INTERNET BANKARSTVO –

Preporuke za osiguravanje sigurnosti u sustavu

Sadržaj

1 UVOD

Ovim tekstom htjeli bismo Vam skrenuti pažnju na potencijalne rizike prilikom upotrebe Internet bankarstva i upoznati Vas s istima u što većoj mjeri.

Opisane mjere koje Vam donosimo u nastavku ovoga teksta, ne mogu Vas u cijelosti upoznati sa svim poznatim i manje poznatim načinima zlouporabe, niti Vas mogu u potpunosti zaštititi od svih opasnosti kojima ste izloženi prilikom uporabe interneta i Internet bankarstva.

Koje ćete mjere primjenjivati kako bi ste smanjili mogućnost zlouporabe na najmanju moguću mjeru, odlučujete proizvoljno.

Korištenje Internet bankarstva odnosi se na skup aktivnosti od kojih je svaka podložna nekim rizicima, pri čemu su ti rizici podijeljeni između korisnika i KentBank d.d. (u daljnjem tekstu: Banka).

Banka može provoditi mjere za smanjenje i kontrolu tih rizika u područjima na koje može utjecati, npr.:

- aplikacija Internet bankarstva ima ugrađene kontrole
- računalna infrastruktura je pod stalnim nadzorom
- procesi vezani za plaćanja su kontrolirani
- i slično.

Međutim, Banka ne može spriječiti moguće zlouporabe koje mogu biti rezultat slabosti kontrola i mjera koje provode sami korisnici, npr.:

- neadekvatna zaštićenost korisnikovih računala
- nepostojanje kontrole pristupa računalima
- nepostojanje evidencije korisnika Internet bankarstva
- otvorena dostupnost korisnikovog mobilnog telefona
- nepostojanje zaštite
- dostupan stalni PIN[1]
- i slično.

2 Rizik zaraze virusima i neovlaštenog upada u mrežu računala ili računalo

Da bi ste mogli koristiti Internet bankarstvo, morate imati pristup internetu.
Dok se koristite internetom, Vaše računalo dio je mreže računala i ako je nezaštićeno postoji mogućnost neovlaštenog preuzimanja kontrole nad Vašim računalom, preuzimanja podataka ili samo nadzora nad aktivnostima, a bilo kakva zlouporaba (čitanje, izmjena i brisanje podataka) može se dogoditi i bez Vašeg znanja i odobrenja.

Potpune zaštite od svih postojećih “upada” nema, a sigurnost korištenja interneta možete povećati poduzimajući osnovne mjere zaštite.

[1]PIN – jednokratni broj koji koristite za autentifikaciju i autorizaciju transakcija, a šalje Vam se putem SMS poruke na Vaš mobilni telefon

2.1 Upotreba interneta bez antivirusne zaštite i vatrozida

Najjednostavnija poruka elektroničke pošte može Vam nanijeti velike štete ako u sebi sadrži maliciozni kod, virus ili neki drugi oblik nepoželjnog računalnog programa.

Antivirusni programi su prilično učinkovita zaštita protiv ovakvog načina napada na računala.

Vatrozid omogućuje slijedeću razinu zaštite i u velikoj mjeri ograničava nedozvoljen pristup Vašem računalu. Nedozvoljeni pristup ne odnosi se na fizički pristup računalu, već na tehnike preuzimanja ili zadobivanja kontrole nad računalom putem posebnih programa.

3 Popunjavanje zahtjeva za Internet bankarstvo

Propusti mogu nastati i prije samog korištenja Internet bankarstva, a nastaju uslijed neispravnog popunjavanja obrazaca Banke potrebnih za aktivaciju Internet bankarstva.

Propusti mogu nastati ukoliko:

- zahtjev popunjava osoba koja za to nije ovlaštena
- zahtjev nije pregledan i odobren od strane ovlaštene osobe
- pečat kojim se potvrđuje vjerodostojnost zahtjeva nije dobro čuvan
- se unese pogrešan broj mobilnog telefona na koji korisnik prima SMS poruke s PIN-om za autentifikaciju i autorizaciju

Navedene zlouporabe mogu omogućiti da sredstvima na računu poduzeća ili računu fizičke osobe, raspolaže osoba koja za to nije ovlaštena.

Banka provjerava valjanost potpisa, pečata i prijavljenih računa za raspolaganje putem Internet bankarstva, ali ne i status prijavljenih osoba, to jest da li su one zaista zaposlenici ili ovlaštene osobe.

4 Korištenje aplikacije Internet bankarstva

Neželjeni događaji koji mogu prouzročiti pogrešnu upotrebu Internet bankarstva, a i novčanu štetu mogu se javiti:

- **Prilikom popunjavanja naloga:**

Podaci na nalogu mogu biti netočni (iznos, datum, krivi broj računa…).

Banka ne provjerava da li su podaci na nalogu točni, već samo formalnu ispravnost (jesu li sva potrebna polja popunjena, je li datum u skladu s pravilima, i slično). Odgovornost za točnost podataka za plaćanje, snosi korisnik.

