Dodatne bezbednosne informacije

1. Vi ste vaša najbolja odbrana

Pre svega, samo najnovija rešenja za sajber bezbednost vas ne mogu u potpunosti zaštititi od malicioznih aktera. Napadači uglavnom postižu rezultate ciljajući vas sa ključnim ciljem krađe lozinki, brojeva kreditnih kartica ili uopšteno kompromitovanja vašeg uređaja - često stvaranjem osećaja hitnosti. Na primer, mogu poslati e-mail upozorenja u ime banke u kojem zahtevaju da sledite određeni, ali štetan link. Koristeći zdrav razum i obraćajući pažnju na pojedinosti, možete uočiti i izbeći takve prevare.

2. Budite oprezni

Kada primite neočekivani e-mail ili tekstualnu poruku, obratite veliku pažnju na male pojedinosti. Ako postoji hiperlink povezan sa tekstom ili referenciranim HTML dugmetom, upotrebite svoj računar i zadržite pokazivač miša iznad njih - većina veb pregledača ili e-mail klijenata će prikazati stvarnu povezanu vezu. Ako nema službenog URL-a ili ga kliknete sa svog mobilnog uređaja, a stranica zahteva da unesete lozinku ili preuzmete bilo što, jednostavno ih odbacite. S druge strane, ako postoji prilog, proverite nastavak datoteke. Uobičajeni maliciozni programi koriste .exe, .scr, .vbs, .rtf, .doc, .docm, .xls, .xlsm, .zip itd. Osim ako u potpunosti ne verujete pošiljaocu, nikada nemojte kliknuti na dugme „Omogući uređivanje“ u programima Microsoft Office.

3. Posebno vodite računa o svojim osetljivim podacima

Akreditivi kao što su lozinke, PIN brojevi i podaci o kreditnoj kartici trebaju biti privatni i bezbedno uskladišteni na bezbednim lokacijama. Brzine moderne računarske mreže učinile su stereotip od osam karaktera ranjivim, stoga treba koristiti složenu i prepoznatljivu lozinku. Ako za skladištenje akreditiva e-bankarstva koristite menadžera lozinki, treba postaviti i glavnu lozinku koja će vam dobro doći ako je uređaj ugrožen. Imajte na umu da Raiffeisen banka ili javni organi nikada ne traže bilo koju od gore navedenih osetljivih informacija.

4. Javni računari i mreže nisu bezbedni

Uopšteno, povezivanje vašeg uređaja sa mrežama poput javne Wi-Fi mreže vas može izložiti velikom broju rizika od sajber napada. Maliciozne strane mogu lako klonirati Wi-Fi javnu pristupnu tačku dobro poznatog naziva mreže (SSID) koji ste ranije koristili-na koji se vaš telefon automatski povezuje, iako protiv vaše volje; čime vaš uređaj postaje sklon presretanju komunikacije i manipulaciji. Uz malo socijalnog inženjeringa, mogli bi vas čak prevariti da odate akreditive, dok je, na primer, domen e-bankarstva legitiman. Javne računare takođe treba potpuno izbegavati, napadači mogu snimiti tastere udarene na tastaturi (proces poznat kao „*keylogging*“) i poslati im kopiju lozinke koju ste upravo uneli.

