Upute za sigurnost internetskih plaćanja

Obavezno koristite antivirusni program

- licencirani korisnici operativnog sustava Microsoft Windows imaju pravo besplatnog korištenja Microsoft antivirusnog programa:
  http://www.microsoft.com/security/portal
- popis ostalih proizvođača Windows antivirusnog programa:
  http://windows.microsoft.com/en-US/windows/antivirus-partners

Redovito ažurirajte računalo i uključite osobni vatrozid (eng. *personal firewall*)

- koristite licencirani operativni sustav
- redovito ažurirajte operativni sustav
- redovito ažurirajte antivirusni program
- redovito ažurirajte klijentski program (web preglednik, PDF preglednik, uredske pakete/program...)
- obavezno uključite vatrozid (eng. *firewall)* unutar operativnog sustava, a po mogućnosti i na postavkama Vašeg pružatelja internetskih usluga

Računalo ne koristite s administratorskim privilegijama

- koristite računalo kao regularan korisnik bez administratorskih privilegija
- uključite UAC (User Account Control) notify ukoliko je raspoloživ
- idealno:
  - koristite zaseban primjerak operativnog sustava namijenjen samo korištenju internetskog bankarstva i kupovini na Internetu
  - koristite zasebno, pažljivo održavano, računalo za istu namjenu

Koristite snažne lozinke i mehanizme za odobravanje

- snažne lozinke sadržavaju slova, brojeve i specijalne znakove minimalne dužine 10 znakova
- preporučljivo je koristiti rečenice umjesto riječi kao lozinke (ako imate opciju, umjesto lozinke, koristite jednokratne lozinke)
- svoje računalo kod privremenog nekorištenja, makar i na svega nekoliko minuta, uvijek zaključajte
- redovito mijenjajte lozinke za pristup Internet servisima, elektronskoj pošti i operativnom sustavu

Koristite isključivo najpopularnije Internet preglednike i redovno ih ažurirajte na aktualnu verziju

- ne koristite nepotrebne dodatke preglednika i ne preuzimajte dodatke s neprovjerenih lokacija
- obavezno uključite automatsko ažuriranje dodataka Adobe Flash, Microsoft Silverlight, PDF preglednika (Adobe Reader, FoxIT Reader, ...) ili iste onemogućite/uklonite
- neka su web filteri protiv zloćudnih stranica uvijek uključeni *(Block reported web forgeries, SmartScreen Filter, …)*

Ne preuzimajte i ne pokrećite nepotrebne izvršne datoteke, posebice s neprovjerenih lokacija

- provjerite točan naziv potpisanog izdavača *(Publisher)* aplikacija prije nego dopustite pokretanje i ne pokrećite nepotpisane aplikacije

Ne posjećujte stranice sumnjivog karaktera, posebice stranice ilegalnog software-a i sadržaja, sumnjivih poslovnih ponuda, te stranica za odrasle

- ukoliko takve stranice posjećujete, ne posjećujte ih s istog računala na kojem obavljate internetsko bankarstvo

Ne otvarajte e-mail poruke sumnjivog sadržaja i od sasvim nepoznatih pošiljatelja

- ne otvarajte poveznice (linkove) iz istih
- ne otvarajte i ne pokrećite privitke (uključujući i naizgled bezopasne neizvršne datoteke kao što su PDF dokumenti)
- budite posebno oprezni pri otvaranju poruka koje Vam navodno šalje Banka, a znate da niste poslali nikakve izričite zahtjeve za istima
- imajte na umu da se e-mail poruke i adrese vrlo lako krivotvore

Izbjegavajte korištenje CD medija te USB memory stick-ova nepoznatog porijekla

- vanjski navedeni mediji su vrlo često izvor zaraze zloćudnim software-om

Koja sigurnosno osjetljiva pitanja Vas Banka nikada neće upitati?

- PIN bilo koje RBA kartice ili RBA autentifikacijskog uređaja
- Sigurnosni kôd kreditne kartice (CSC / CVV / CVC / CID)
- Instalaciju nekog alata poslanog putem e-mail poruke
- Datum, vrijeme i iznos ili MAC kod prijave na RBA iDIREKT

Kako prepoznati i izbjeći moguću prijevaru Bančine aplikacije na internetu?

Pri svakom pristupanju uvijek vrlo pažljivo pregledajte web adresu Banke (https://www.rba.hr)

- u odnosu na autentičnu Bančinu web adresu, web adrese podmetnute od strane napadača mogu imati samo jedno slovo, znak ili točku razlike, te na prvi pogled mogu izgledati vrlo poznato

Uvijek dodatno provjerite koristi li Bančina adresa sigurnosni zaštićeni protokol (SSL) te valjanost digitalnog certifikata

- pažljivo provjerite počinje li web adresa s https:// što upućuje na korištenje zaštićenog kriptiranog kanala (SSL/TLS) između Bančinog web poslužitelja i Vašeg Internet preglednika
- odaberite ikonu lokota u web adresi Vašeg preglednika kako bi provjerili da je Bančina web adresa potpisana *(Verified by: VeriSign, Inc.)* certifikatom izdanim od strane svjetski najrenomiranijeg izdavača tvrtke VeriSign, Inc.

Kod unosa autentifikacijskih parametara za prijavu u internetsko bankarstvo obratite pozornost:

- za prijavu isključivo koristite broj kartice/tokena/mTokena i jednokratnu lozinka/OTP. Banka Vas nikada neće zatražiti dodatnu autentifikaciju prijave na servis putem Autorizacije/MAC-a.
- kod unosa autentifikacijskih parametara, pažljivo unosite svaki znak. Ukoliko je Vaše računalo napadnuto, napadač preuzima Vaše autentifikacijske parametre, a Vas informira da je došlo do neke vrste greške i traži da ih unesete ponovo. Ukoliko se to opetovano događa, a sigurni ste da dobro unosite sve parametre, Vaše računalo je vrlo vjerojatno zaraženo i preporučamo da ga isključite iz Interneta te potražite pomoć stručnjaka.

Za autorizaciju naloga za plaćanje, Banka će Vas tražiti generiranje Autorizacije/MAC-a . Upute za autorizaciju se nalaze u Uputama za korištenje servisa, te unutar samog servisa na ekranu autorizacije. Molimo da posebnu pozornost usmjerite na sadržaj sljedećih polja:

- Datum – predstavlja tekući datum ili zadnjih 8 znamenki broja računa primatelja
- Vrijeme – vrijeme autorizacije
- Iznos – zaokružena kunska protuvrijednost sume transakcija koje autorizirate (obratite dodatnu pozornost da prikazani iznos odgovara stvarnom iznosu transakcija koje želite autorizirati)
- Banka Vas nikada neće tražiti generiranje i upis Auitorizacije/MAC-a prilikom prijave na servis internetskog bankarstva ili unutar samog servisa, osim u slučajevima autorizacije naloga za plaćanje/zahtjeva.

Dodatne preporuke za poslovne subjekte:

- ukoliko imate više ovlaštenih osoba za raspolaganje sredstvima po računu, ugovorite autorizaciju transakcija s dva potpisnika
- ukoliko ste jedini ovlaštenik koji samostalno potpisuje transakcije koristeći ActivKey USB/SmartCard uređaj, zatražite token kao dodatni uređaj za autorizaciju
- kod nekorištenja aplikacije iDIREKT uvijek isključite ActivKey USB/SmartCard uređaj

Iznimno je važno primjenjivati sve preporuke dosljedno i istovremeno. Da zauzme Vaše računalo, napadač treba iskoristiti Vašu nepažnju ili nedosljednost samo jedne preporuke i to samo jednom!