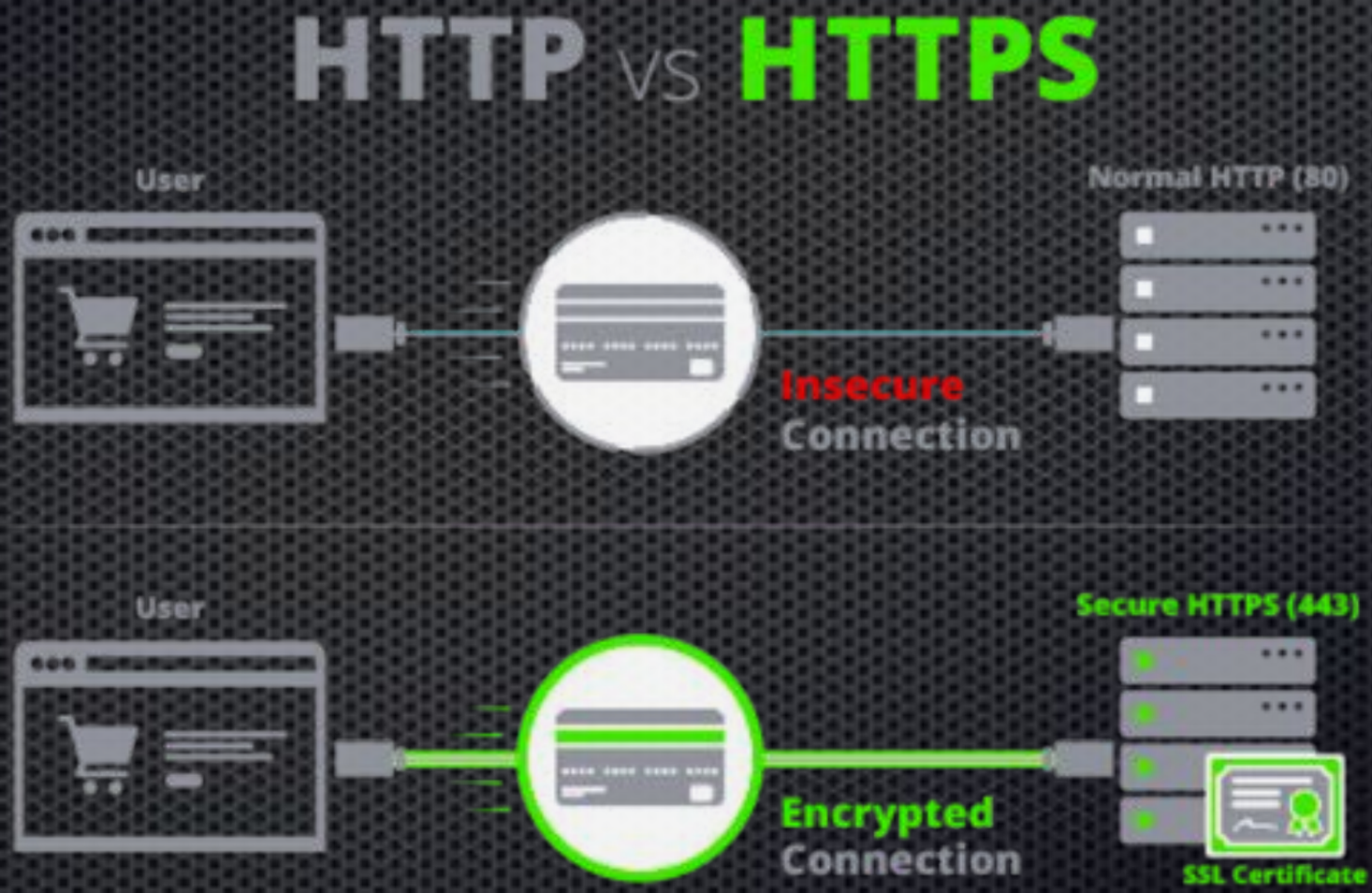
U tri koraka do zelenog address bara

Anja Kiš
Net++ technology

Šta su SSL sertifikati?



Šta je SSL/TLS?

Secure Socket Layer

SSL sertifikat ima dve glavne funkcije:

- **Kriptovanje podataka**
  - SSL omogućava enkripciju, štiti informacije koje se razmenjuju preko mreže
- **Autentifikacija i verifikacija**
  - SSL sertifikat potvrđuje identitet web sajta, preduzeća ili pojedinca

Šta su sertifikaciona tela (CA)?

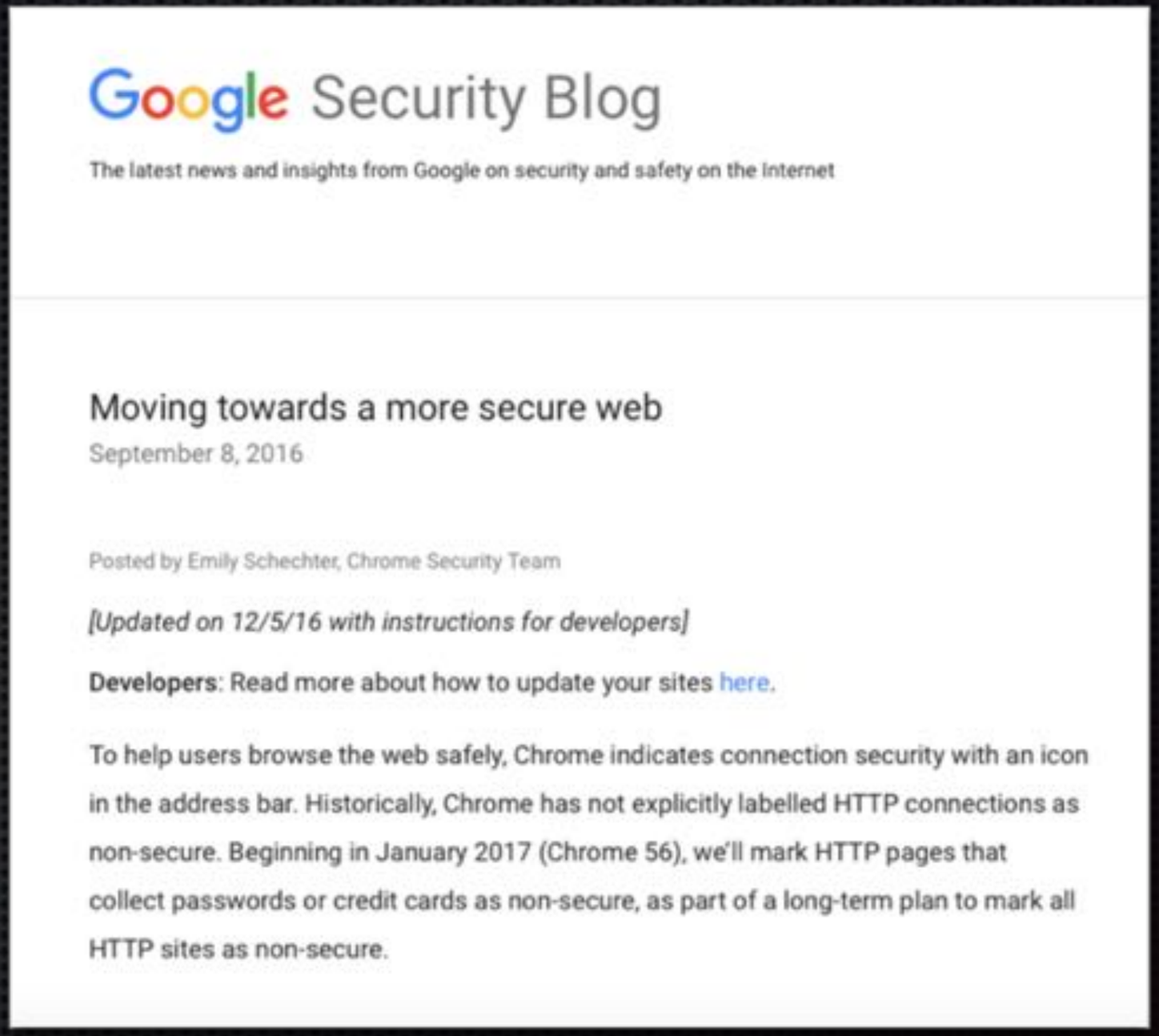
Nezavisna tela koja izdaju SSL sertifikate