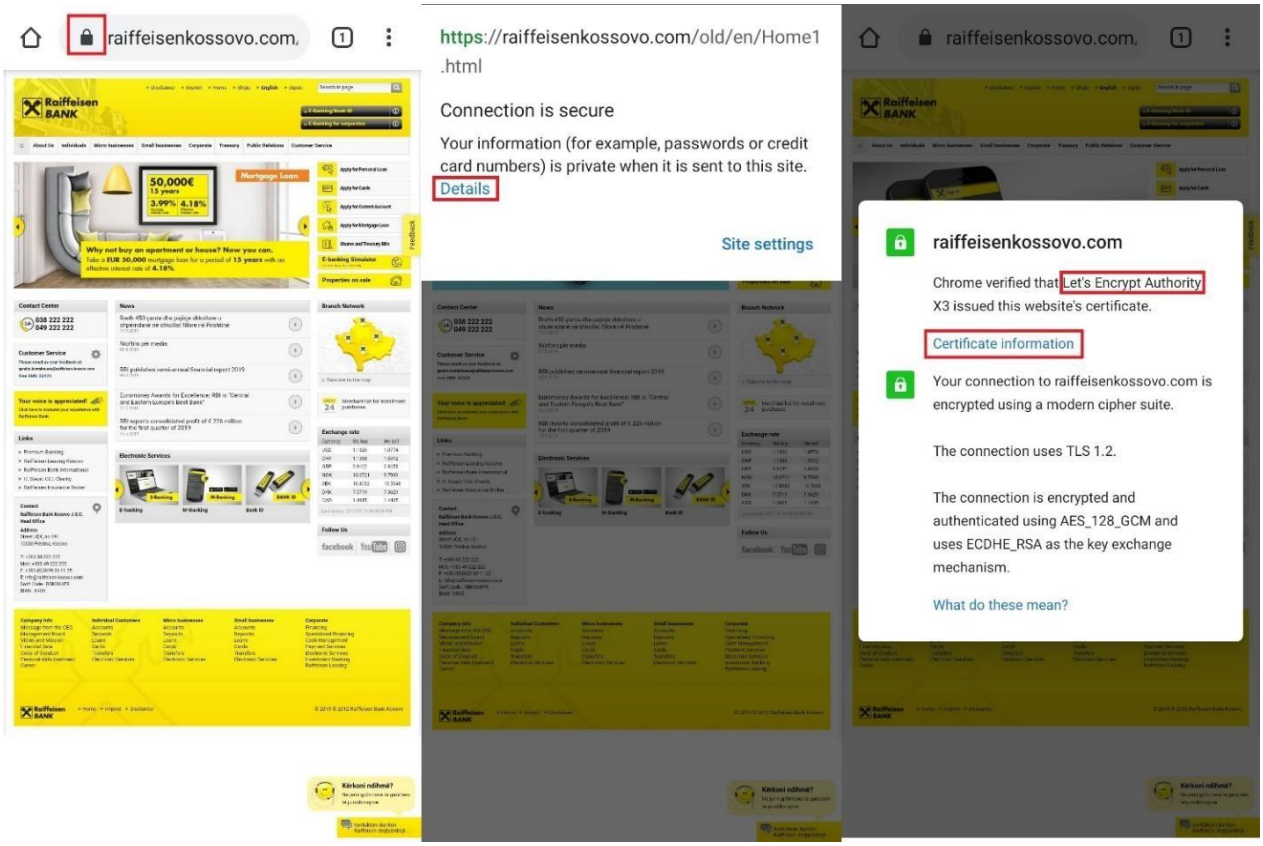
5. Osigurajte bezbedno okruženje

Operativni sistemi i aplikacije stalno dobijaju ažuriranja od dobavljača radi uvođenja funkcija i bezbednosnih zakrpa, stoga je važno ostati u petlji i ne odbaciti ih. Uverite se da imate instaliran antivirus i da je zaštitni zid omogućen. Nikada nemojte da instalirate programe iz nepoznatih ili nepouzdanih izvora, u protivnom rizikujete prenos malicioznog softvera zajedno sa njima. Štaviše, redovne bezbednosne kopije su važne i treba ih skladištiti odvojeno od uređaja koji(e) često koristite.

Veb stranice za prevare

Kloniranje legitimnih veb stranica je jednostavno i vrlo uobičajeno, gde sa druge strane, registracija sličnog lažnog domena koji je teško uočiti zahteva kreativnost i sreću - koliko god je to moguće. Pre nekoliko godina većina ovih uvredljivih veb stranica nije bila opremljena SSL/TLS sertifikatom za šifriranje komunikacije između vašeg uređaja i poslužitelja, što je za početak bila crvena zastavica. Današnji napadači koriste i sertifikate i pouzdane posrednike, poput CloudFlare, dok i dalje kradu akreditive.

Posledično, uočavanje lažnih veb stranica zahteva određeni rad s obzirom na to da ne poseduju svi tehničko znanje. Uzeli smo primer upotrebe za „*raiffeisenkossovo.com*“ – koji je klon stare platforme veb stranice opremljen SSL-om pre objavljivanja Raiffeisen Plus-i koji je sličan našem legitimnom „raiffeisen-kosovo.com“. Kako bismo potvrdili da je ova veb stranica zaista lažna, možemo započeti klikom na ikonu zaključavanja (koja potvrđuje prisutnost SSL sertifikata), prelaskom u „Detalji“, nakon čega se podiže prva crvena zastavica kao što je prikazano na slici 1.

