Informata shtesë të sigurisë

1. Ju jeni mbrojtja më e mirë e vetes tuaj

Para së gjithash, softuerët e fundit të sigurisë kibernetike nuk mund t'ju mbrojnë plotësisht nga akterë dashakeqë. Sulmuesit kryesisht arrijnë rezultate duke iu targetuar juve me qëllimin kryesor të vjedhjes së fjalëkalimeve, numrave të kredit kartelës, apo me qëllim të kompromentimit të pajisjes tuaj në përgjithësi – dhe këtë shpesh e bëjnë duke krijuar ndjenjën e urgjencës. Për shembull, mund të ju dërgojnë paralajmërime përmes e-mail në emër të bankës duke iu kërkuar që të klikoni ndonjë link specifik por të dëmshëm. Ju mund t'i vëreni dhe shmangi këto mashtrime vetëm duke përdorur logjiken dhe duke i kushtuar vëmendje detajeve.

2. Bëhuni vigjilent

Kur pranoni e-mail apo mesazhe të papritura, kushtoni vëmendje të veçantë detajeve të vogla. Nëse ka link të bashkëngjitur në mesazh apo HTML buton të referuar, atëherë përdorni kompjuterin dhe mbani kursorin mbi to - shumica e shfletuesve të faqeve të internetit apo ofruesit e shërbimeve të e-mail do t'ju tregojnë linkun e vërtetë. Nëse nuk ka URL zyrtare, apo ju klikoni mbi to nga pajisja juaj mobile dhe më pas kërkohet të shkruani fjalëkalimin apo të shkarkoni diçka, thjeshtë largoni ato faqe. Në anën tjetër, nëse ka dokumente të bashkëngjitura, kontrolloni formatin e fajllit. Programet e zakonshme dashakeqe përdorin formatin .exe, .scr, .vbs, .rtf, .doc, .docm, .xls, .xlsm, .zip, e të tjera. Asnjëherë mos klikoni mbi butonin “Enable Editing” (Mundëso Editimin) në programet e Microsoft Office, përveç nëse i besoni absolutisht dërguesit.

3. Kushtoni kujdes të posaçëm informatave tuaja të ndjeshme

Kredencialet siç janë fjalëkalimet, numrat PIN, dhe detajet e kredit kartelës duhet të mbahen private dhe të ruhen në mënyrë të sigurtë në vende të sigurta. Shpejtësitë moderne të qëllimit të fjalëkalimeve kanë bërë që stereotipi me tetë karaktere të bëhet i cenueshëm, prandaj duhet të përdoren fjalëkalime më komplekse dhe të dalluara. Nëse përdorni menaxherin e fjalëkalimeve për të ruajtur kredencialet e shërbimit e-Banking, atëherë duhet të keni edhe fjalëkalimin “master” i cili do të aktivizohet në rastet kur pajisja është e kompromet uar. Ju lutem vini re që Raiffeisen Bank apo autoritetet publike asnjëherë nuk kërkojnë asnjë prej informatave të ndjeshme të përmendura më lart.

4. Kompjuterët dhe rrjetet publike nuk janë të sigurta

Në përgjithësi, konektimi i pajisjes tuaj me rrjete sikurse Wi-Fi publike mund të bëjë që të ekspozoheni ndaj një numri të gjerë të sulmeve kibernetike. Palët dashakeqe lehtësisht mund të klonojnë pikat e njohura të Wi-Fi të një rrjeti (SSID) të cilat ju i keni përdorur më parë - me të cilin automatikisht, qoftë edhe pa dëshirën tuaj, lidhet telefoni juaj; duke e bërë kështu pajisjen tuaj më të prirur për përgjime dhe manipulime të komunikimeve. Për më shumë, përmes manipulimit, ata mund t'ju mashtrojnë që të jepni kredencialet tuaja gjersa, për shembull, domeni i e-Banking është legjitim. Kompjuterët publik duhet të shmangen tërësisht. Sulmuesit mund të regjistrojnë tastet e shtypura në tastierë (procesi i njohur si “keylogging”) dhe të marrin kopjen e fjalëkalimit që sapo keni shkruar.

5. Siguroni mjedis të sigurtë

Sistemet operative dhe aplikacionet vazhdimisht marrin përditësime nga shitësit për të futur tipare dhe përditësime të sigurisë, prandaj, është e rëndësishme të qëndroni në rrjedha dhe të mos i injoroni ato. Sigurohuni që keni antivirus të instaluar dhe firewall të aktivizuar. Asnjëherë mos instaloni programe nga burime të pa njohura apo të pa besuara, përndryshe rrezikoni të transferoni malware së bashku me to. Për më tepër, backup (kopjet rezervë) të rregullta janë të rëndësishme dhe duhet të ruhen veçmas nga pajisja/pajisjet që i përdorni rregullisht.

