# Sigurnost elektroničkog poslovanja

Putem Interneta kradljivci vrlo aktivno djeluju pokušavajući steći materijalnu korist, "Internet kradljivci" su „nevidljivi", tehnološki vrlo napredni i mogu doći od bilo kuda. Dovoljan im je pristup Internetu i mogu napasti bilo koga u svijetu, a ne samo nekoga u istom gradu ili istoj državi. U 2013. godini u svijetu je pronevjereno najmanje 113 milijardi dolara - BDP Hrvatske je 59.77 milijardi dolara, odnosno nešto veći od polovine iznosa pronevjera.

Na meti su pojedinci i usluge koji im omogućavaju stjecanje financijske dobiti, a jedna od takvih usluga je i Internet bankarstvo i korisnici Internet bankarstva. Cilj im je preuzeti kontrolu nad računalom koje potencijalna žrtva koristi za Internet bankarstvo, potom upravljajući tim računalom izdaleka prenose novčana sredstva na pomoćne račune koji mogu biti bilo gdje. Preuzimanje kontrole nad računalom gotovo je neprimjetno, a prvo napadaju manje zaštićene.

Preporukama u nastavku možete pridonijeti zaštiti sigurnosti vašeg računala i korištenja Internet bankarstva.

## SPRJEČAVANJE (PREVENCIJA)

Preventivno djelovanje značajno doprinosi zaštiti vašeg računala i računalnog sustava. Svaka ljudska nepažnja značajno narušava sigurnost računala.

### Redovna nadogradnja operacijskih sustava i programa na računalu

Operacijski sustav i programe na računalu potrebno je redovno nadograđivati - kontinuirano se pronalaze sigurnosni propusti, pogreške i nedostaci koji se ispravljaju nadogradnjama.

### Antivirusna zaštita

Antivirusnu zaštitu potrebno je koristiti na računalu, te ju redovito nadograđivati - potrebno je prilikom odabira antivirusnog programa voditi računa o njegovoj djelotvornosti i obuhvatu, te posebno o nadogradnjama koje moraju biti redovite.

### Vatrozid (firewall)

Postavljanje i pravilno podešavanje vatrozida te nadogradnje istoga - postavljanje vatrozida potrebno je provesti sukladno vašoj okolini, te je potrebno provoditi redovite kontrole postavki i nadogradnje.

### Instalirati samo programsku podršku koja je nužna za rad

Korištenje zasebnog računala na kojem je postavljena samo programska podrška nužna za Internet bankarstvo - umanjuje sigurnosne propuste, što manje programa na računalu, manje će biti sigurnosnih propusta. Računalo koje se koristi za Internet bankarstvo poželjno je ne koristiti u druge razne svrhe posebno one koje nisu nužne za rad.

### Ograničeni pristup Web stranicama na Internetu

Ne posjećivati sumnjive i nepoznate Web stranice na Internetu, posebno stranice s ilegalnim sadržajem, a posebno ne instalirati bilo kakav neprovjereni program.

### Pažnja s elektroničkom poštom

Ne otvarati i ne prosljeđivati elektroničku poštu koja je od nepoznatog pošiljatelja i/ili neočekivanog i/ili sumnjivog sadržaja - bilo kakve sumnjive e-mailove, e-mailove od nepoznate osobe, neočekivane e-mailove ili e-mailove sa sumnjivim prilozima ili linkovima nemojte otvarati i prosljeđivati već ih izbrišite.

### Pažnja s USB uređajima i CDROM/DVD

Ne stavljati nepoznate USB uređaje i CDROM/DVD medije u računalo - USB uređaj ili CDROM/DVD medij često su zaraženi i vrlo lako se prenosi zloćudni kod na računalo.

### Čuvanje podataka za pristup

Podatke za autorizaciju i autentifikaciju potrebno je čuvati - osobni autorizacijski podaci ne smiju se nikome odavati. Banka niti u kojem slučaju neće od klijenta tražiti takve podatke bilo kojem putem.

### Nadzor računala

Računalo je potrebno ugasiti ili zaključati kada niste prisutni - kada ne koristite računalo nužno je računalo ne ostavljati na način da se istom može pristupiti s Vašim ovlastima.

### Nadzor kartice

Kartice za Internet bankarstvo i ostala autentifikacijska obilježja nužno je čuvati i koristi na primjeren način - kada ne koristite karticu odnosno drugo autentifikacijsko sredstvo isto je potrebno obavezno izvaditi iz računala/čitača i čuvati na način da se ne omogući pristup i/ili korištenje neovlaštenoj osobi.

### Zaštita osobnih podataka

Ne odavati osobne podatke putem Interneta niti na drugi način.

## UOČAVANJE (DETEKCIJA) I PRIJAVA PROBLEMA

Kontinuirano je potrebno provoditi i mjere detekcije neovlaštene uporabe računala. Svako neuobičajeno ponašanje potrebno je provjeriti i utvrditi uzroke.

### Promjena izgleda Web stranice

Svaka neočekivana promjena stranice Internet bankarstva i podataka koji se traže za autentifikaciju i autorizaciju je potencijalno prijetnja koju je potrebno prijaviti Banci. U slučaju da Banka odluči promijeniti izgled Internet bankarstva kako Web stranice i/ili podataka koji se traže za autentifikaciju i autorizaciju, Banka će poslati obavijest o tome putem Internet bankarstva, kao i objaviti na svojoj web stranici obavijest o promjenama.

### Neočekivane aktivnosti

U slučajevima samoinicijativnog izlaska računala na Internet, nekontrolirane Internet aktivnosti - promjene stranice ili upada pop-up prozora, pojavljivanja neželjenih ekrana, slanje e-mail poruka ne inicirano od korisnika - svaku aktivnost koja nije inicirana od korisnika ili je na drugi način neočekivana potrebno je dodatno provjeriti.

### Neočekivane promjene

Promjene veličine datoteka, raspoložive radne memorije, zagušenje mreže, usporavanje rada računala ili načina rada programa mogu biti indikator problema s računalom - svaku neočekivanu pojavu kojoj nije poznat uzrok potrebno je dodatno provjeriti kako bi se utvrdilo uzrok i eliminiralo mogućnost zloćudnog koda ili drugih problema s računalom.

## PRIJAVA PROBLEMA

Primjenom navedenih preporuka umanjuje se mogućnost prijevare, ali je i dalje potreban kontinuirani oprez i angažman svakog korisnika Internet bankarstva, a u slučaju mogućeg problema važna je pravovremena reakcija i prijava problema kako bi se moglo pravovremeno djelovati.

Ako primijetite bilo što neuobičajeno, sumnjivo ili drugačije:

- izvadite karticu iz čitača
- isključite računalo i/ili ga odspojite s mreže - Interneta
- nazovite korisničku podršku na telefonski broj 01 4602 300

Banka ne preuzima odgovornost za zloupotrebu sadržaja ove obavijesti, odnosno posljedice radnji koje bi proizašle njenom primjenom.

**PARTNER BANKA d.d. ZAGREB**