Addiko Bank

Kjer je 2+2=4

Priporočila za varno internetno poslovanje

Addiko Bank d.d.

Addiko Bank

Priporočila za varno internetno poslovanje

V zadnjih letih se je brezgotovinsko poslovanje izjemno razširilo, zato si večina ne more predstavljati življenja brez plačilnih kartic, mnogi pa tudi brez nakupov preko spleta in uporabe spletnega in mobilnega bančništva ne. Z vedno bolj razširjeno uporabo pametnih mobilnih telefonov in tablic je internet uporabnikom še bolj dostopen, a se hkrati s tem odpirajo tudi nove možnosti za zlorabe. Udobje brezgotovinskega poslovanja nas zato lahko hitro pripravi do občutka lažne varnosti, kar kriminalci vedno bolj izkoriščajo. Za nekatere vrste zlorab se je uveljavilo poimenovanje "tatvina identitete", pri katerih se kriminalci izdajajo za osebo, ki je legitimni uporabnik plačilnega sredstva. Tovrstna zloraba se lahko zgodi vsakemu od nas.

Radi bi vas opozorili na največje nevarnosti pri brezgotovinskem poslovanju, hkrati pa podali napotke, kako se pred njimi najučinkoviteje zavarujemo. Osredotočili smo se na največkrat uporabljane načine brezgotovinskega poslovanja, in sicer plačilne kartice, internetna plačila in spletne banke. Dodali smo tudi napotke o tem, kaj storiti, ko zlorabo odkrijete. Priporočamo, da na strokovnih spletnih straneh, kot je na primer Varni na internetu (https://www.varninainternetu.si/) redno spremljate novice in napotke o varnosti.

O vseh varnostnih težavah ali z vprašanji iz področja varnosti poslovanja s plačilnimi karticami ali e-bančništvom nas lahko obvestite osebno, po telefonu 01 580 40 00, z elektronsko pošto na naslov varnost.si@addiko.com ali običajno pošto na naslov Addiko Bank d.d., Dunajska cesta 117, Ljubljana.

V nujnih primerih lahko 24 ur na dan vse dni v letu ob sumu zlorabe ali za preklic plačilnih kartic pokličete na telefonsko številko +386 (0)1 583 41 83 (Bankart d.o.o., Ljubljana), ob sumu zlorabe oziroma za blokado e-bančništva pa na +386 (0)1 580 43 00 (pomoč uporabnikom Addiko EBank in Addiko Mobile).

Najpogostejši načini zlorab podatkov

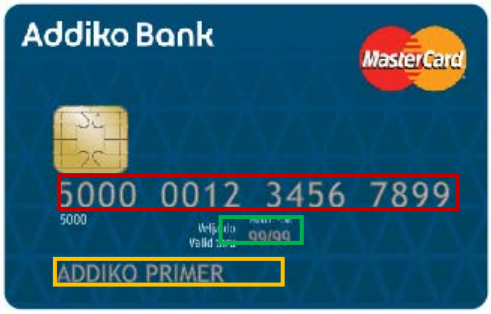
Najpogostejša načina zlorabe podatkov plačilnih kartic sta izdelava ponarejenih magnetnih plačilnih kartic in zloraba podatkov pri oddaljenih nakupih prek spleta. Ponarejene magnetne plačilne kartice kriminalci nato uporabijo na prodajnih mestih ali bankomatih, oziroma jih pri oddaljenih nakupih uporabijo neposredno, pri tem pa včasih zaradi neustreznih varnostnih zaščit na prodajnem mestu niti ne potrebujejo številke PIN ali varnostne kode za oddaljene nakupe.

Pri zlorabi podatkov za uporabo spletnega bančništva sta najpogostejša načina zlorabe prenakazovanje denarnih sredstev na račune kriminalcev preko računov prenašalcev, ki so lahko fizične ali pravne osebe, imenovane tudi denarne mule. Ti največkrat lahkomiselno računajo na hiter zaslužek s provizijo za prenakazilo, in prenos sredstev v tujino s pomočjo različnih storitev (npr. Western Union), kjer jih kriminalci z zvijačo dvignejo v banki posrednici, nato pa se za denarjem izgubi vsaka sled.

