Additional Security Information

1. You are your best defense

First and foremost, the latest cybersecurity solutions alone cannot fully protect you from malicious actors. Attackers mainly achieve results by targeting you with the key objective of stealing passwords, credit card numbers, or compromise your device in general – often by creating a sense of urgency. For instance, they might deliver email warnings in the name of the bank that require you to follow a specific, but harmful, link. By using common sense and paying close attention to details, you can spot and avoid such scams.

2. Be vigilant

When receiving an unexpected email or text message, pay close attention to small details. If there is a hyperlink attached to text or an HTML button referenced, then use your computer and hover your mouse over them – most of web browsers or email clients will show the real link associated. If there is no official URL, or you click them from your mobile device and the page requires you to enter a password or download anything, simply dismiss them. On the other hand, if there is an attachment, check the extension of the file. Common malicious programs use *.exe, .scr, .vbs, .rtf, .doc, .docm, .xls, .xlsm, .zip,* and so on. Unless you absolutely trust the sender party, never click on the "*Enable Editing*" button in Microsoft Office programs.

3. Take extra care of your sensitive information

Credentials such as passwords, PIN numbers, and Credit Card details should be kept private and securely stored in safe locations. Modern computing speeds have made the eight-character stereotype vulnerable, therefore a complex and distinguished password should be used. If you use a password manager to store e-Banking credentials, a master password should be also set which comes in handy if the device is compromised. Please be aware that Raiffeisen Bank or public authorities never ask for any of the above-mentioned sensitive information.

4. Public computers and networks are not safe

In general, connecting your device to networks such as a public Wi-Fi may expose you to a broad number of cyber-attacks. Malicious parties can easily clone the Wi-Fi hotspot of a well-known network name (SSID) you used before – which your phone automatically connects to, if not with your own desire; thus, making your device prone to communication interception and manipulation. With a little bit of social engineering, they may even trick you into giving away credentials while the, for instance, e-Banking domain is legitimate. Public computers should also be completely avoided, attackers can record keys struck on a keyboard (a process known as "*keylogging*") and send a copy of the password you just typed back to them.

