

# Sigurnost

OTP banka d.d. je tijekom razvoja i implementacije usluga Internet bankarstva koristila i primijenila niz mjera sigurnosti koje stvaraju pouzdano i sigurno okruženje za rad korisnika naših Internet usluga.

U cilju smanjenja svih vrsta rizika uključenih u korištenje usluga Internet bankarstva donosimo vam nekoliko savjeta koji značajno smanjuju mogućnost pojave bilo kojeg oblika zloupotrebe usluge.

## Zaštita vašeg osobnog računala

Za vrijeme korištenje usluge OTPdirekt Internet bankarstva, odnosno općenito kad ste na Internetu, trebali bi djelovati s najvećom mogućom pažnjom kako bi se zaštitili od pokušaja preuzimanja kontrole nad vašim računalom (tzv. hacking) i raznih virusnih programa uz pomoć vatrozida i antivirusnih programa. Virusi mogu naštetiti vašem računalu, uništiti podatke koje posjedujete ili čak pronaći povjerljive podatke koje ste prilikom rada na računalu unosili i poslali ih trećoj osobi.

Praktični savjeti:

- Redovito ažurirajte i instalirajte zakrpe za vaš operacijski sustav i Internet preglednik
- Ne šalžite povjerljive informacije i podatke nesigurnim kanalima (e-mail ili socijalne mreže)
- Izbjegavajte preuzimanje sadržaja s Interneta iz neprovjerenih izvora
- Ne koristite linkove iz elektroničke pošte ukoliko niste sigurni u pošiljatelja poruke
- Nakon završetka korištenja usluge Internet bankarstva zatvorite vaš Internet preglednik

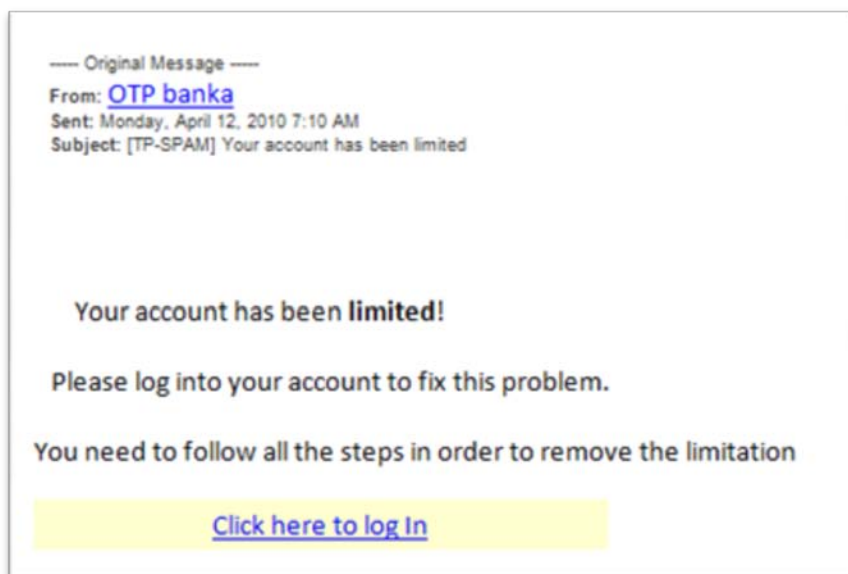
Za vašu zaštitu preporučamo da postavite zaštitu podataka u vašem Internet pregledniku na najvišu razinu kako bi osigurali najveću moguću razinu sigurnosti. To znači da će vas vaš preglednik upozoriti svaki put prije nego otvorite sadržaj koji bi mogao naštetiti vašem računalu.

## Prevenција i prepoznavanje prevare

Na potencijalni pokušaj prevare mogu vam ukazati neki od ovih događaja:

- Primitak lažne e-mail poruke unutar koje je sadržan link na krivotvorene stranice (vizualni izgled stranice vrlo sličan ili identičan stranicama Banke) na kojem se traži unos osobnih podataka, lozinki, podataka o računu, broja kartice ili PIN-a korisnika.

**Primjer lažne e-mail poruke:**



- Telefonski poziv u kojem se netko predstavlja u ime OTP banke ili neke druge institucije te traži osobne podatke koje banka ne bi tražila na takav način.

**VAŽNO: PIN je osobni identifikacijski broj poznat samo korisniku kartice i PIN-om se korisnik kartice identificira jedino i isključivo na bankomatu ili eventualno POS uređaju.**

**PIN debitne/kreditne kartice se nikada ne smije unositi prilikom pristupa bilo kojoj aplikaciji na Internetu.**

- Kada se tijekom korištenja usluge Internet bankarstva pojave **sumnjivi** prozori u vašem Internet pregledniku unutar kojih se traži unos osobnih podataka ili se pojavljuju **sumnjive** poruke vezane za rad Internet aplikacije.

## Phishing

**Phishing** (izvedenica iz engleske riječi fishing – ribolov) metoda je kojom se koriste prevaranti, i to u najvećem broju slučajeva e-mail porukom kao svojevrsnom “udicom” na koju se korisnik treba “upecati” kako bi se neovlašteno došlo do podataka o kartici i PIN-u te je u tom slučaju potrebno posebnu pozornost obratiti na web stranicu na koju se korisnik prijavio (adresu u gornjem lijevom kutu www...).