Nisu svi SSL sertifikati isti

- Domain Validation (DV)
- Organization Validation (OV)
- Extended Validation (EV)

Google Chrome inicijativa

2016. Počeo proces unapređenja bezbednosti internet konekcije



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Moving towards a more secure web

September 8, 2016

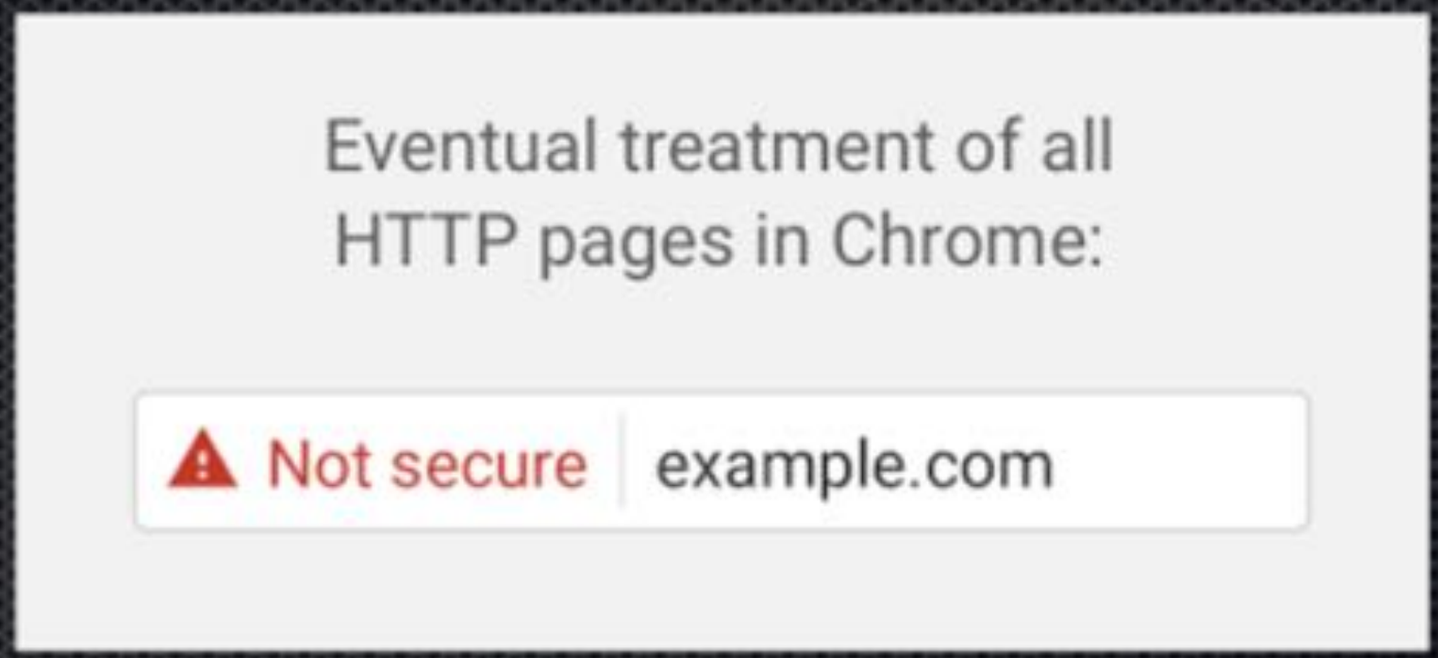
Posted by Emily Schechter, Chrome Security Team

[Updated on 12/5/16 with instructions for developers]

Developers: Read more about how to update your sites here.

To help users browse the web safely, Chrome indicates connection security with an icon in the address bar. Historically, Chrome has not explicitly labelled HTTP connections as non-secure. Beginning in January 2017 (Chrome 56), we'll mark HTTP pages that collect passwords or credit cards as non-secure, as part of a long-term plan to mark all HTTP sites as non-secure.

Budućnost HTTP sajtova



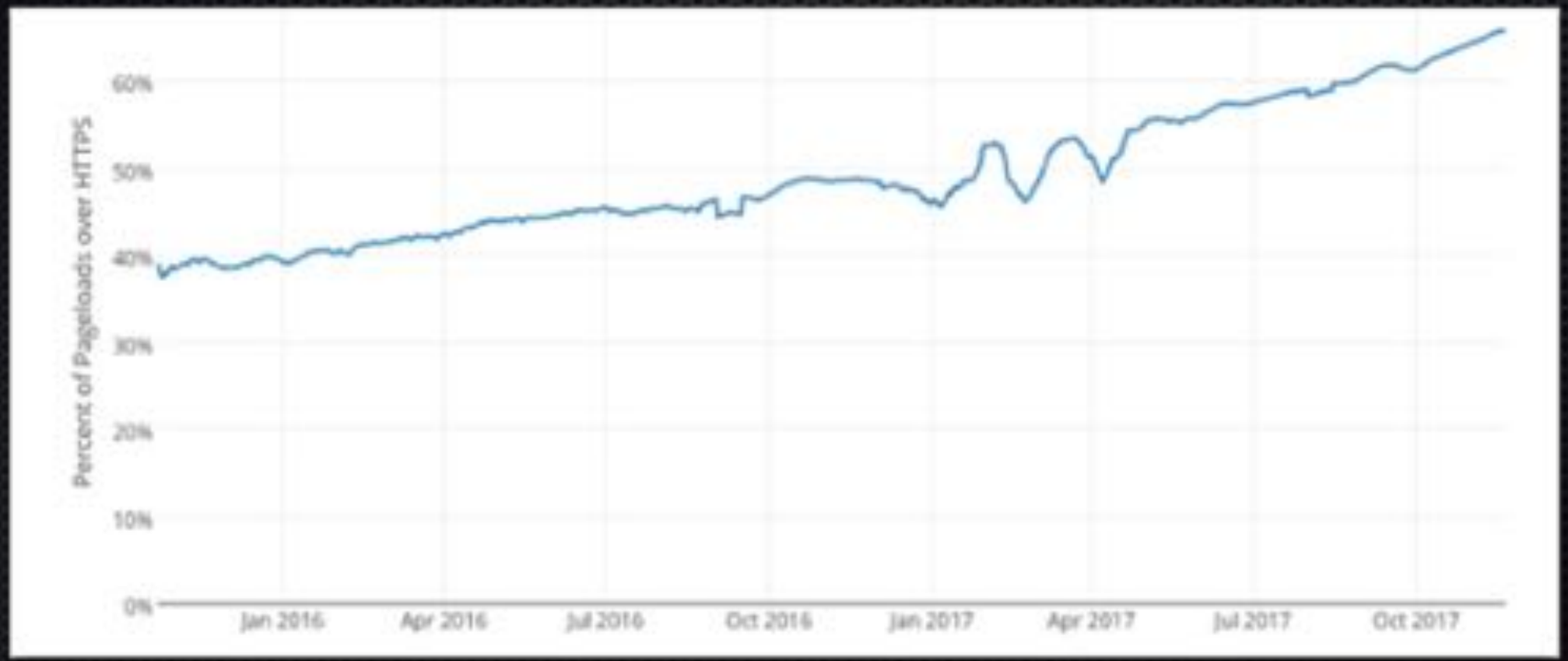
3. faza počinje u julu 2018.