- **Prilikom autorizacije naloga:**

Podaci o plaćanjima mogu biti neprovjereni, ali autorizirani.

Odgovornost za ispravnost podataka o plaćanju snosi isključivo osoba koja je autorizirala nalog putem uređaja za autorizaciju. Banka ne provjerava identitet osobe koja je nalog autorizirala već samo ispravnost same autorizacije.
Autoriziran i izvršen nalog ne može se opozvati.

5 Čuvanje mobilnih telefona koji su prijavljeni za upotrebu Internet bankarstva

Ograničavanje pristupa mobilnom telefonu koji je prijavljen za primanje SMS poruka s PIN-om, u isključivoj je domeni i odgovornosti osobe koja ga posjeduje. Moguće zlouporabe uslijed nestanka, otuđenja ili kratkotrajne "posudbe" je teško dokazati.

1) Neadekvatno čuvanje mobilnog telefona

Ostavljanje mobilnog telefona bez nadzora omogućuje drugim osobama pristup uređaju i eventualnim SMS porukama o jednokratnom PIN-u.

2) "Posudba" mobilnog telefona

Posudba mobilnog telefona drugoj osobi je potencijalna opasnost.

Mobilni telefon koji ste prijavili za upotrebu Internet bankarstva, sredstvo je za autentifikaciju i autorizaciju platnih naloga. Putem istog zaprimate jednokratni PIN.

Ako druga osoba zna vaš OIB, JMBG i stalni PIN, imajući Vaš mobilni telefon, može napraviti i autorizirati platne transakcije, pri čemu ćete vrlo teško dokazati da iste niste izvršili sami.

6 Kratke upute za povećanje sigurnosti

Navedene upute ne mogu u potpunosti onemogućiti eventualne zlouporabe Internet bankarstva, već služe isključivo za povećanje sigurnosti i smanjenje rizika njegovog korištenja.

1) Računalo pomoću kojeg ćete koristiti Internet bankarstvo treba imati aktiviranu i funkcionalnu odgovarajuću antivirusnu zaštitu i vatrozid ili mreža na koju je računalo spojeno mora imati vatrozid

Dodatno se možete posavjetovati sa svojim dobavljačem računalne opreme u vezi s povećanjem sigurnosti upotrebe interneta.

2) Kontrolirajte pristup pečatu Vašeg poduzeća koji Vam je povjeren na čuvanje

Pečat je jedan od priznatih načina utvrđivanja vjerodostojnosti dokumenata, a može se zloupotrijebiti za izdavanje raznih punomoći i ovlasti.

3) Provjerite sve podatke na zahtjevu za Internet bankarstvo

Prije potpisivanja zahtjeva, obavezno provjerite sve podatke, posebice podatke o korisniku usluge i korisničkim pravima.

4) Ne posuđujte svoj mobitel i ne ostavljajte ga bez nadzora

Današnja tehnologija omogućuje postavljanje aplikacija koje mogu SMS poruke poslane Vašem mobilnom telefonu, proslijediti na neki drugi mobilni telefon. Na ovaj način Vaš jednokratni PIN može biti dostupan nepoznatim osobama.

5) **Izbrišite SMS poruke s jednokratnim PIN-om neposredno nakon iskorištenja PIN-a**

6) **Provjerite podatke naloga za plaćanje tijekom unosa i prije autorizacije**

Banka ne provjerava točnost ni istinitost podataka, a unesene i autorizirane podatke je vrlo teško osporiti.

7) **Ne ostavljajte pokrenutu aplikaciju Internet bankarstva bez nadzora**

I 3 minute su sasvim dovoljne da se napravi šteta.

8) **Djelatnici Banke Vas nikada neće niti smiju tražiti da otkrivate svoj stalni PIN ili jednokratni koji dobivate prilikom ulaska u sustav ili za potrebe autorizacije**

Svaki neuobičajeni zahtjev od strane osoba koje se predstavljaju u ime Banke, molimo Vas budite slobodni prijaviti nam odmah po njihovim nastupu.

9) **Banka se nikada neće spajati na računala klijenta kako bi sudjelovala u izradi i provođenju transakcija ili zapažanju potencijalnih nepravilnosti na računalima klijenta**

Svaki neuobičajeni zahtjev u smislu gore izrečenog, obavezno prijavite Banci.

10) **O svim neuobičajenim događajima prilikom upotrebe Internet bankarstva, obavijestite djelatnike Banke**

Nemojte se ustručavati. Zatražite pomoć kada god Vam je potrebna. Obavijestite Banku o svakoj neuobičajenoj pojavi.

Sve preporuke koje iznosimo u ovom dokumentu, nisu jamstvo apsolutne zaštite i sigurne uporabe interneta i Internet bankarstva.

Banka nije odgovorna za bilo kakvu štetu ili posljedice koje mogu biti rezultat implementacije ovdje iznesenih preporuka.

U Zagrebu, 28. svibnja 2014.