Sigurnost na internetu

ProCredit Bank

1.Malware

Šta je malware?

Zlonamjerni program koji nanosi štetu podacima, uređajima ili ljudima najčešće instaliran na računar sa/bez znanja korisnika.

Kako?

Moguća instalacija na računar korisnika:
- Bez znanja korisnika: Posjeta zaraženih web stranica
- Akcijom korisnika: Otvaranje zaraženog priloga ili attachmenta mail-a, pokretanje linkova, otvaranje pop-up reklama itd.

Zašto?

Krađa osjetljivih informacija korisnika u svrhu zloupotrebe npr. krađa kredencijala (korisničko ime/šifra), informacija o broju kartice/PIN-a ili drugih osjetljivih informacija za ostvarivanje finansijske koristi.

Kako prepoznati da je Vaš računar zaražen?!

- lažne sigurnosne notifikacije,
- usporen sistem,
- pretjerana količina pop up reklama, itd.

1.Malware

Mjere zaštite:

- Instalirajte antivirus,
- Pažljivo preuzimajte programe sa interneta
- Pravite rezervne kopije podataka
- Ne otvarajte linkove/priloge sumnjivih mailova
- Koristite različite šifre i često ih mijenjajte

Grupe malware prema nacinu širenja:

Virus - je zlonamjerni softver pridružen dokumentu ili datoteci koji podržava makronaredbe za izvršavanje koda i širenje od računara do računara. Nakon preuzimanja, virus će mirovati dok se datoteka ne otvori i ne koristi. Virusi su dizajnirani da poremete sposobnost rada sistema. Kao rezultat, virusi mogu uzrokovati značajne operativne probleme i gubitak podataka.

Crvi - su zlonamjerni softver koji se brzo replicira i širi na bilo koji uređaj u mreži. Za razliku od virusa, crvi ne trebaju programe na računaru za širenje. Crv zarazi uređaj putem preuzete datoteke ili mrežne veze prije nego što se razmnoži i raspršiekspponencijalnom brzinom. Poput virusa, crvi mogu ozbiljno poremetiti rad uređaja i prouzročiti gubitak podataka.

Trojanski virusi - maskirani su u korisne softverske programe. No nakon što ga korisnik preuzme, trojanski virus može dobiti pristup osjetljivim podacima, a zatim ih mijenjati, blokirati ili brisati. To može biti izuzetno štetno za rad uređaja kao i pristup osjetljivim informacijama. Za razliku od virusa i crva, trojanski virusi nisu dizajnirani da se sami repliciraju.

2.Phishing

Šta je phishing?

Internet prevara u kojoj napadač pokušava iskoristiti povjerenje korisnika i doći do privatnih podataka (korisničkog imena, šifre, podataka o platnim karticama).

Kako?

Napadač se predstavlja kao pouzdana osoba ili firma iz korisnikovog svakodnevnog okruženja. Koristeći ovu metodu, napadač korisnika navodi na lažnu e-mail adresu/web stranicu, te zahtjeva unos privatnih podataka.

Zašto?

Napadači koriste phishing kako bi došli do korisnikovih privatnih podatka i iskoristili ih za svoju finansijsku korist.

Pošiljaoc je nepoznat:

- Sumnjiva domena - xxxxxxx@jszklo.lo
- Nepersonalizirani naziv e-mail adrese frtd2125@gmail.com
- Sadržaj e-maila upućuje na otvaranje linkova i priloga u mailu

Pošiljaoc je poznat:

- Zahtjeva dostavljanje privatnih podataka
- Zahtjeva uplatu novčanih sredstava
- Šalje podatke o promjeni računa i zahtjeva uplatu

2.Phishing

Mjere zaštite:

- Nepovjerljivost prema svakom mailu koji zahtjeva unos ličnih podatka/uplatu novčanih sredstava
- Na društvenim mrežama ograničiti dostupnost ličnim podacima
- Ne otvarati linkove/priloge iz neočekivanih mailova
- Ne odgovarati na sumnjive mailove
- Provjeravati da li web stranica ima sigurnosnu vezu „https://“ ispred naziva
- Sumnjive mailove provjeravati putem telefona ili drugih komunikacijskih kanala poznatih od ranije

Vrste phishinga:

E-mail spoofing – Napad e-mail porukama sa falsifikovanih adresa (krađa domene). E-mail ne sadrži elemente sumnjivog mail-a i traži otvaranje dokumenta u prilogu. Otvaranjem priloga instalira se zlonamjerna skripta koja prikuplja povjerljive podatke.