Faqet mashtruese

Klonimi i faqeve legjitime të internetit është i lehtë dhe është diçka që haset shpesh. Me gjithë faktin se regjistrimi i domenit të ngjashëm mashtrues që është vështirë i dallueshëm kërkon kreativitet dhe fat – diçka e tillë është plotësisht e mundshme. Disa vite më parë, shumica e këtyre faqeve abuzive të internetit nuk kanë qenë të pajisura me certifikatë SSL/TLS për enkriptimin e komunikimit ndërmjet pajisjes dhe serverit tuaj, gjë që ka paraqitur shenjën e parë të rrezikut. Por, sulmuesit e sotëm përdorin certifikatat dhe ndërmjetësit e besueshëm siç janë CloudFlare gjersa vjedhin kredenciale.
Rrjedhimisht, dallimi i faqeve të rreme të internetit kërkon angazhim duke marrë parasysh se jo të gjithë njerëzit posedojnë njohuri teknike. Ne kemi marrë rastin e "*raiffeisenkossovo.com*" - që është klon i pajisur me SSL i platformës së vjetër të faqes së internetit para se të lëshohej platforma Raiffeisen Plus - dhe që është i ngjashëm me faqen tonë legjitime të internetit "raiffeisen-kosovo.com". Për të konfirmuar që kjo faqe e internetit është mashtruese, mund të fillojmë duke klikuar ikonën e kyçit (që konfirmon praninë e certifikatës SSL), dhe kur vazhdojmë tek opsioni "Details" (Detajet) aty shohim shenjën e parë të rrezikut siç edhe shihet në figurën 1.

