Uputa za sigurnost internetskih plaćanja

SADRŽAJ

1 UVOD

BANKA KOVANICA d.d. (dalje u tekstu Banka) kontinuirano brine o sigurnosti svih svojih financijskih servisa pa tako i usluge Internet bankarstva (nadalje „KOnet“) primjenom najsuvremenijih tehnologija zaštite te provodi preventivne mjere kako bi se i ubuduće osigurala maksimalna moguća zaštita.

Usluga je dostupna uz visoku fleksibilnost te joj je moguće pristupiti s različitih tipova uređaja (računalo, tablet, smartphone uređaj i dr. povezanih s Internetom), neovisno o lokaciji korisnika.

Korisnici KOnet-a osiguravaju visoki nivo zaštite ako se pridržavaju niže navedenih naputaka.

2 SVRHA DOKUMENTA

Opisati pravila kojima se osigurava sigurnije korištenje usluge Internet bankarstvo.

3 SIGURNOST INTERENETSKIH PLAĆANJA

Kako bi osigurali sigurnije korištenje usluge Internet bankarstva potrebno je pridržavati se naputaka koje opisujemo u ovom poglavlju.

3.1 Licencirani operativni softver (OS-a) te ostale aplikacija novije generacije

- Korištenje licenciranih verzija OS-a (minimalno Windows 7 ili novije) ili alternativnih besplatnih OS-ova (novije verzije Linux-a ili Androida/iOS za smartphon uređaje).
- Automatsko preuzimanje i pravovremena instalacija (čim su izdane) sigurnosnih zakrpi za operativni sustav.
- Instalacije najnovijih zakrpa klijentskih aplikacija (poznatijih Internet i PDF preglednika – Google Chrome, Internet Explorer, Firefox, Acrobat Reader i dr.) instaliranih na uređajima čime se ranjivosti softvera smanjuju na najmanju moguću mjeru.
- Prilikom redovnog rada na računalu koristite korisnički račun sa smanjenim privilegijama (standardni korisnik) i s uključenom „korisničkom kontrolom pristupa“ (UAC -User Acces Control) notifikacijom.
- Preporuka je da prilikom prijave ili korištenja KOnet-a ne posjećujete druge web stranice ili otvarate druge aplikacije.

3.2 Antivirusni i antimalver program te osobni vatrozid

- Na uređaju s kojeg pristupate usluzi KOnet važno je imati instaliran antivirusni program (besplatno ili komercijalno rješenje) koji će prepoznati i sprečavati djelovanje malicioznog softvera.
- Moderni OS imaju ugrađen i osobni vatrozid. Potrebno je imati uključenu i ovu funkcionalnost koja će ograničavati i kontrolirati mrežnu komunikaciju sa Internetom.

3.3 Snažna zaporka i pravilna pohrana

- Na korisničkim računima OS-a te aplikacijama koje dnevno koristite (email, Skype, socijalne mreže itd..) prilikom kreiranja zaporki upotrebljavajte minimalno 10 znakova sa velikim i malim slovima brojevima te specijalnim znakovima (koje nisu smislene riječi iz rječnika). Na taj način stvarate snažnu zaporku (npr. 100%L3atHeR).
- Zaporke je vrlo važno periodički (preporuka svakih 90 dana) mijenjati, čak i ukoliko Vas sustav ne prisiljava na to.
- Zaporke ne zapisujte na papire oko računala, bilježnice ili u word, excel dokumente na računalu. Za pohranu zaporki koristite aplikacije za upravljanje zaporkama. Izbjegavajte aplikacije za upravljanje zaporkama koje vaše zaporke pohranjuju u cloud.

3.4 Općenite sigurnosne preporuke

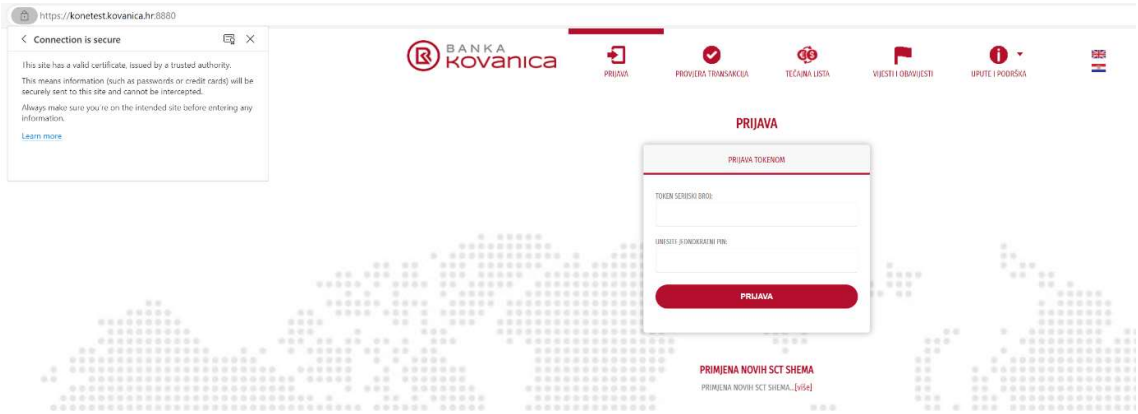
- Prilikom dnevnog korištenja računala ne dopustite izvršavanje aplikacija koje niste željeli pokrenuti i niste sigurni koja je njihova namjena (npr. lažni antivirusni program). Takve aplikacije se pojavljuju prilikom posjećivanja stranica sumnjivog karaktera (ilegalni softver i sadržaj, sumnjive poslovne ponude te stranice za odrasle) pa ih je preporučljivo ne posjećivati s računala koje koristite za financijske usluge banke.
- Ne otvarajte email poruke i privitke ili poveznice sumnjivog sadržaja i nepoznatog pošiljatelja.
- Ne šaljite nikakve osobne podatke, podatke o karticama ili tokenu kao odgovor na poruke ili telefonske pozive koje Vam „navodno“ šalje Banka (a da znate da niste tražili izričite zahtjeve za istima ili niste prethodno bili u kontaktu s Bankom).
- Nemojte javno objavljivati Vaše osobne dokumente (osobna, zdravstvena, vozačka, bankovne kartice) kako ne bi postali žrtva krađe identiteta ili prijevare.