E-mail pharming – Napad e-mail porukama koje sadrže link lažne web stranice, koja je pritom identična izvornoj stranici. Unosom podataka putem te stranice korisnik napadaču pruža mogućnost da zloupotrijebi podatke.

3.Ransomware

Šta je ransomware?

Digitalni mehanizam, kreiran za iznudu finansijskih sredstava, koji širi malware na računar i šifruje sve lične datoteke.

Kako?

Napadač šalje mail u kojem traži pokretanje linka ili otvaranje priloga mail-a. Na taj način pokreće se maliciozni program koji nečujno u pozadini računara šifrira datoteke. Nakon što je šifriranje završeno, korisnik je prisiljen da izvrši otkup svojih datoteka bez garancije da će datoteke zaista biti vraćene.

Zašto?

Cilj napadača je da dođe do finansijskih sredstava.

Pošiljaoc je nepoznat:

- Sumnjiva domena - xxxxxxx@jszklo.lo
- Nepersonalizirani naziv e-mail adrese frtd2125@gmail.com
- Sadržaj e-maila upućuje na otvaranje linkova i priloga u mailu

Pošiljaoc je poznat:

- Zahtjeva dostavljanje privatnih podataka
- Zahtjeva uplatu novčanih sredstava
- Šalje podatke o promjeni računa i zahtjeva uplatu

3.Ransomware

Mjere zaštite:

- Instaliranje antivirus alata
- Instaliranje anit-ransomware alata
- Redovno ažuriranje operativnog sistema i aplikacija instaliranih na računaru
- Ne otvarati linkove/priloge sumnjivog maila, pop up oglase na web stranicama
- Praviti rezervne kopije podataka
- Upotrebljavati privatne virtualne mreže (VPN) kad god je moguće

4.Hakovanje

Šta je hakovanje?

Hakovanje opisuje aktivnosti koje pojedinci ili organizacije sprovode kako bi dobili neovlašteni pristup računarskim sistemima. Izazvano je različitim motivima-profit, protest, osveta, izazov itd.

Kako?

Napadi se sastoje obično od tri koraka:
- Prikupljanje informacija o žrtvi
- Analiza ranjivosti žrtve
- Iskorištavanje prikupljenih podataka za napad i postizanje ciljeva

Za napade se koriste različite tehnike i alati. Najčešće se koriste skeneri ranjivosti, dekoderi lozinki, packet snifferi, spoofing napadi (phishing), social engineering, trojanci, virusi, crvi. Svi napadi pomenuti u ovoj brošuri pomažu napadaču da preuzme kontrolu nad podacima/računarom.

Zašto?

Hakovanjem računara, haker dolazi do privatnih informacija korisnika koje kasnije može iskoristiti protiv žrtve ili poznanika iz njegovog okruženja. Hakovanje na Internetu može imati za cilj rušenje ili tzv. deface (promjena izgleda naslovne stranice) web stranica, krađu informacija sa servera e-maila, krađu novca od e-trgovina i tako dalje.

4.Hakovanje

Kako prepoznati da je Vaš računar zaražen?

- Antivirus je isključen
- Neki od programa i datoteka su izbrisani
- Pojavljivanje nepoznatih ikonica na računaru
- Računar je veoma spor
- Neobično ponašanje web kamere
- Printer ne radi kako treba

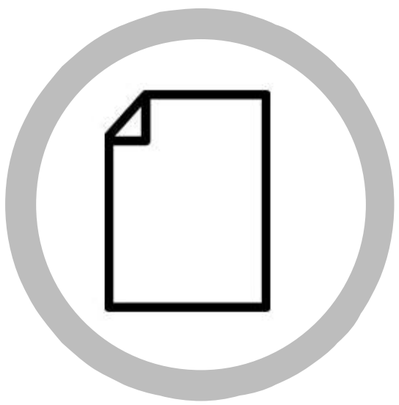
Neke od mjera zaštite:

- Koristite jake šifre (ne treba uključivati u šifru lične informacije)
- Koristite duplu potvrdu (verifikacije) gdje god je moguće
- Budite oprezni sa otvorenim Wi-Fi mrežama
- Ne ostavljajte lične podatke na sumnjivim web stranicama
- Na društvenim mrežama ograničite količine ličnih podataka

Elementi sigurne web stranice/e-maila

Kako prepoznati legitimnu web stranicu

Postoje mnogi načini prikrivanja lažne web stranice i kada stranica izgleda identično originalnoj stranici.