Početkom jula 2018. izlazi nova verzija Google Chrome

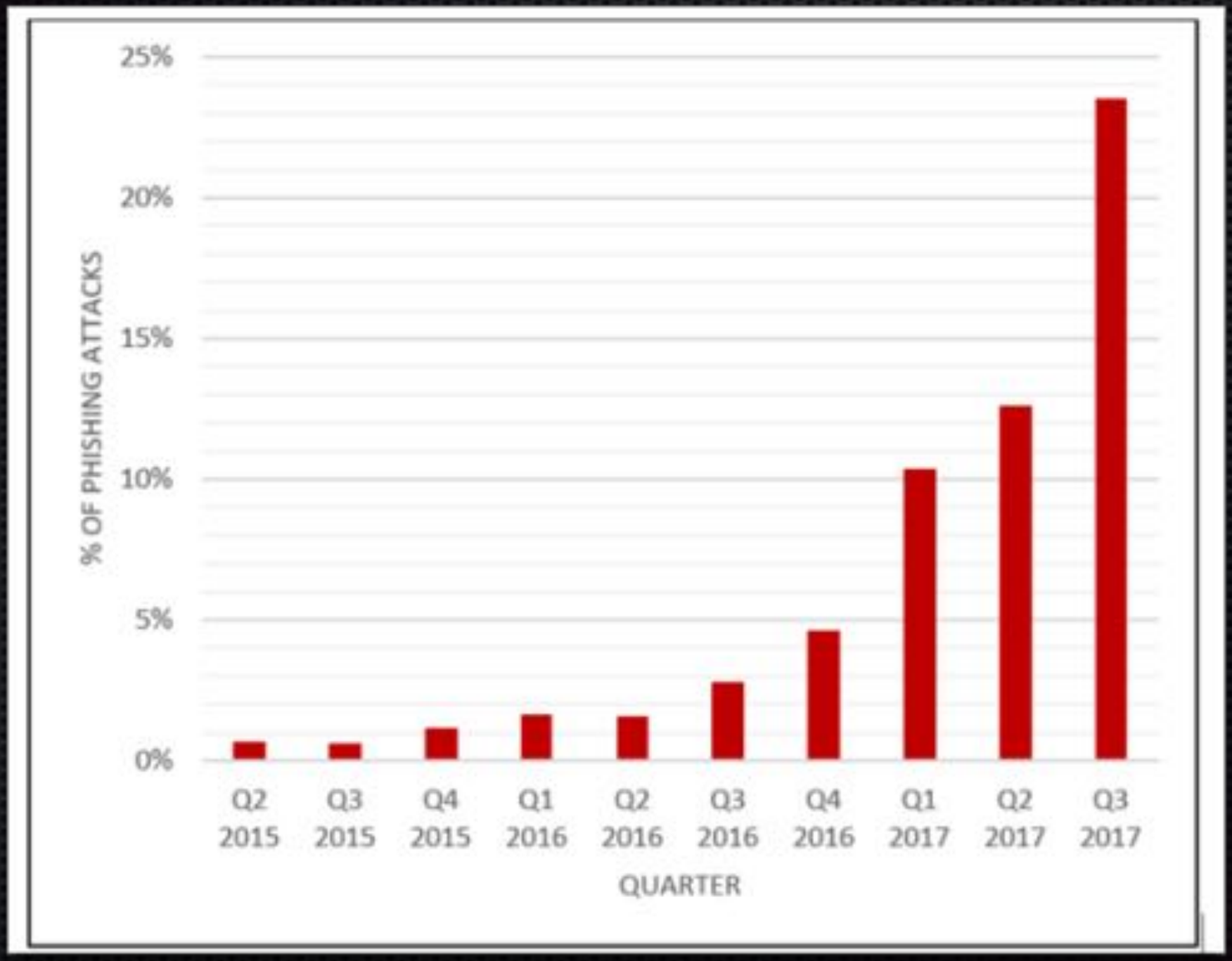
Svi sajtovi koji i dalje koriste http protokol biti označeni kao nebezbedni

Da li je prelazak na HTTPS uticao na bezbednost Weba?