Z ukradenimi podatki o plačilnih karticah in drugimi podatki, ki so potrebni za izvedbo transakcij (npr. pri spletni banki), ter z morebitnimi ostalimi protipravno pridobljenimi osebnimi podatki, kot sta davčna številka ali EMŠO, se lahko kriminalci zlahka izdajajo za drugo osebo. Tatvina identitete je lahko za lastnika zlorabljenih podatkov hud finančni udarec, saj zlikovcu omogoča zlorabo plačilne kartice, sklepanje kreditnih pogodb, uporabo spletne banke in drugo.

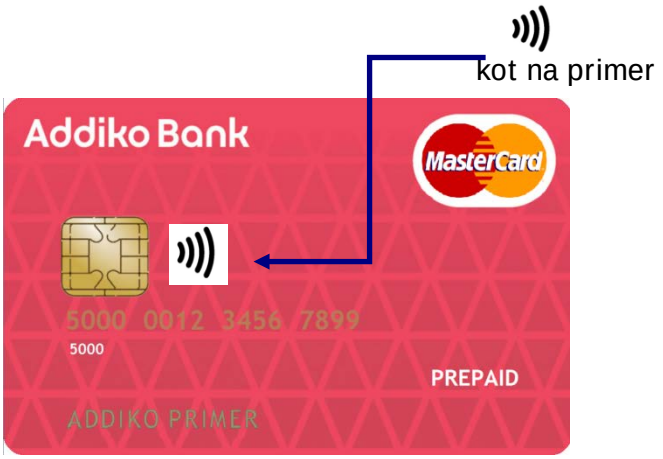
Addiko Bank

Med najpomembnejšimi podatki na magnetni plačilni kartici so podatki o uporabniku, številka kartice oziroma PAN (angl. *Primary Account Number*) in datum veljavnosti kartice, ki so odtisnjeni na sprednji strani kartice. Na nekaterih plačilnih karticah je vtisnjena varnostna številka kartice, ki se uporablja pri oddaljenih nakupih. Na karticah MasterCard Addiko Bank d.d. je ta v obliki 3-mestnega števila, ki se imenuje CVC2 (angl. *Card Verification Code*), zapisana na zadnji strani kartice. Izdajatelji plačilnih kartic varnostno številko (angl. *Card Security Code – CSC*) za oddaljene nakupe poimenujejo različno: CVC2, CVV2 in CID, kar naj vas ne zmoti, saj gre za isto stvar.



Čipne kartice, ki jih izdaja Addiko Bank d.d., so pri uporabi na terminalih POS ali bankomatih od magnetnih varnejše le v primeru, da so te naprave skladne s standardom EMV, saj uporaba čipa sicer ni možna in se podatki še vedno berejo z magnetne steze. Pri uporabi zastarelih terminalov POS in bankomatov v Sloveniji in predvsem tujini se torej še vedno soočate s starimi tveganji, zato previdnost na takih prodajnih mestih ni odveč.

Nekatere naše plačilne kartice imajo že vgrajeno najsodobnejšo tehnologijo za brezstično plačevanje PayPass, ki je enako varna kot čipna tehnologija. Te kartice imajo natisnjen znak:



Prodajna mesta, na katerih je možno brezstično plačevanje, so označena z znakom:

Addiko Bank

Brezstično plačevanje pomeni, da sta tako terminal POS kot tudi kartica opremljena s tehnologijo za brezstično plačevanje. Pri brezstičnem plačevanju se PIN uporablja le za nakupe, vredne več kot 15 evrov. Za nakupe nižjih vrednosti pa je dovolj, da kartico k terminalu le prislonite.