Ikona - ova se ikona prikazuje za http:// web lokaciju. Na takvoj stranici izbjegavajte unošenje osobnih podataka kao što su korisničko ime, lozinka ili podatke o bankovnim računima.

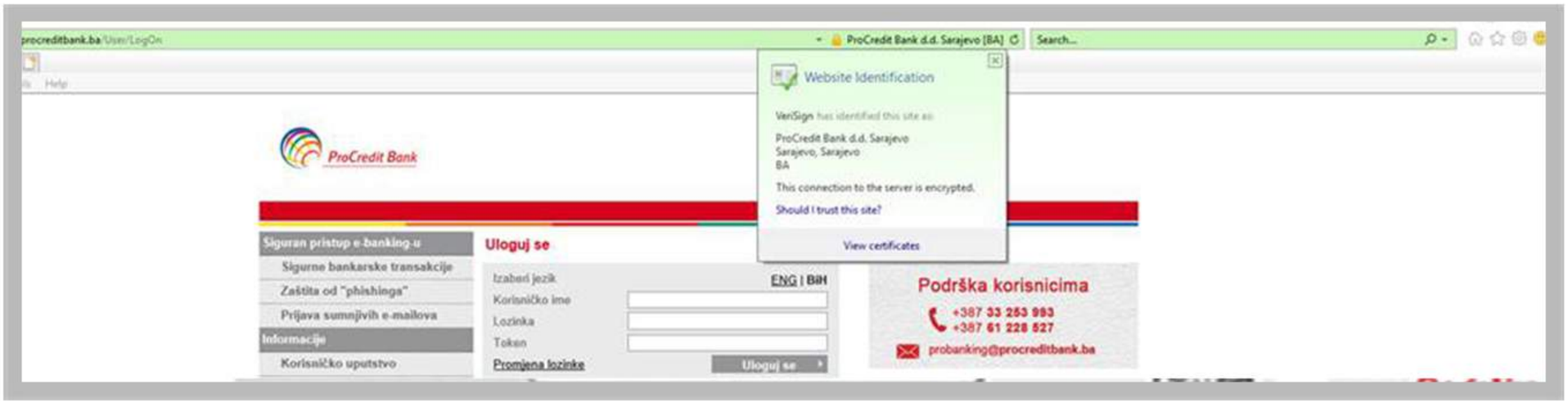
Ikona - ova ikona se prikazuje za https:// web lokaciju. Na toj stranici je preglednik uspostavio sigurnu vezu s posjećenom stranicom.
Provjerite adresu (URL) – da li je ispravno napisana, da li u nazivu nedostaju slova (npr. Paipal umjesto Paypal ili neka druga vrsta permutacije slova i detalja) Primjer elemenata zaštite web stranice donosimo kroz primjer web platformi ProCredit Banke.