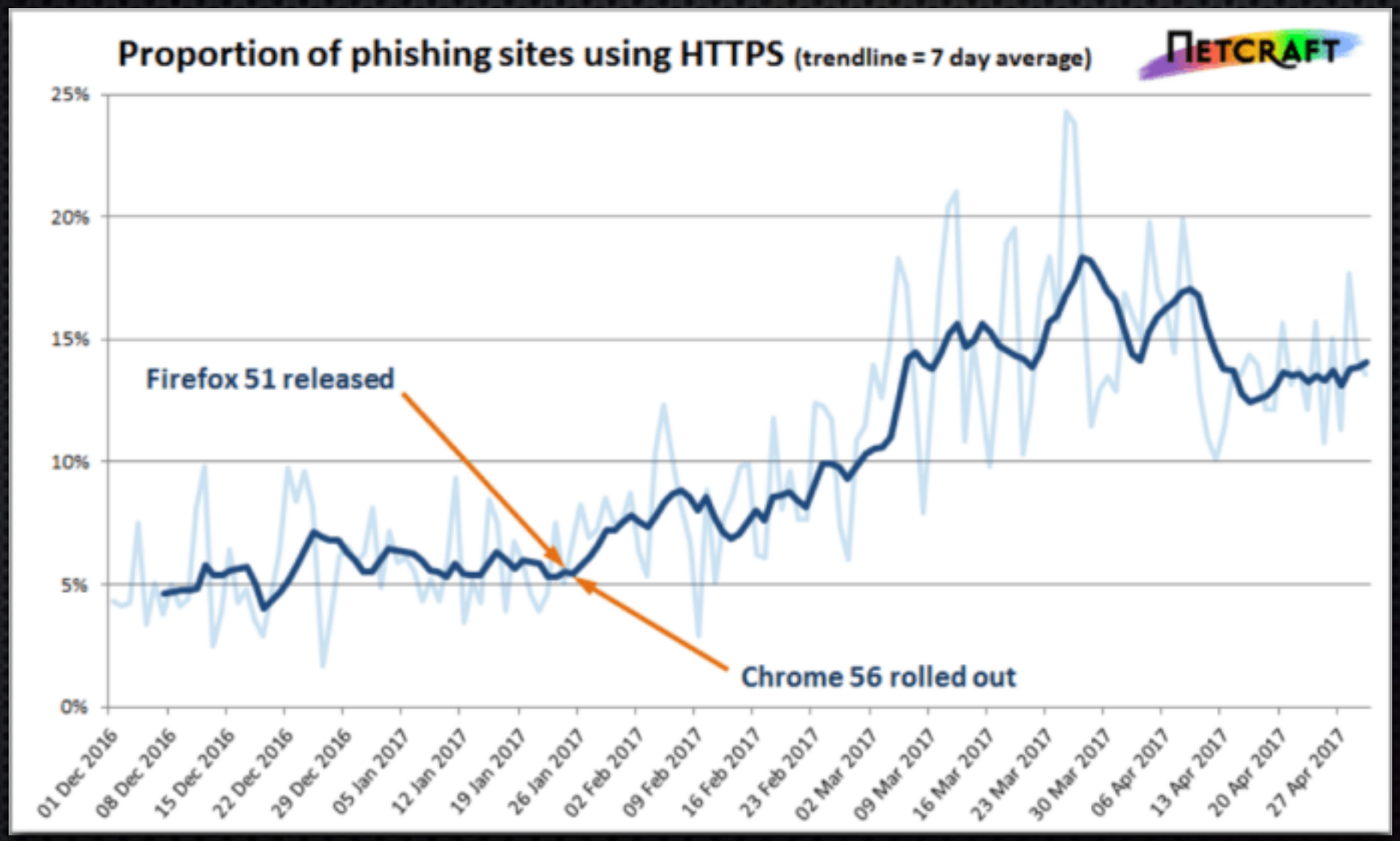
Procenat HTTPS sajtova



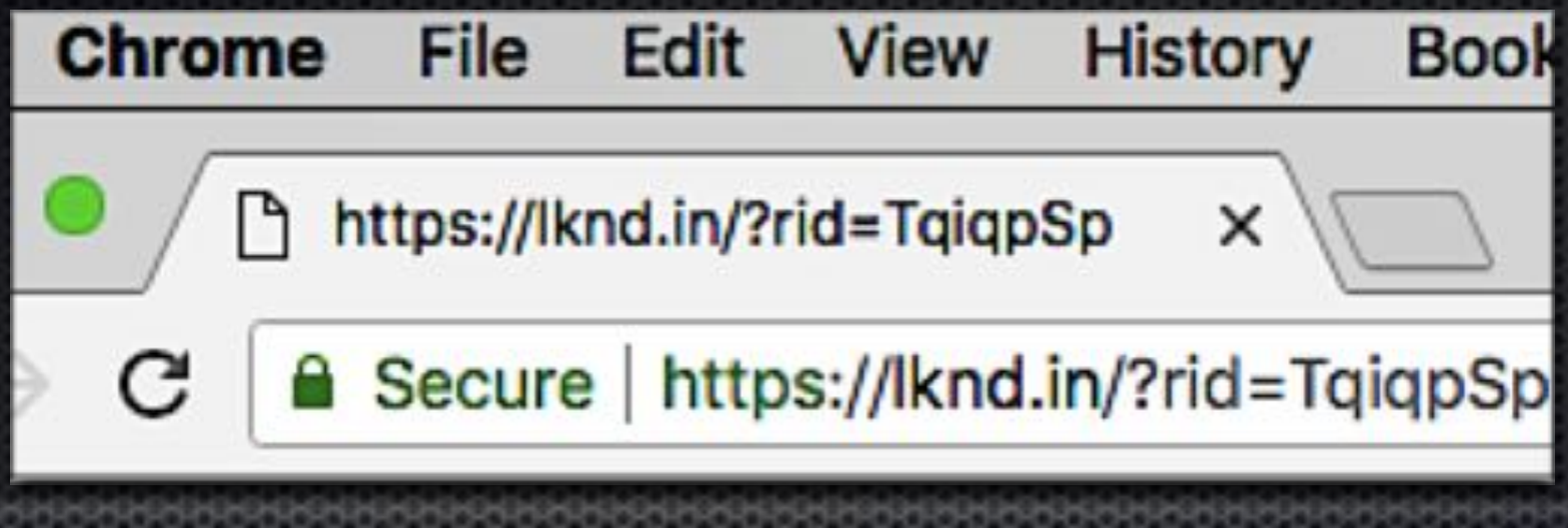
Procenat phishing sajtova



Broj HTTPS phishing sajtova



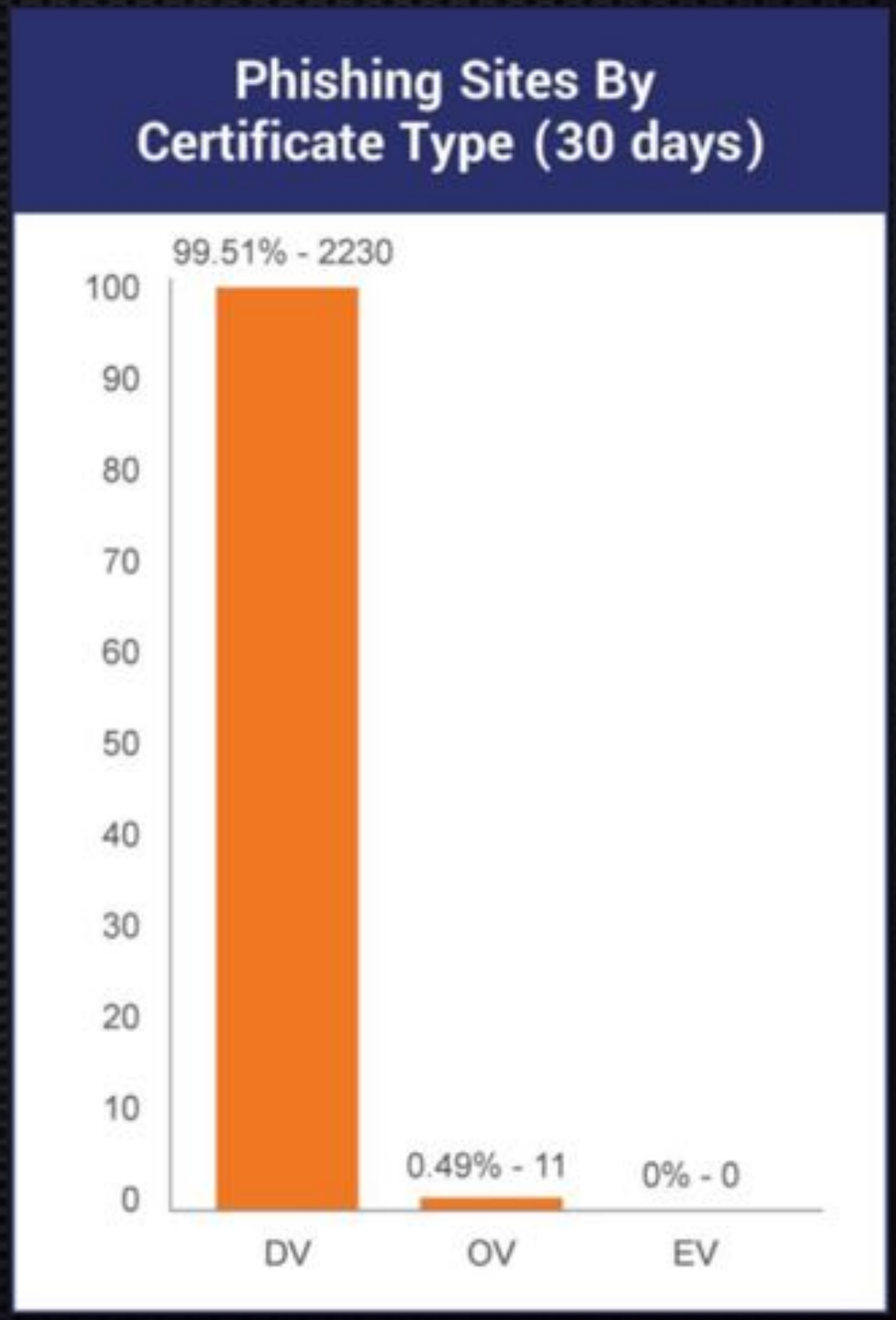