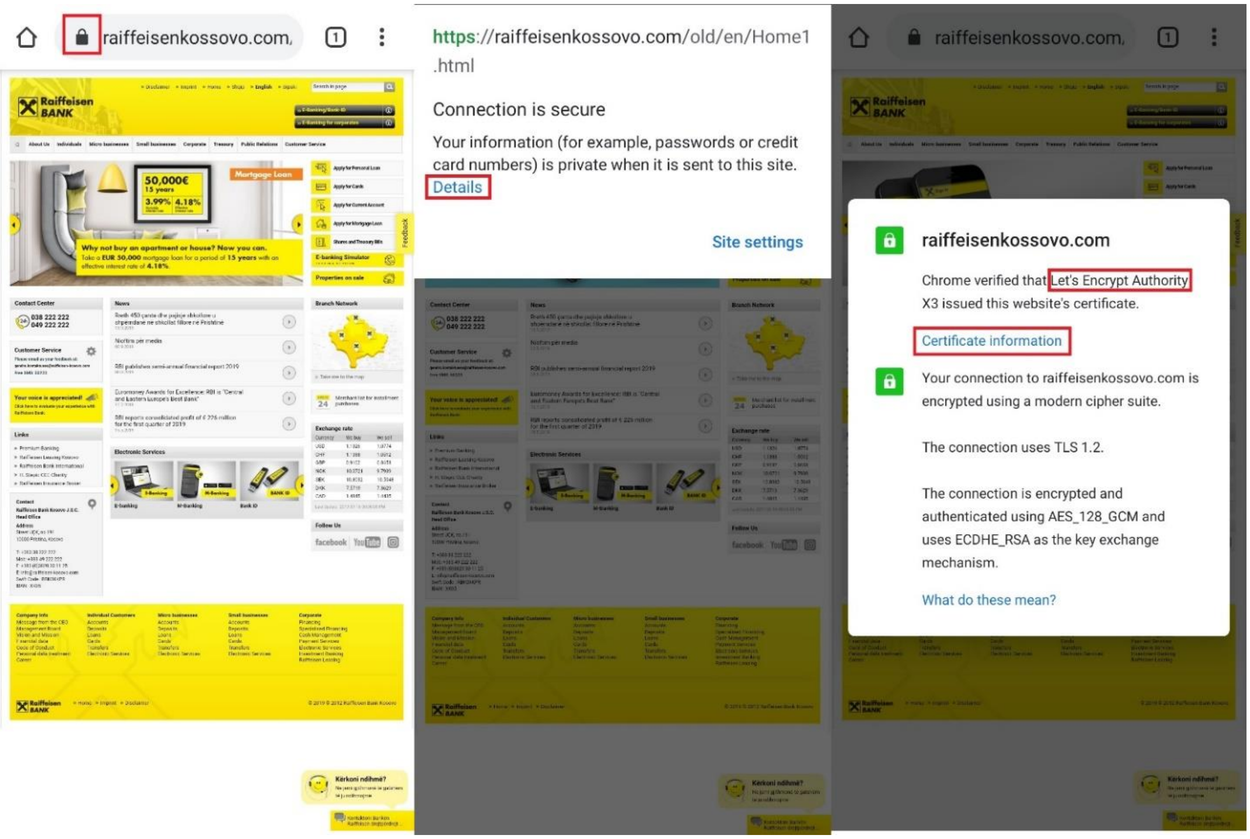
5. Ensure a safe environment

Operating systems and applications constantly receive updates from vendors to introduce features and security patches, hence, it is important to stay on the loop and not dismiss them. Make sure that you have an antivirus solution installed and the firewall enabled. Never install programs from unknown or untrusted sources, otherwise you risk of transferring malware along with them. Moreover, regular backups are important, and they should be stored separately from the device(s) you frequently use.

Fraud Websites

Cloning legitimate websites is easy and very common, where on the other hand, registering a similar fraudulent domain which are hard to spot requires creativity and luck – however totally possible. A few years ago, most of these abusive websites were not equipped with an SSL/TLS certificate to encrypt the communication between your device and server, which was a red flag to begin with. Today's attackers are using both certificates and trusted intermediaries such as CloudFlare while still stealing credentials.

Consequently, spotting fake websites requires some work considering that not everyone possesses technical knowledge. We took a use case for "*raiffeisenkossovo.com*" – which is an SSL-equipped clone of the old website platform before Raiffeisen Plus was released – and which is similar to our legitimate "raiffeisen-kosovo.com". To confirm that this website is indeed fraudulent, we can commence by clicking the lock icon (which confirms the presence of an SSL certificate), going into "Details", after which the first red flag is raised as seen in Figure 1.



https://raiffeisenkossovo.com/old/en/Home1.html

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

raiffeisenkossovo.com

Chrome verified that Let's Encrypt Authority X3 issued this website's certificate.

Your connection to raiffeisenkossovo.com is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