Elementi sigurne web stranice/e-maila

Elementi sigurne web stranice

Primjer: ProCredit Bank

Internet bankarstvo
https://probanking.procreditbank.ba

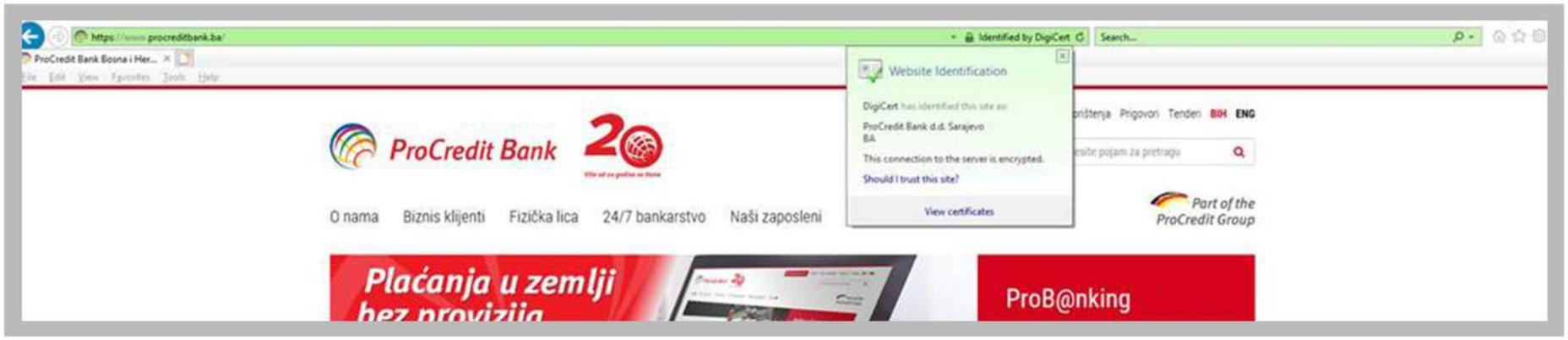


Elementi sigurne web stranice/e-maila

Elementi sigurne web stranice

Primjer: ProCredit Bank

Web stranica
https://procreditbank.ba



Elementi sigurne web stranice/e-maila

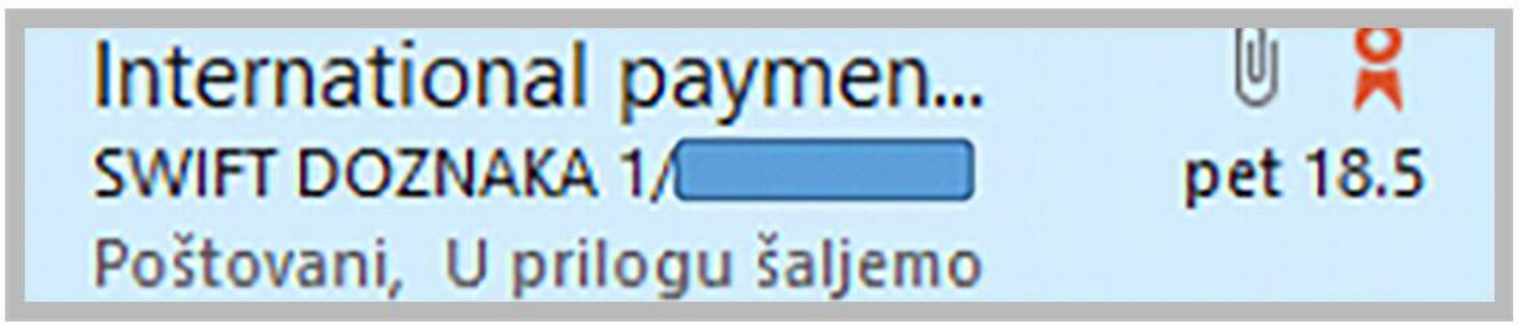
Elementi sigurnog e-maila

Primjer: ProCredit Bank

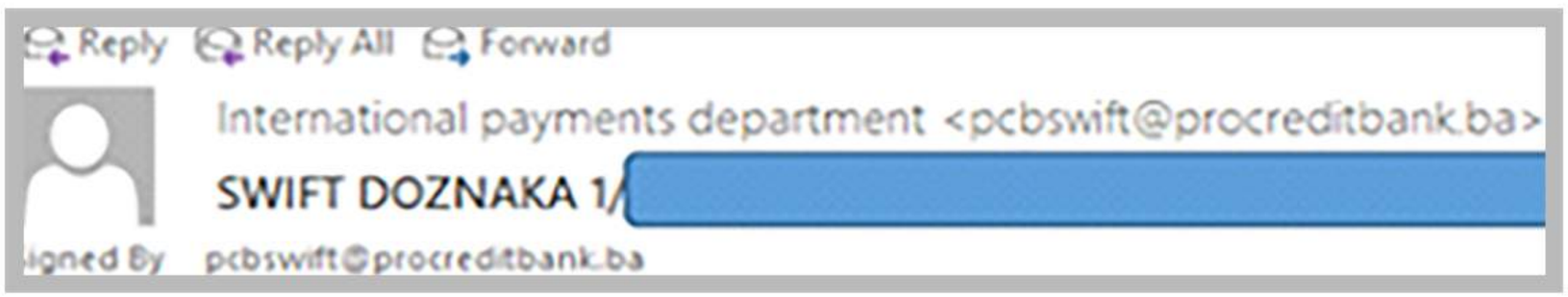
Digitalni certifikati

Za korisnike SWIFT servisa ističemo da mail banke pcbswift@procreditbank.ba sadrži digitalni certifikat/potpis.
Kako prepoznati digitalni certifikat?

