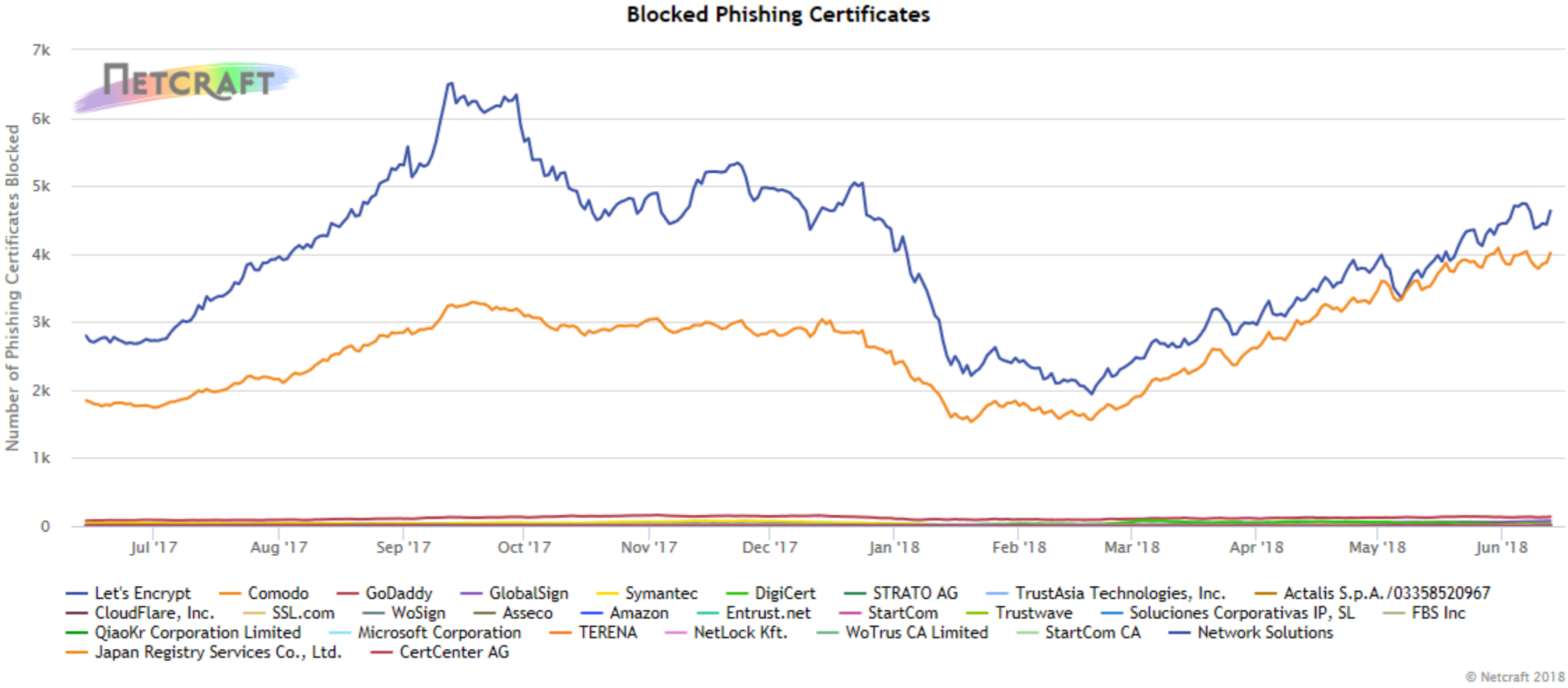
- Approximately 1,700 server certs with QCStatements extension seen in June 2018
- TLDs
  - 60% Spain
  - 12% Great Britain
  - 5% Germany
- Issuers
  - FNMT-RCM (35%)
  - ACCV (35%)
  - Certinomis (19%)

Source: Netcraft Data

Select Certificate Breakdown by Country (May 2018)

Country	DV	OV	EV
France	95.1%	4.4%	.5%
Germany	96.8%	2.8%	.4%
Greece	93.6%	5.5%	.9%
Italy	96.2%	3.3%	.5%
Netherlands	96.4%	2.7%	.9%
Poland	85.5%	13.7%	.7%
Spain	94.9%	4.3%	.7%
United Kingdom	94.8%	4.1%	1.1%
Switzerland	94.1%	5.0%	1.0%
Norway	88.7%	9.3%	2.0%
Denmark	97.5%	2.1%	.4%
Russia	98.4%	1.3%	.2%

According to Netcraft...



Dean Coclin
DigiCert
@chosensecurity