SSL na phishing sajtovima



- Jedan od 4 phishing sajta ima SSL sertifikat
- Google Chrome "Secure" indikatorom povećao efikasnost phishinga

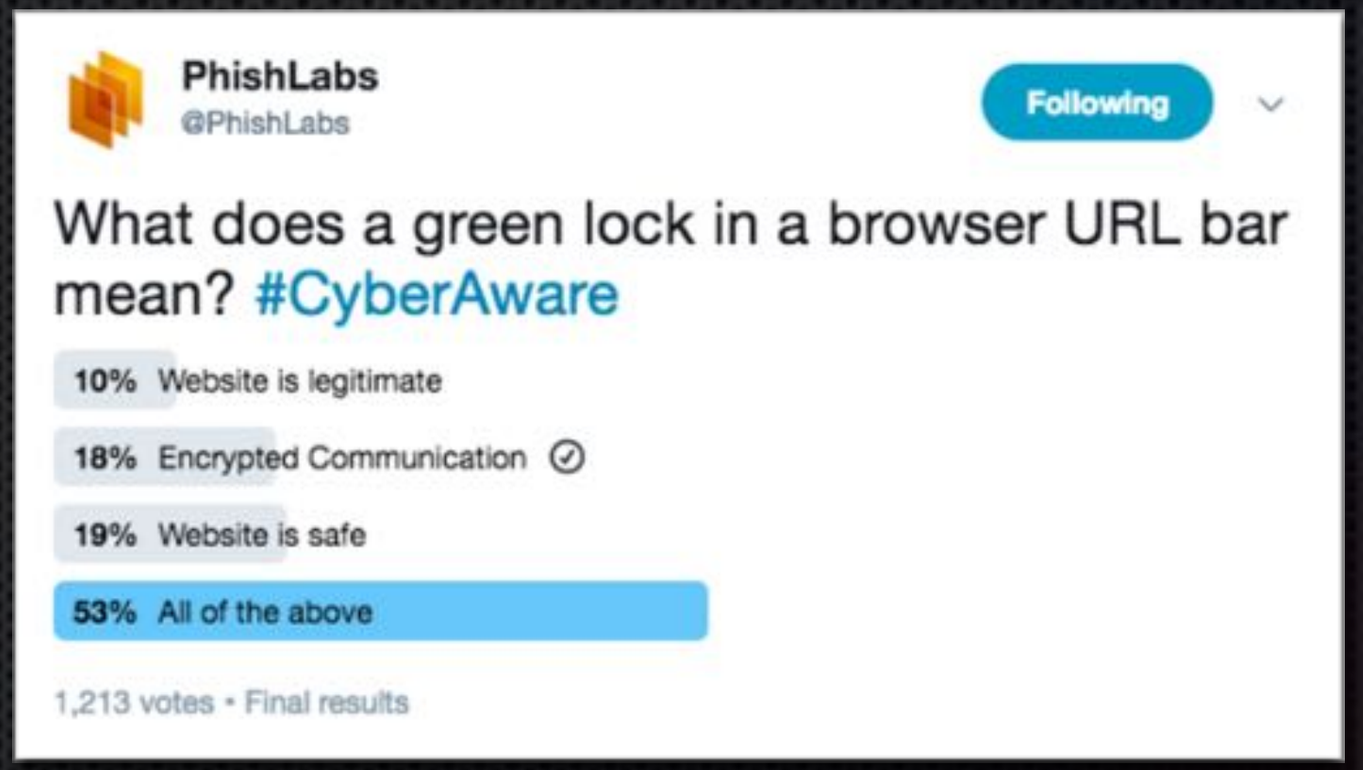
Otkud phishing sajtovima SSL?