- Zaštitite računalo/laptop i pametni telefon od krađe, gubitka i neovlaštenog uvida u podatke, pogotovo u javnim prostorima
- Više o cyber sigurnosti na poveznici: https://www.cert.hr/ (CERT je nacionalno tijelo RH za prevenciju i zaštitu od računalnih ugroza) ili na poveznici https://www.cert.hr/jesi-li-i-ti-hrvatski-naivac/

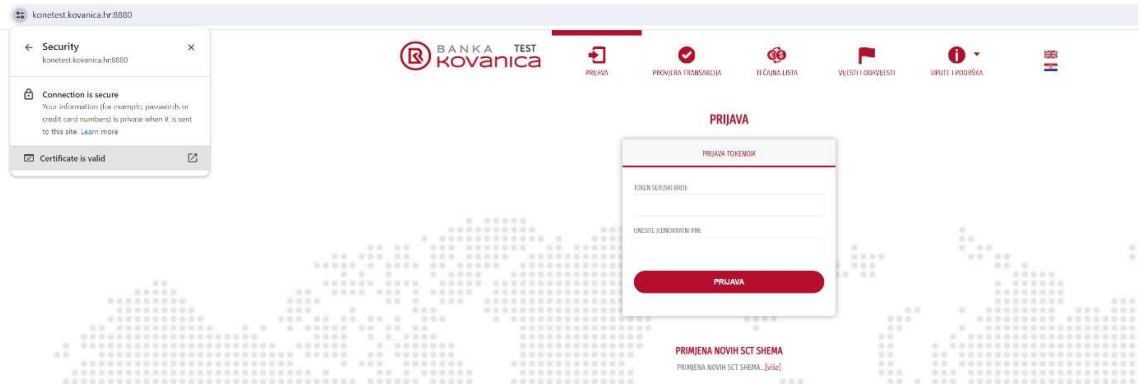
Važno! Banka Vam može poslati e-poruke s korisnim savjetima i informacijama o proizvodima ili uslugama, ali Vas nikada neće tražiti putem e-poruke podatke o računu, PIN ili sigurnosni kod kartice (CVC) ili kreiranje jednokratnih lozinki putem tokena.

3.5 Pristup KOnet usluzi te kako prepoznati Bančinu aplikaciju na Internetu

- Uvijek pristupajte aplikaciji KOnet na način da sami upisujete web adresu (engl.URL) https://konet.kovanica.hr u web preglednik ili koristite link sa službene stranice Banke https://www.kovanica.hr.
- Nikada nemojte koristiti poveznice koje ste zaprimili od nekog putem e-maila ili preko neke druge web stranice koja ne pripada Banci.
- Da biste bili sigurni da ste na pravoj adresi svakako prije korištenja KOnet usluge provjerite koristi li Bančina adresa sigurnosni zaštićeni protokol te valjanost digitalnog certifikata izdanog od DigiCert renomiranog izdavača.



Slika 1. Primjer izgleda Konet certifikata na Microsoft Edge web pregledniku



Slika 2. Primjer izgleda KOnet certifikata na Google Chrome web pregledniku

- Ukoliko ste poslovni subjekt, a imate više ovlaštenih osoba za raspolaganje sredstvima na računu, svakako ugovorite autorizaciju transakcija s više od jednog potpisnika

4 ZAVRŠNE ODREDBE

S ciljem postizanja što veće sigurnosti korištenja uređaja s kojeg pristupate KOnet usluzi iznimno je važno primjenjivati sve navedene preporuke. Često je napadaču dovoljno da korisnik ne primijeni samo jednu od navedenih preporuka, što mu onda omogućuje kompromitaciju računala te u konačnici i direktni financijski gubitak.