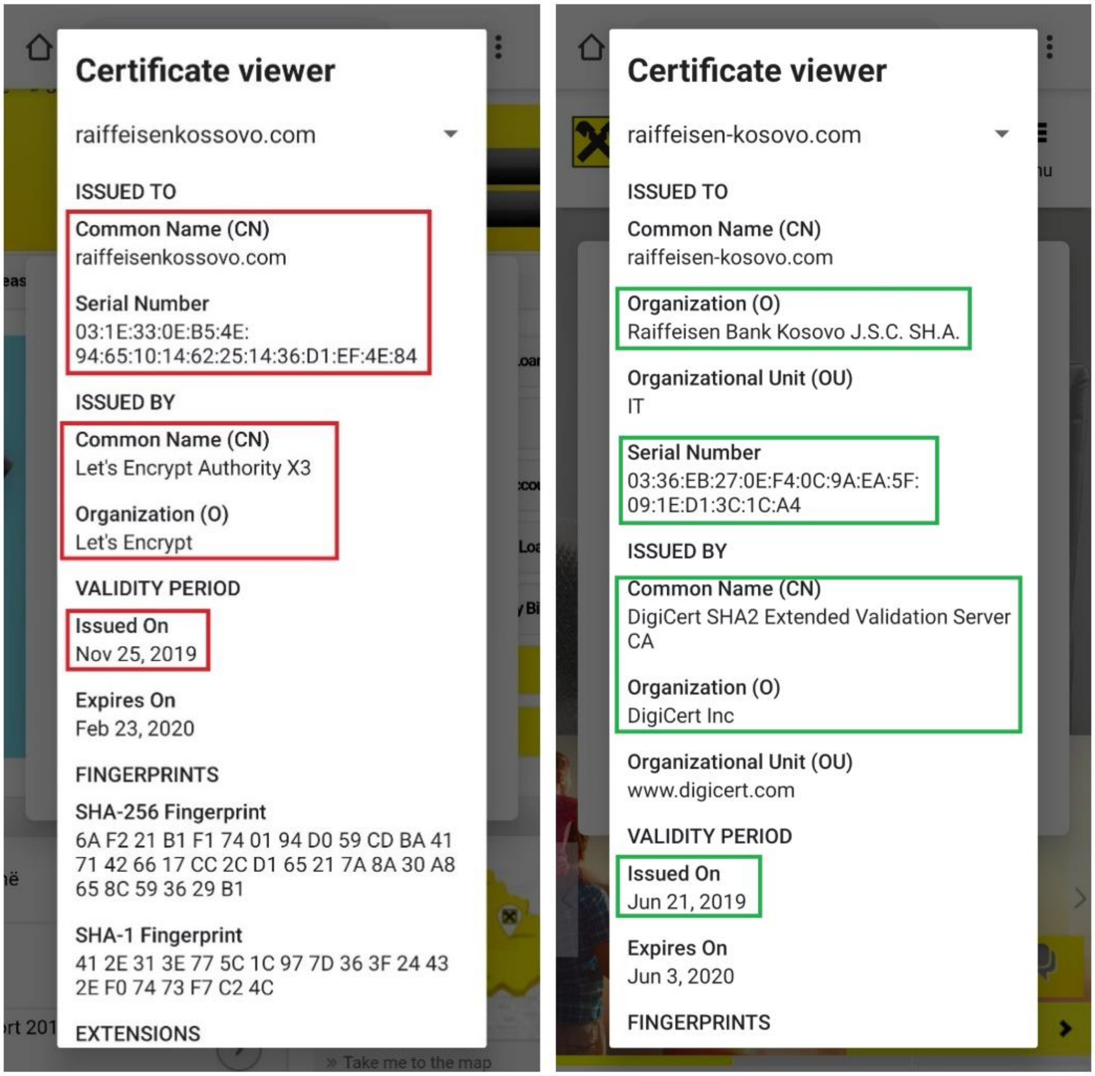
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

Figure 1 - Verifying site authenticity via phone

A certificate authority (CA) is an entity which validates the identities of companies and organizations worldwide by issuing these trusted SSL/TLS certificates. There are many such well-known authorities, some which offer free certificates and others issue paid ones. While the level of protection from encryption does not differ, free SSL certificates authenticate only the domain that is used for while paid SSL certificates have a much higher level of identity validation.

"*Let's Encrypt*" is a free and open CA which is often abused by cyber criminals to authenticate their fraudulent domains such as "*raiffeisenkossovo.com*". On the other hand, Raiffeisen Bank uses "*DigiCert*" as its CA, a company which provides the highest authentication available which makes the process of abusing our correct brand name unfeasible.

Figure 2 shows the comparison between "*raiffeisenkossovo.com*" and the legitimate "*raiffeisen-kosovo.com*":



Certificate viewer

raiffeisenkossovo.com

ISSUED TO

Common Name (CN)
raiffeisenkossovo.com

Serial Number
03:1E:33:0E:B5:4E:
94:65:10:14:62:25:14:36:D1:EF:4E:84

ISSUED BY

Common Name (CN)
Let's Encrypt Authority X3

Organization (O)
Let's Encrypt

VALIDITY PERIOD

Issued On
Nov 25, 2019

Expires On
Feb 23, 2020

FINGERPRINTS

SHA-256 Fingerprint
6A F2 21 B1 F1 74 01 94 D0 59 CD BA 41
71 42 66 17 CC 2C D1 65 21 7A 8A 30 A8
65 8C 59 36 29 B1

SHA-1 Fingerprint
41 2E 31 3E 77 5C 1C 97 7D 36 3F 24 43
2E F0 74 73 F7 C2 4C

EXTENSIONS

Certificate viewer

raiffeisen-kosovo.com

ISSUED TO

Common Name (CN)
raiffeisen-kosovo.com

Organization (O)
Raiffeisen Bank Kosovo J.S.C. SH.A.