- Svako može da dobije DV SSL sertifikat, čak i besplatno

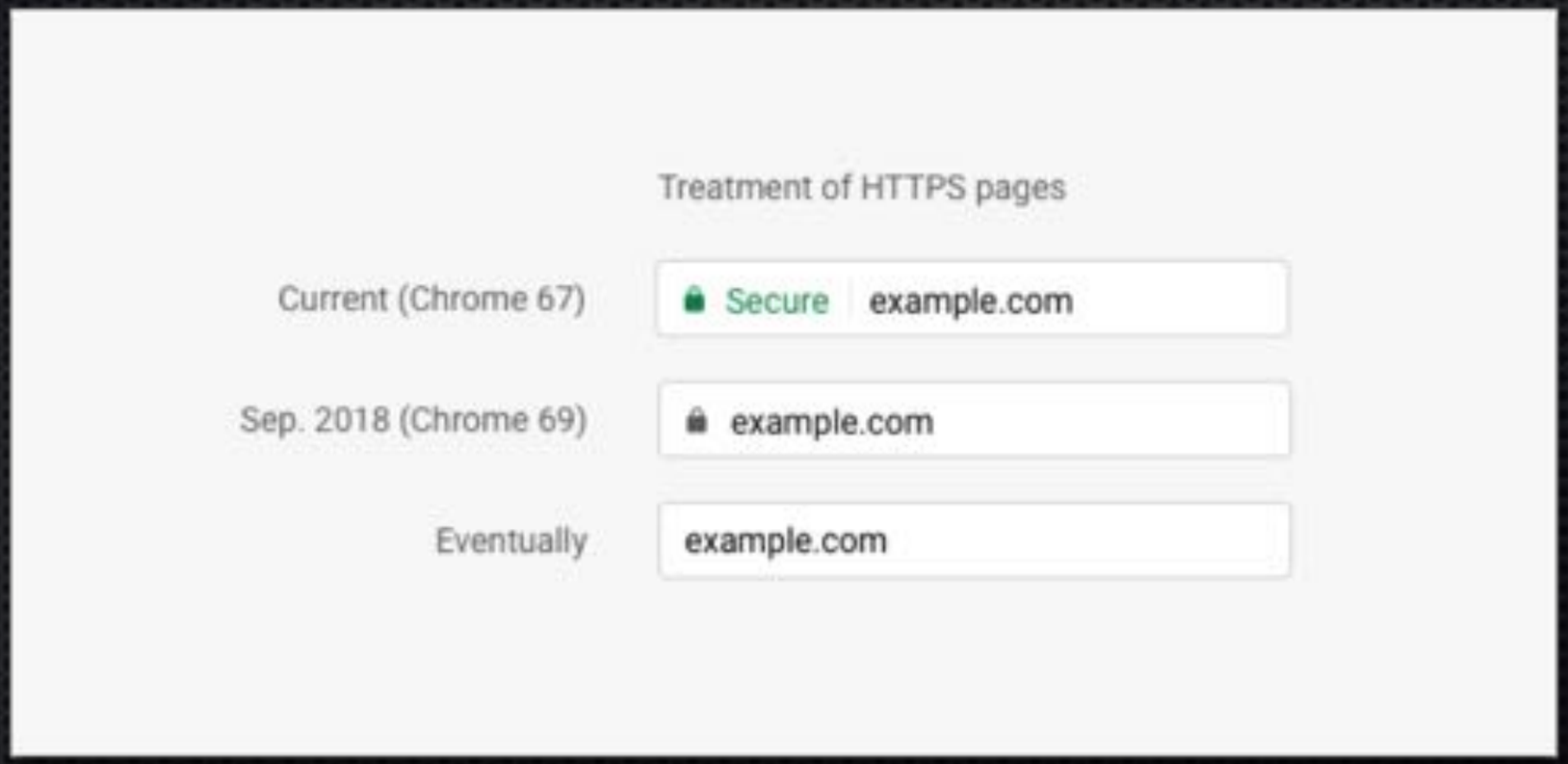


Zašto phishing sajtovi koriste SSL?

- Zato što https sajt deluje legitimno
- Znaju da ljudi veruju da zeleni katanac u browseru znači bezbedan sajt!



Google ukida "Secure" indikator za HTTPS



Phishing
attempts
cost large enterprises
over $3.7
million a year

CSO Online, 2015

50% of all
network attacks
will come from a site with
poorly-validated
SSL

InfoWorld, 2015

More than
466,000
phising websites
pop up every
month

Anti-Phishing Working Group, 2016

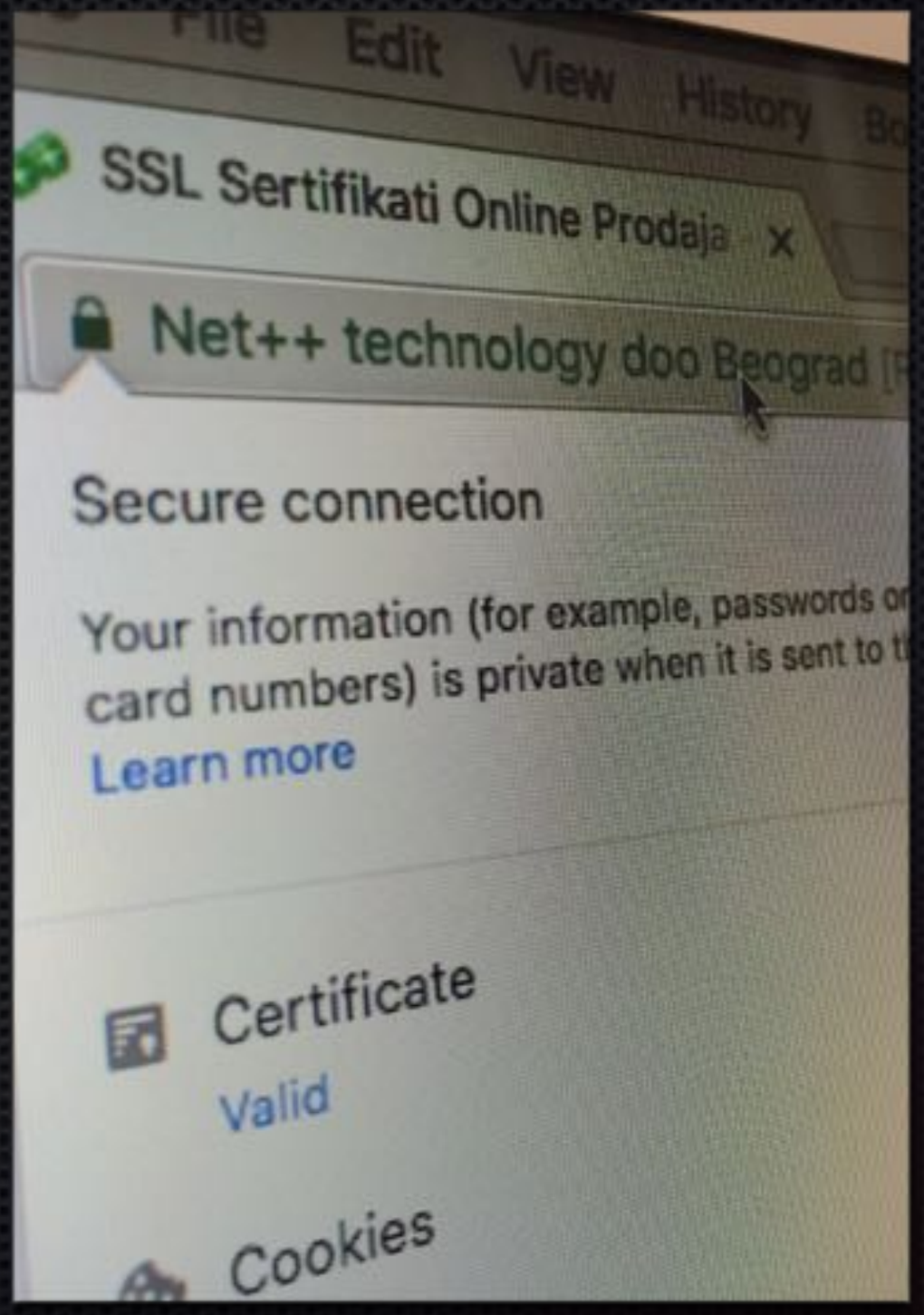
Phishers
target over
400
new businesses
every month

Anti-Phishing Working Group, 2016

Extended Validation SSL

Osmišljeni 2007. kao mera zaštite od phishinga

SSL industrija prepoznala da će doći do zloupotreba DV SSL



Svrha EV SSL sertifikata

1. Identifikacija pravnog lica koje kontroliše Web sajt
2. Omogućavanje kriptovane komunikacije sa Web sajtom

“Sekundarna svrha EV sertifikata je da doprinesu uspostavljanju legitimnosti pravnog lica koje upravlja Web sajtom i da budu sredstvo koje će pomoći u rešavanju problema povezanih sa phishingom, malverom i drugim formama online prevara.”