Korisnike koji su dobili ovakve ili slične poruke pozivamo da niti jedan podatak ne odaju te da o svemu obavijeste banku.

OTP banka iz sigurnosnih razloga nikada na takav način od klijenata ne traži tu vrstu informacija te stoga želi upozoriti svoje klijente da su takve poruke opasne i da otkrivanje podataka s kartica ili PIN broja može imati ozbiljne posljedice. Ukoliko primite takvu poruku nipošto ne smijete na nju odgovarati. Treba napomenuti da banka koja je izdala karticu **ne zna, nema pravo i nikada neće tražiti** broj PIN-a te da na ovakav način **neće nikada tražiti** podatke o kartici od klijenta.

Sigurnosni sustavi banaka u Hrvatskoj su na najvišoj razini. No, svaki korisnik je dužan i sam voditi računa o svakodnevnoj zaštiti podataka s kartice te se pridržavati Upute o sigurnom korištenju koji se nalaze na web stranici OTP banke i u Općim uvjetima korištenja kartica. To znači da se broj PIN- nikada nikome ne odaje, niti se podaci o karticama odaju trećim osobama, a posebnu pozornost treba posvetiti i sigurnosti zaštite računala koje se koristi za pristup Internetu.

Prilikom korištenja Internet stranica i usluga Internet bankarstva OTP banke uvjerite se da vaše računalo komunicira sa serverom OTP banke. Kako bi bili sigurni provjerite sljedeće:

1. Provjerite da adresa (URL) stranice koje posjećujete ima jedan od sljedećih oblika:

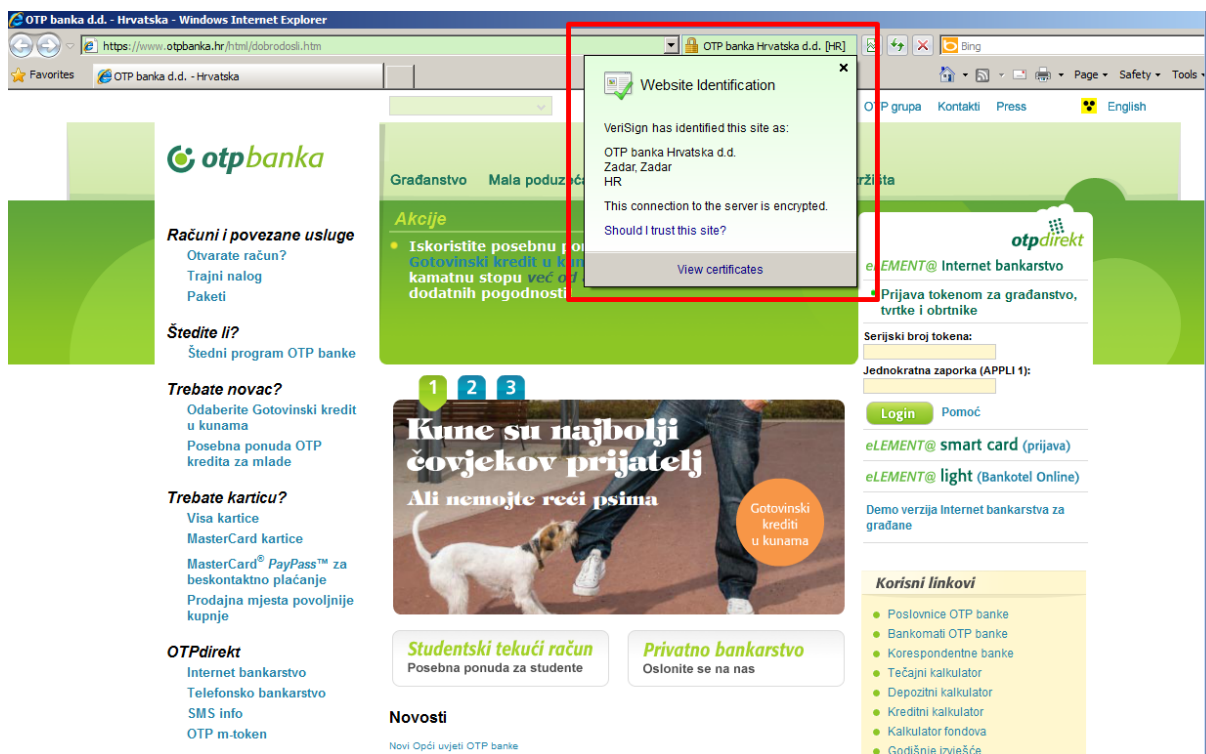
[https://www.otpbanka.hr/ ...](https://www.otpbanka.hr/)

[https://elementa.otpbanka.hr/ ...](https://elementa.otpbanka.hr/)

[https://smart.otpbanka.hr/ ...](https://smart.otpbanka.hr/)

2. Provjerite primjenu VeriSign-ovog digitalnog certifikata koji potvrđuje autentičnost servera s kojim se odvija komunikacija.

**Primjer za [https://www.otpbanka.hr/ ...](https://www.otpbanka.hr/)**



U slučaju bilo kakve nedoumice ili sumnje obavezno kontaktirajte Kontakt centar na broj 062 201 555.