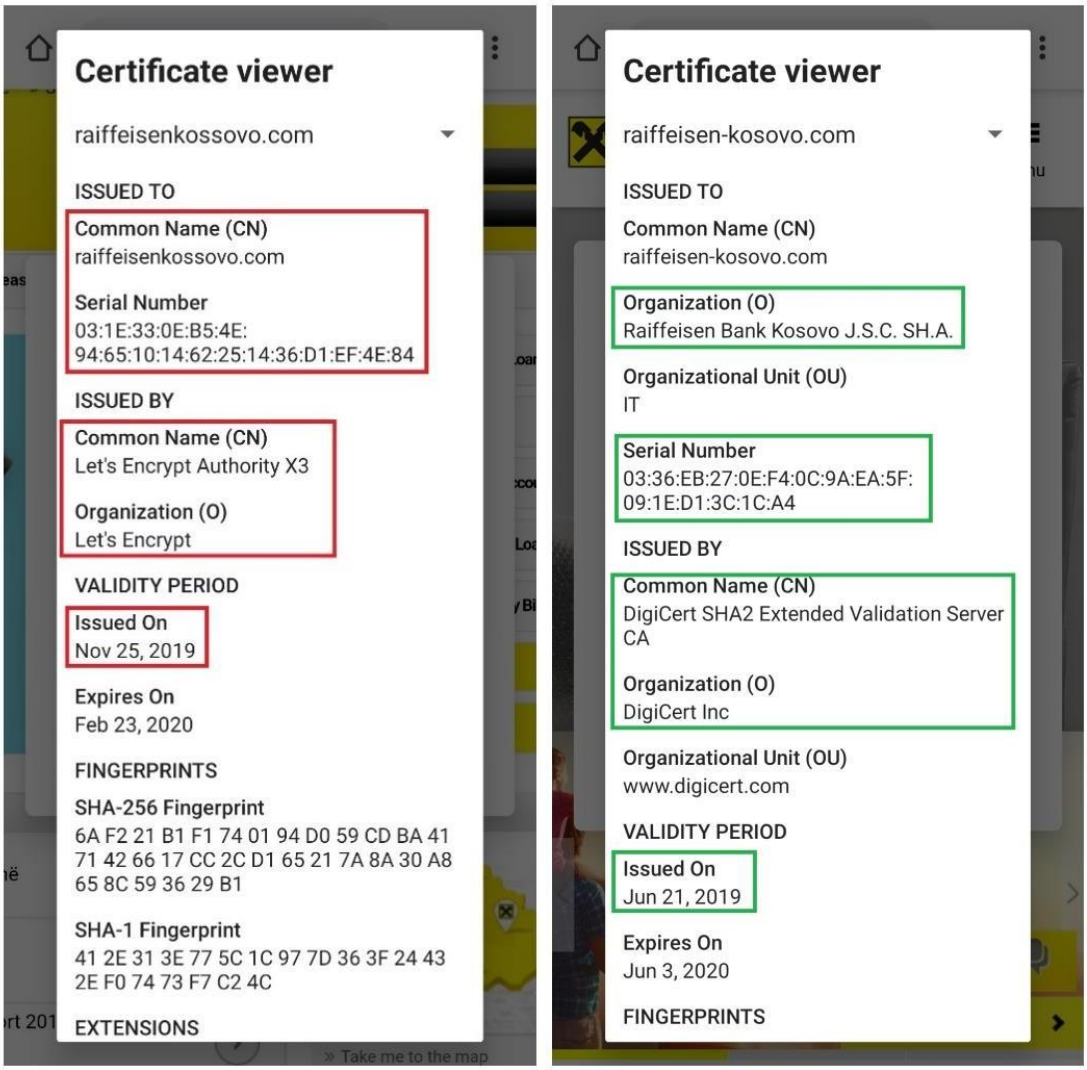


Slika 1 - Provera autentičnosti veb stranice putem telefona

Autoritet za sertifikate (CA) je entitet koji potvrđuje identitete kompanija i organizacija širom sveta izdavanjem ovih pouzdanih SSL/TLS sertifikata. Postoji mnogo takvih dobro poznatih autoriteta, neki nude besplatne sertifikate, dok drugi izdaju one plaćene. Iako se nivo zaštite od šifriranja ne razlikuje, besplatni SSL sertifikati proveravaju autentičnost samo domena za koju se koristi, dok plaćeni SSL sertifikati imaju mnogo viši nivo provere identiteta.