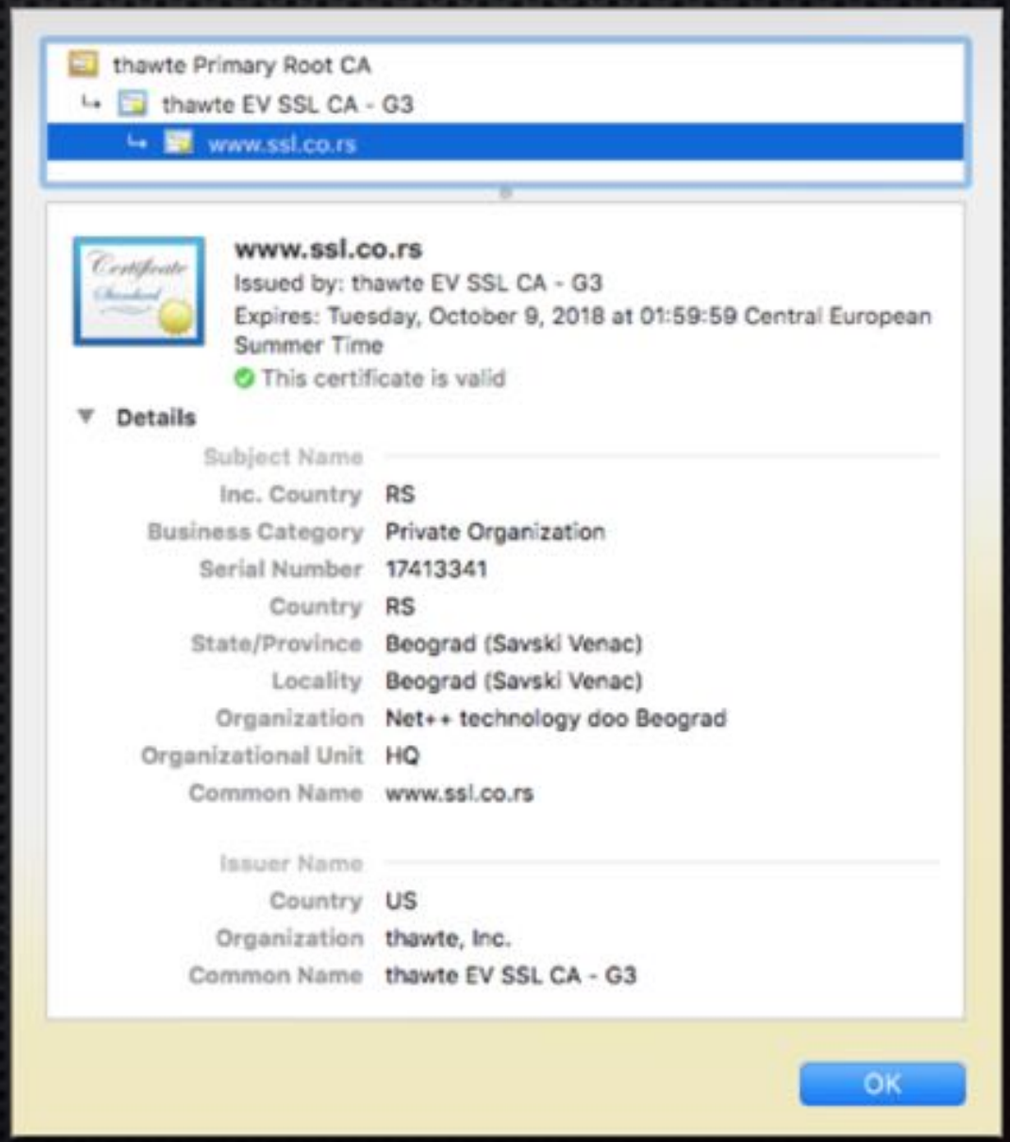
– CA/Browser Forum

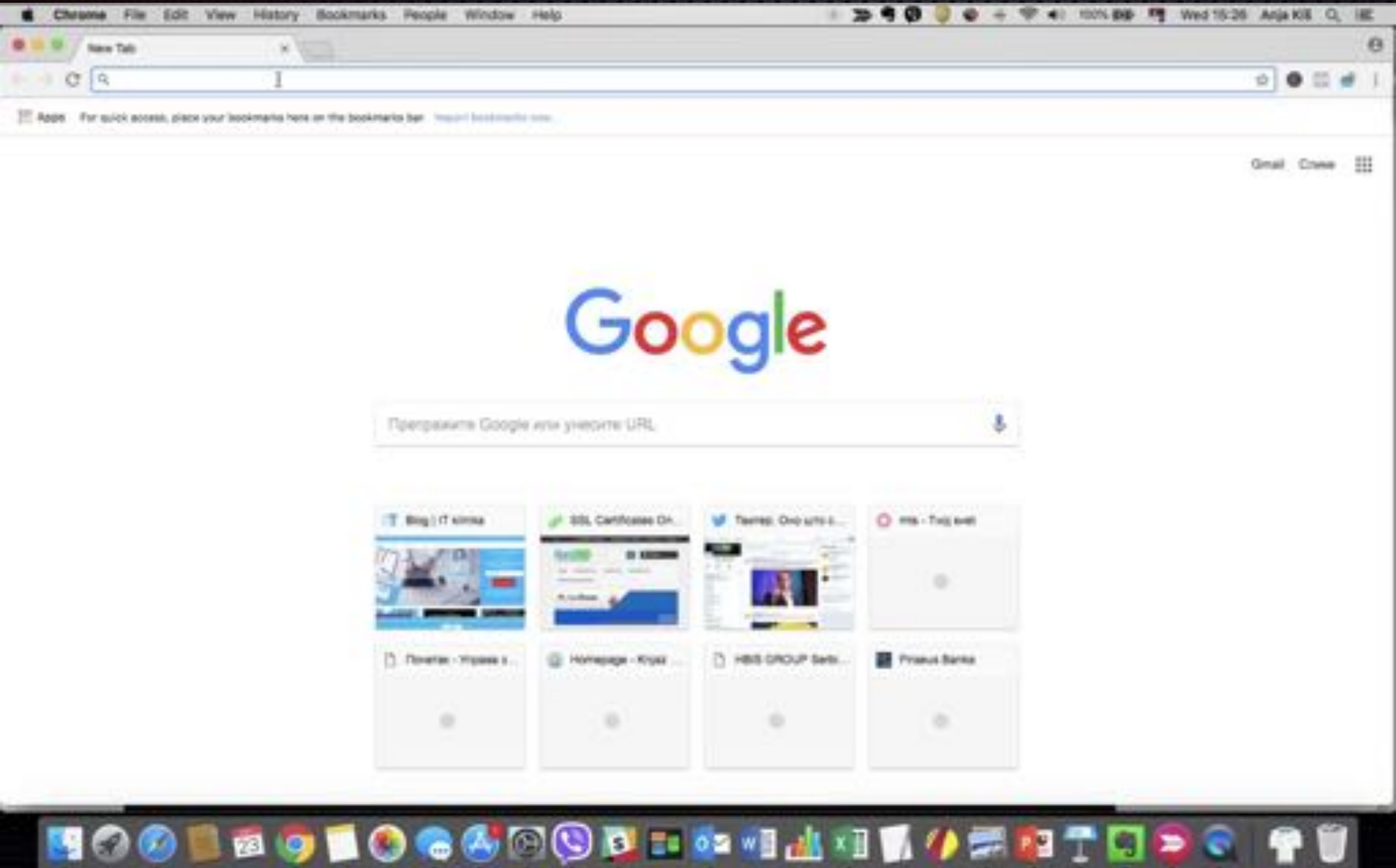
Sekundarna svrha

- Otežati sprovođenje phishing napada korišćenjem sertifikata.
- Pomoći kompanijama koje su meta phishing napada ili online prevara gde se zloupotrebljava identitet da dođu do alata pomoću kog će lakše dokazivati svoj identitet korisnicima.
- Pružanje pomoći organima zakona u istrazi phishinga i drugih online prevara uključujući i kontaktiranje, istragu ili pravne mere protiv subjekta.

CA koje izdaje EV SSL garantuje:

- Pravno postojanje
- Identitet
- Pravo korišćenja domena
- Autorizaciju EV sertifikata
- Tačnost podataka
- Ugovorni odnos
- Status sertifikata
- Opoziv




Chrome File Edit View History Bookmarks People Window Help
New Tab
Apps
For quick access, place your bookmarks here on the bookmarks bar
Gmail
Google
Blog | IT klinika
SSL Certificates On...
Piraeus Banka

3 koraka do zelenog address bara

Procedura izdavanja EV SSL sertifikata

KORAK
01

zašto?

Zato što sertifikat treba da garantuje da iza sajta stoji stvarna organizacija

Validacija Organizacije

CA proverava da li je vaša organizacija registrovana, pod kojim imenom i na kojoj adresi.