1. Za korisnike Microsoft Outlook programa:
Email sadrži crveni pečat kao na slici:



Ispod naslova mail-a nalazi se poruka „Signed by: pcbswift@procreditbank.ba“



Elementi sigurne web stranice/e-maila

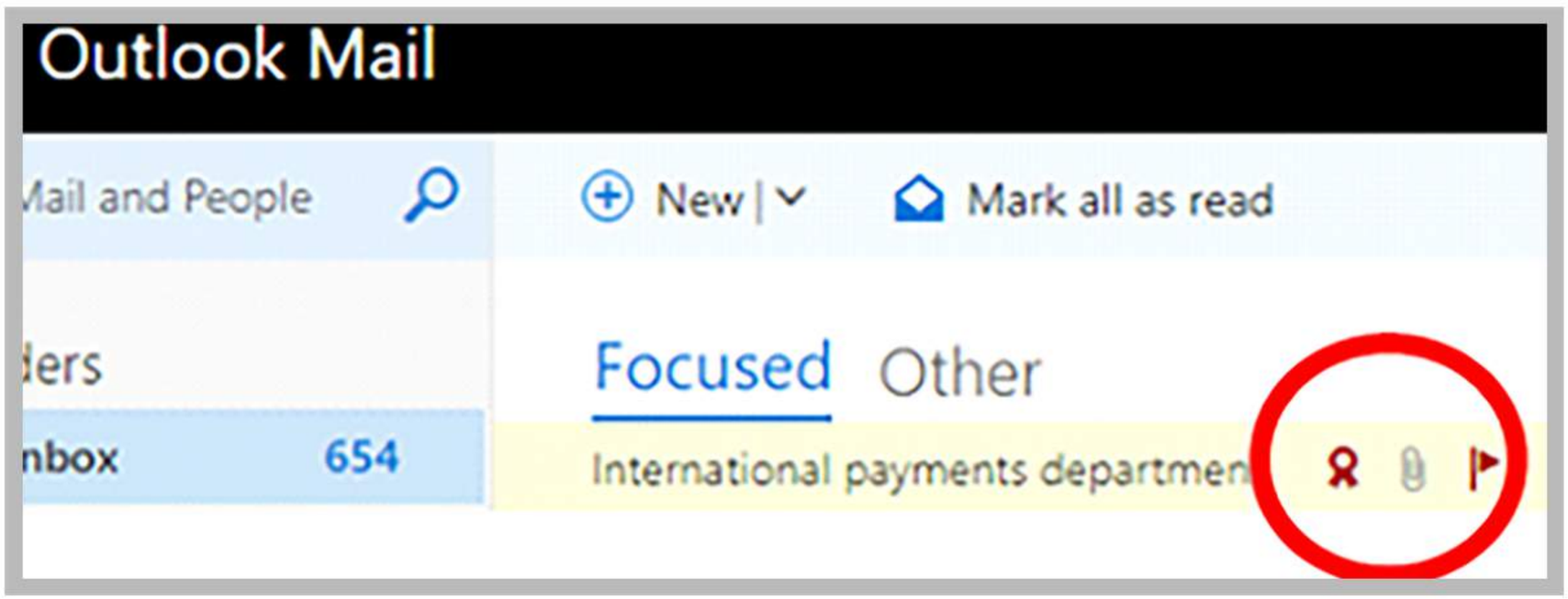
Elementi sigurnog e-maila

Primjer: ProCredit Bank

Digitalni certifikati

2. Za korisnike internet pretraživača za pristup mail-u (live.com; hotmail.com; outlook.com):

Email također posjeduje oznaku digitalnog certifikata, kao na slici:



Elementi sigurne web stranice/e-maila

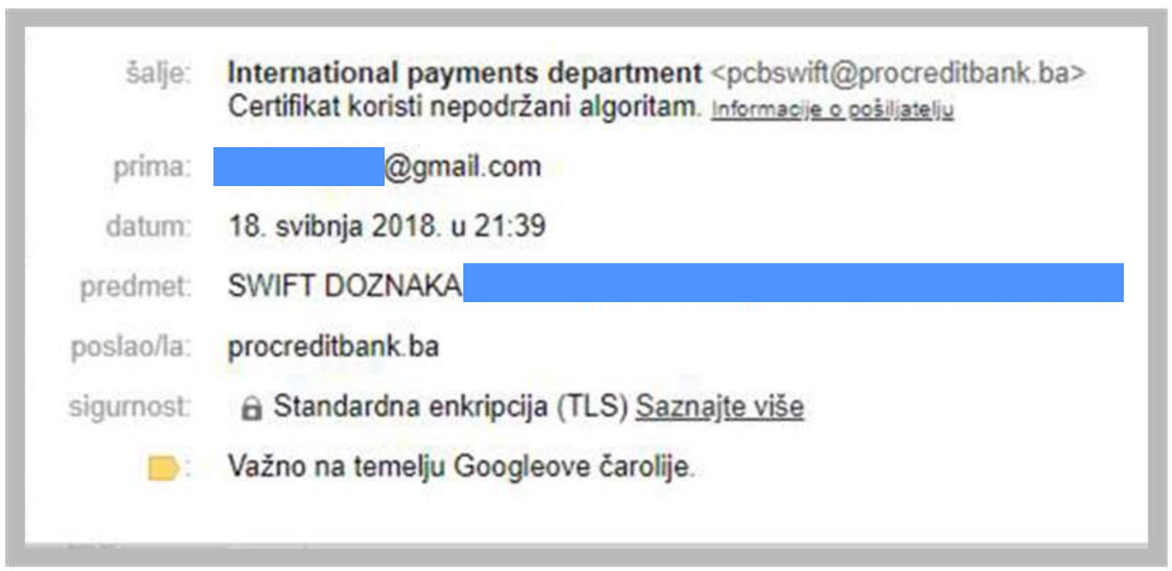
Elementi sigurnog e-maila

Primjer: ProCredit Bank

Digitalni certifikati

3. Za Gmail korisnike:

Ukoliko koristite Gmail kao Vaš primarni mailbox za isporuku Swift doznaka otvaranjem mail-a od ProCredit banke (swift mail –pcbswift@procreditbank.ba) potrebno je da izaberete „Informacije o pošiljaocu“ kao na slici niže:



Odabirom „Informacije o pošiljaocu“ dobit ćete dokaz da je e-mail digitalno potpisan od strane ProCredit banke (kao na slici):

Ostale preporuke Banke za internet sigurnost

- *Redovno ažurirajte antivirusnu zaštitu na računarima koje koristite*
- *Redovno održavajte vatrozid/firewall rješenje*
- *Zaštitite bežične mreže*
- *Redovno ažurirajte internet pretraživače koje koristite*
- *Obratite pažnju na ispravnu konfiguraciju mail servisa*
- *Koristite servise za zaustavljanje neželjene pošte (anti-spam)*
- *PIN, karticu, USB uređaj te pametni telefon čuvajte i ne činite dostupnim drugim osobama*
- *Redovno mijenjajte PIN-ove i korisničke šifre*
- *Odjavite se nakon što završite s korištenjem internet bankarstva*
- *Budite oprezni u slučajevima socijalnog inženjeringa (phishing) -svoje identifikacijske oznake, PIN-ove i druge povjerljive podatke, ne odajite drugim osobama ni na koji način*
- *Ne koristite računar u svakodnevnom radu kao administrator*
- *Radite samo s provjerenim i pouzdanim serviserima IT opreme*

Jednostavno, dostupno i transparentno!

ProCredit Bank je jedina banka u BiH sa 100% njemačkim kapitalom. Kako bi bankarstvo učinili što jednostavnijim, dostupnijim i transparentnijim, nudimo Vam da samostalno upravljate svojim finansijama kada god Vi to želite bez brige o netransparentnim troškovima.

Za više informacija o ProCredit Bank i uslugama koje nudimo posjetite web platformu koju smo razvili isključivo za vas **www.procreditbank-direct.com** ili kontaktirajte Call Center Banke na **033/250-950.**