„*Hajde da šifriramo"* je besplatan i otvoren CA koji sajber kriminalci često zloupotrebljavaju radi provere autentičnosti svojih lažnih domena, poput „*raiffeisenkossovo.com*". Sa druge strane, Raiffeisen banka koristi „DigiCert" kao svoj CA, kompaniju koja pruža najveću dostupnu proveru autentičnosti koja čini proces zloupotrebe našeg ispravnog naziva marke neizvodljivim.

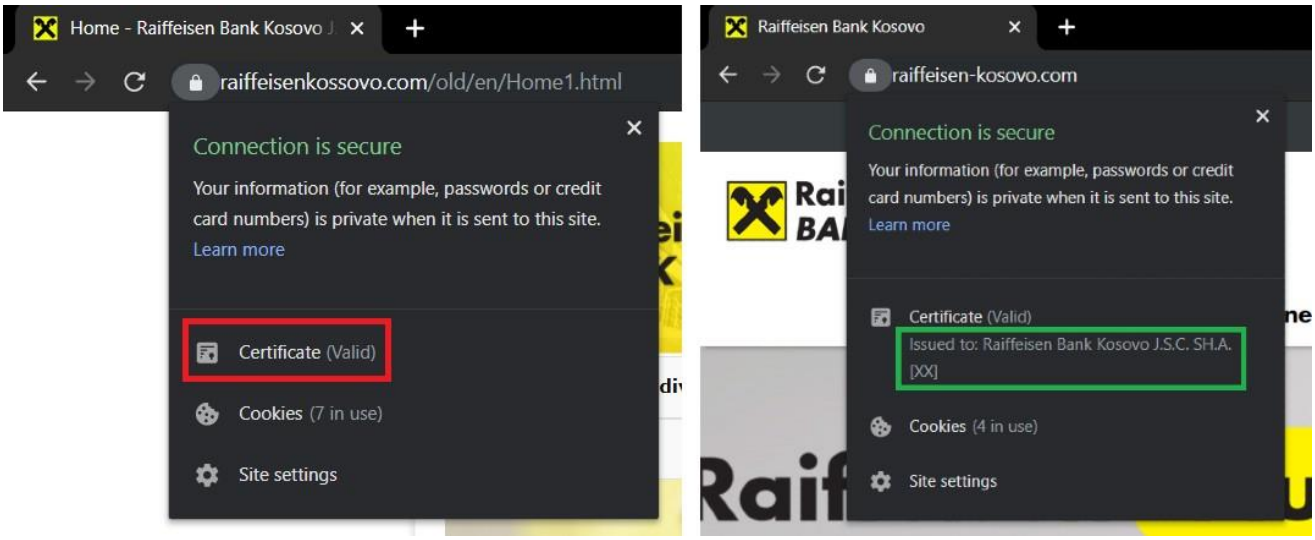
Slika 2 prikazuje poređenje između „*raiffeisenkossovo.com*" i legitimnog „*raiffeisen- kosovo.com*":



Slika 2 - Pojedinosti sertifikata putem mobilnog telefona

- „*raiffeisenkossovo.com*" koristi besplatan autoritet „Hajde da šifriramo", što je prva crvena zastavica, dok „*raiffeisen-kosovo.com*" koristi plaćeni i ispravan „*DigiCert*";
- „*raiffeisenkossovo.com*" je nedavno objavljen (u vreme pisanja ovog dokumenta), što je još jedna crvena zastavica obzirom da takvi domeni ne traju dugo;
- Možete da primetite pun poslovan naziv „*Raiffeisen Bank Kosovo J.S.C. SH.A.*" na „*raiffeisen-kosovo.com*" što je pozitivan pokazatelj da stranica zaista pripada Raiffeisen banci Kosovo.

Slično tome, autentičnost možete proveriti preko desktop računara, što je možda prikladnije:



Slika 3 - Informacije o sertifikatu preko ličnog računara