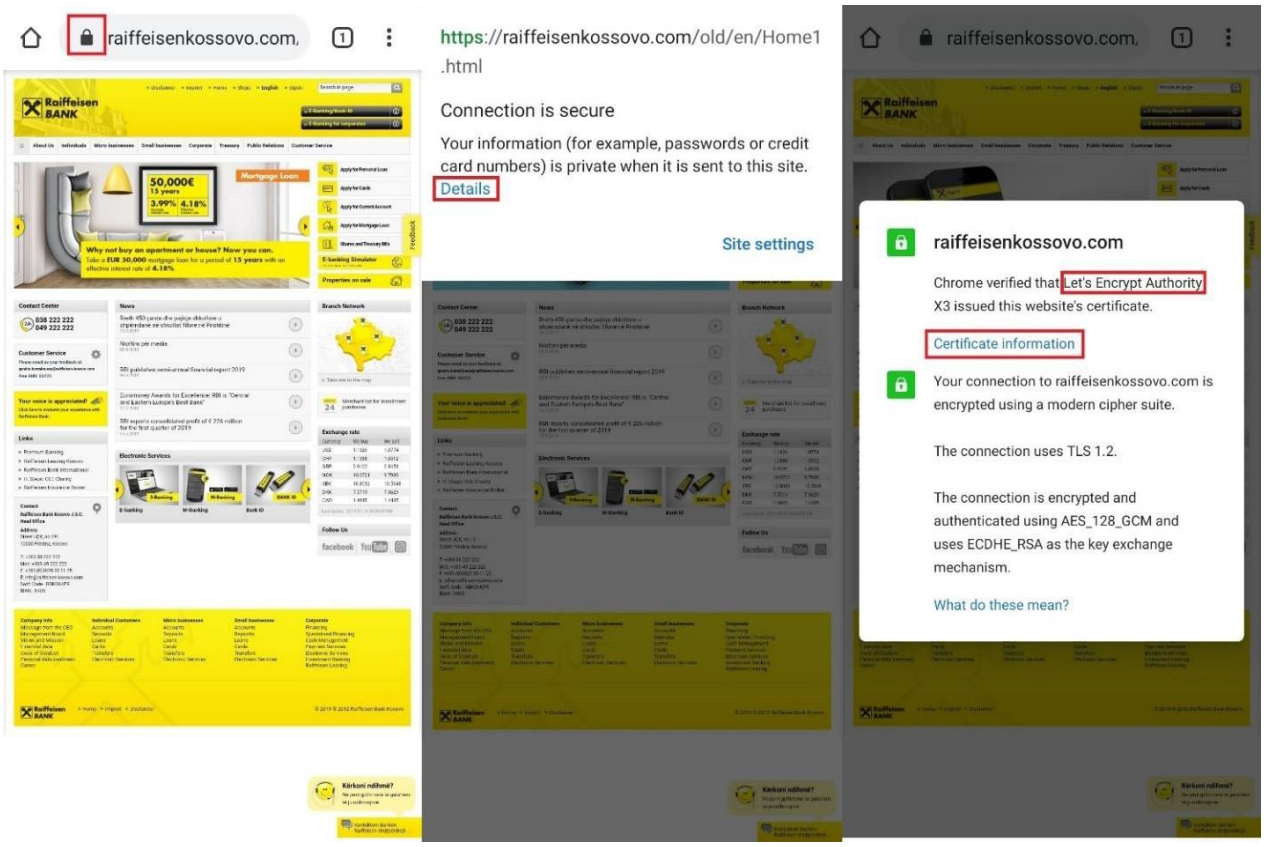

Figura 1 – Verifikimi i autenticitetit të faqes së internetit përmes telefonit

Autoriteti i certifikimit (AC) është subjekt që vërteton identitetin e kompanive dhe organizatave në të gjithë botën duke lëshuar certifikata të besueshme SSL/TLS. Ka shumë autoritete të tilla të njohura. Disa prej tyre ofrojnë certifikata falas dhe disa të tjera i lëshojnë ato me pagesë. Deri sa niveli i mbrojtjes nga enkriptimi nuk ndryshon, certifikatat falas SSL vërtetojnë vetëm domenin i cili përdoret, kurse certifikatat SSL me pagesë kanë nivel shumë më të lartë të vërtetimit të identitetit.

"*Let's Encrypt*" është AC e hapur dhe pa pagesë, që shpesh keqpërdoret nga kriminelët në internet për të vërtetuar domenet e tyre mashtruese si "*raiffeisenkossovo.com*". Në anën tjetër, Raiffeisen Bank përdor "*DigiCert*" si AC-në e saj. Kjo e fundit është kompani që ofron autentifikimin më të lartë në dispozicion, që rrjedhimisht e bën procesin e keqpërdorimit të emrit të saktë të brendit tonë të pamundur.

Figura 2 tregon krahasimin ndërmjet "*raiffeisenkossovo.com*" dhe faqes legjitime "*raiffeisen-kosovo.com*":