Organizational Unit (OU)
IT

Serial Number
03:36:EB:27:0E:F4:0C:9A:EA:5F:
09:1E:D1:3C:1C:A4

ISSUED BY

Common Name (CN)
DigiCert SHA2 Extended Validation Server CA

Organization (O)
DigiCert Inc

Organizational Unit (OU)
www.digicert.com

VALIDITY PERIOD

Issued On
Jun 21, 2019

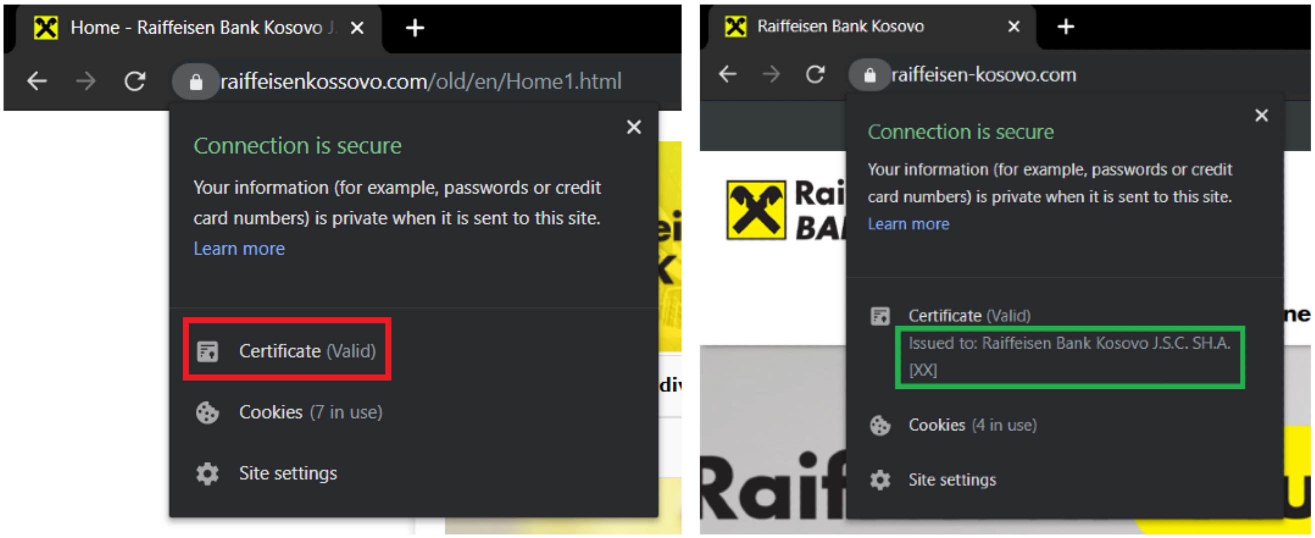
Expires On
Jun 3, 2020

FINGERPRINTS

Figure 2 - Certificate details via mobile

- "*raiffeisenkossovo.com*" uses the free "*Let's Encrypt*" authority, which is the first red flag, whereas "*raiffeisen-kosovo.com*" uses the paid and correct "*DigiCert*" one;
- "*raiffeisenkossovo.com*" is issued recently (at the time of writing this), which is another red flag because typically such domains do not last long;
- You can notice the full business name of "*Raiffeisen Bank Kosovo J.S.C. SH.A.*" at "*raiffeisen-kosovo.com*" which is a positive indicator that the site really belongs to Raiffeisen Bank Kosovo.

Similarly, you can validate authenticity through a desktop computer in a more convenient matter:


Home - Raiffeisen Bank Kosovo J.
raiffeisenkossovo.com/old/en/Home1.html
Raiffeisen Bank Kosovo
raiffeisen-kosovo.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)

Cookies (7 in use)

Site settings

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Learn more

Certificate (Valid)

Issued to: Raiffeisen Bank Kosovo J.S.C. SH.A. [XX]

Cookies (4 in use)

Site settings

Figure 3 - Certificate information via PC