Informacije o organizaciji iz Srbije proveravaju se kod Agencije za privredne registre (APR).

apr.gov.rs

Sve usklađujete sa podacima iz APR-a

KORAK

02

zašto?

Da niko osim vas ne bi mogao da dobije sertifikat za vaš domen

Validacija Domena

CA proverava da li imate pravo da koristite domen za koji tražite sertifikat.

Informacije o domenu se proveravaju slanjem domain approver emaila i uvidom u WHOIS bazu.

whois-search.com

KORAK
03

Telefonska verifikacija

CA poziva Organizacioni kontakt da potvrdi porudžbinu i to **isključivo** na broj telefona organizacije koji je dostupan u javnom imenuku.

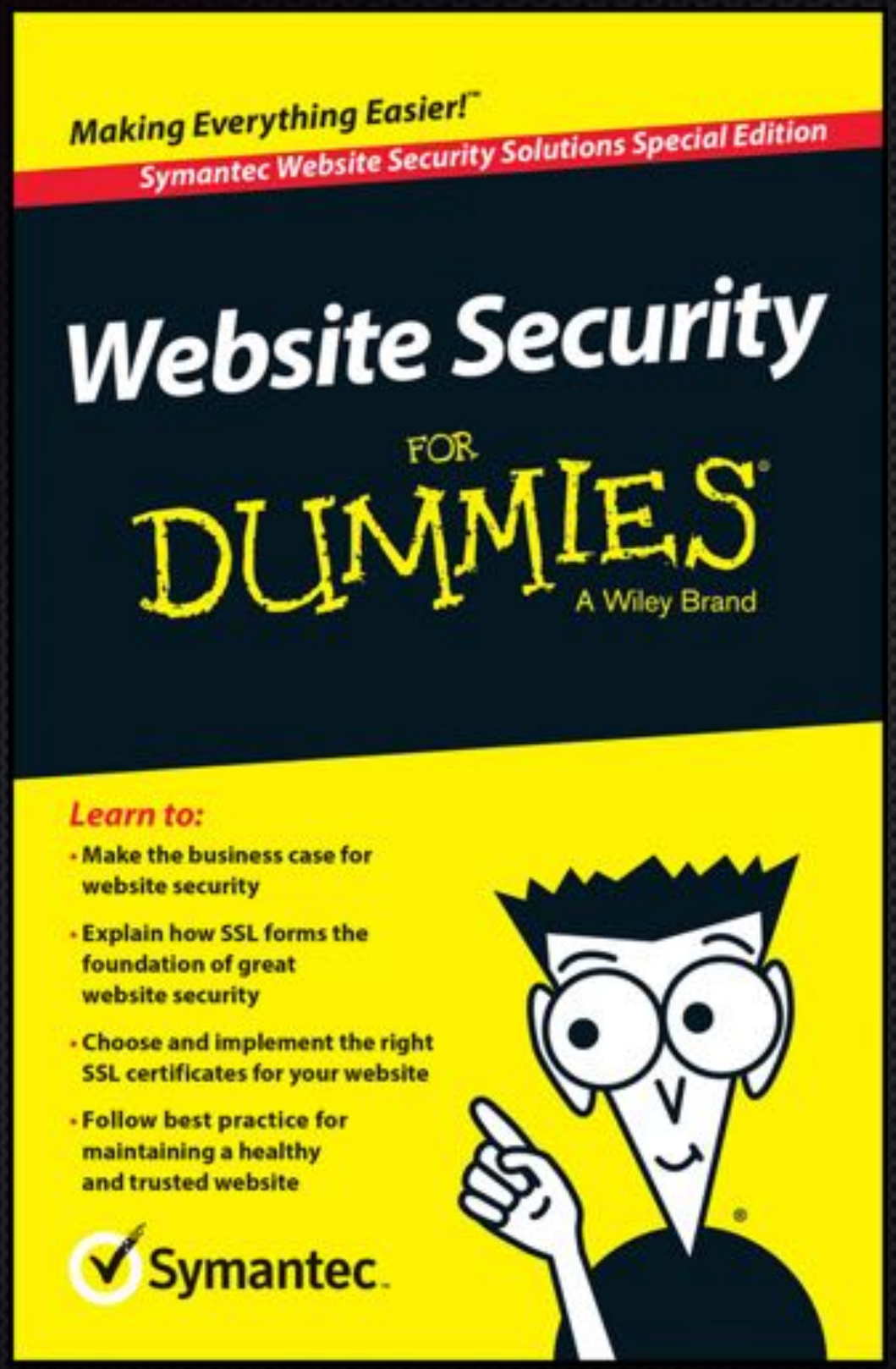
Sa glavnog broja poziv treba da se prosledi Organizacionom kontaktu. Ako poziv ne može da se preusmeri, agentu CA treba da se kaže broj ili email na koji može da dobije Organizacioni kontakt.

Za Srbiju je relevantan imenik Poslovne strane.

www.11811.rs

zašto?

Da bi se potvrdilo da je navedena organizacija zaista poručila sertifikat i da je osoba koja je navedena kao kontakt zaista zaposlena u organizaciji



Više informacija o SSL sertifikatima

- Website Security for Dummies
- www.ssl.co.rs

Hvala na pažnji

Anja Kiš
anja@netpp.rs