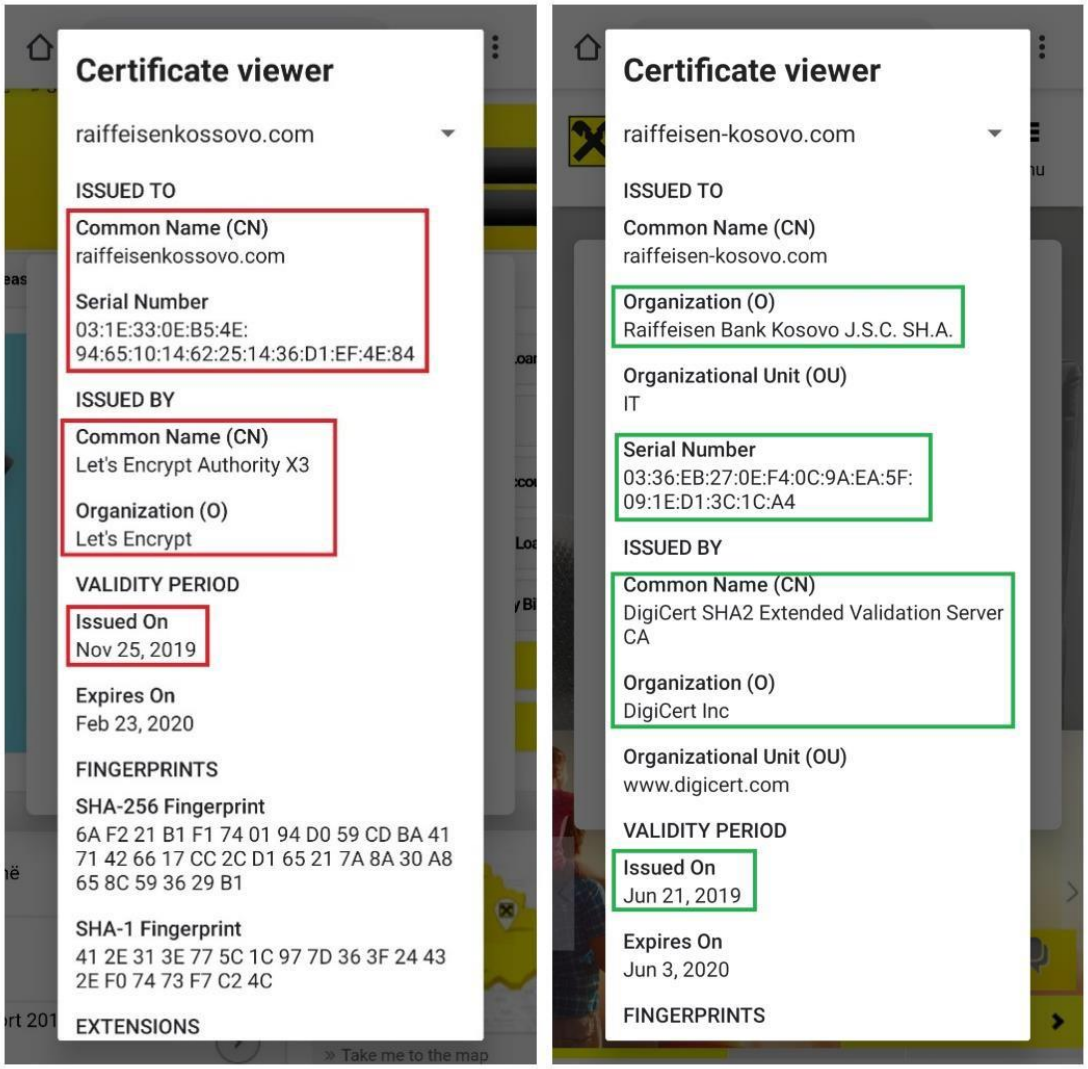

Figura 2 – Detajet e certifikatës përmes telefonit mobil

- "*raiffeisenkossovo.com*" përdor ofruesin pa pagesë "*Let's Encrypt*", që paraqet shenjën e parë të rrezikut, ndërsa "*raiffeisen-kosovo.com*" përdor atë me pagesë dhe të rregullt "*DigiCert*";
- "*raiffeisenkossovo.com*" është hapur kohët e fundit (në kohën e përgatitjes së këtij dokumenti), që është shenjë tjetër e rrezikut, sepse kryesisht domenet tilla nuk kanë jetë të gjatë;
- Në "*raiffeisen- kosovo.com*" mund ta vëreni emrin e plotë të biznesit "*Raiffeisen Bank Kosovo J.S.C. SH.A.*", që është indikator pozitiv se faqja me të vërtetë i përket Raiffeisen Bank Kosova.

Gjithashtu, vërtetimin e autenticitetit, në mënyrë më të përshtatshme, mund ta bëni përmes kompjuterit tuaj:

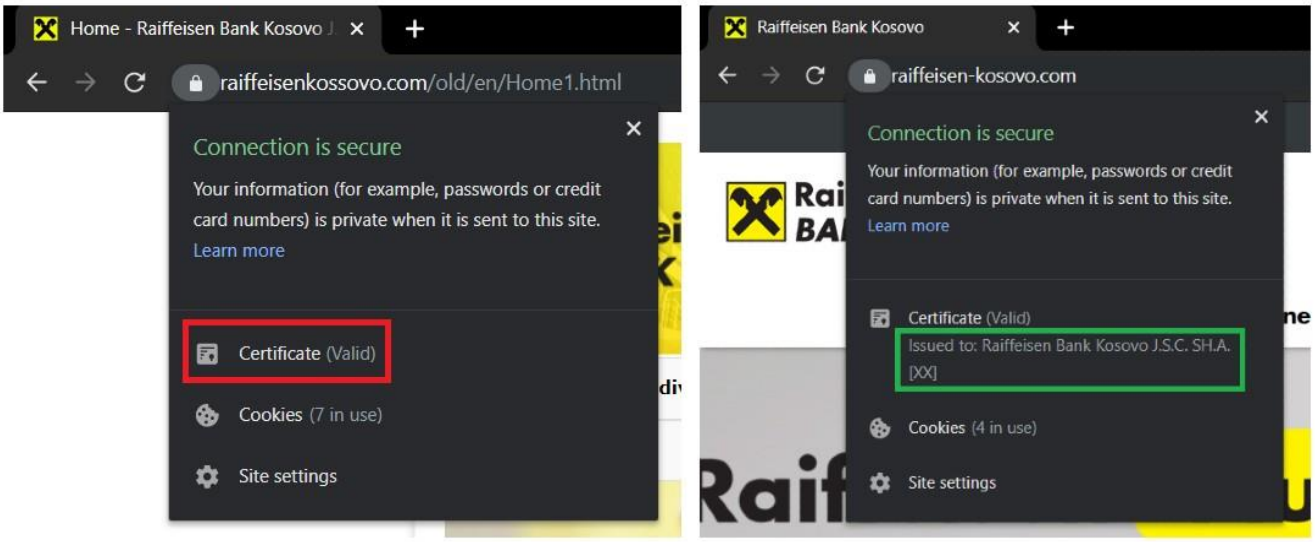

Figura 3 – Informacionet e certifikimit përmes kompjuterit