Plačevanje z brezstično kartico MasterCard je enako varno, kot plačevanje z običajno kartico Maestro ali MasterCard. Razlogi za to so:

- kartico imate ves čas pri sebi in je nikomur ne izročite niti za čas plačila;
- vsaka transakcija je enolična, za izvedbo transakcije pa mora biti kartica zelo blizu, največ nekaj centimetrov oddaljena od terminala POS z zgornjim simbolom;
- na brezstičnem čipu PayPass ni vašega imena, naslova in varnostnega števila CVC2, temveč zgolj številka kartice in datum veljavnosti, ob vsakem plačilu pa se podatkom doda še enkratna enolična številka transakcije;
- na podlagi podatkov prebranih s čipa za brezstično plačevanje ni možno izdelati ponarejene plačilne kartice;
- tudi če bi se s kartico terminala POS dotaknili večkrat, bo obračunan zgolj en nakup oziroma plačilo.

Splošni napotki za povečanje varnosti:

- novo kartico takoj podpišite;
- v mobilni telefon si shranite telefonsko številko za pomoč uporabnikom in preklic plačilnih kartic (+386 (0)1 583 41 83, Bankart, d.o.o.);
- pri plačilih imejte plačilno kartico vedno pri sebi, ne izročajte je nikomur, temveč jo sami vstavite v terminal POS oziroma jo potegnite prek čitalnika magnetnega zapisa;
- redno pregledujte bančne izpiske in preverite zabeležene transakcije, o morebitnih nepravilnostih pa takoj obvestite Addiko Bank d.d.;
- plačilne kartice, bančne izpiske in drugo občutljivo dokumentacijo po uporabi varno uničite (z rezalnikom, s sežiganjem);
- kartice, ki niso več veljavne, uničite tako, da jih prerežete prek čipa in magnetne steze in delce odvrzite v ločene smeti;
- vključite storitev obveščanja o uporabi kartice prek sporočil SMS. To je še posebej primerno, ko potujete v države, kjer so zlorabe pogoste.

Spletna plačila in digitalne identitete

Poslovanje preko spletnih trgovin in drugih vrst spletnih mest, kjer uporabniki za plačilo uporabljajo plačilne kartice, pomeni nižje stroške za trgovce, hotelirje, izposojevalce vozil in podobno, za uporabnike pa večje udobje ter običajno tudi nižje cene. Vedno več je tudi spletnih plačilnih posrednikov in storitev za prenos denarja, kot je na primer PayPal, ter povezav plačilnih kartic z osebnimi računi oziroma spletnimi digitalnimi identitetami kot so Facebook, Apple ID, račun Google in podobno. Digitalne identitete in z njimi povezane plačilne kartice imajo mnogi, predvsem mlajši, ki jih zaradi vedno večje razširjenosti pametnih mobilnih telefonov in tablic večino časa nosijo s seboj, zato je potrebno te naprave pred zlorabo ustrezno zaščititi.

Varnost vseh naštetih je običajno dobra, a večinoma vseeno slabša od varnosti spletnih bank, zato na uporabnike preži kar nekaj pasti, še zlasti, če ne upoštevajo osnovnih varnostnih načel.

Addiko Bank

Nevarnosti za uporabnike

Lažno predstavljanje (angl. *Phishing*)

Pri lažnem predstavljanju kriminalci pošiljajo lažna e-poštna sporočila, ki na prvi pogled delujejo avtentična, v katerih vas pozivajo k obisku spletne strani neke banke ali plačilne ustanove, do katere je spletna povezava vključena v sporočilo. Spletna stran, na kateri naj bi obiskovalec potrdil oziroma obnovil svoje varnostne podatke, seveda ni prava, temveč je ponarejena, na prvi pogled pa lahko deluje pristno. Obiskovalec take spletne strani nepridipravom nevede dejansko sam posreduje podatke o plačilni kartici.

Zvabljanje (angl. *Pharming*)

Zvabljanje je delno podobno lažnemu predstavljanju, le da je še bolj zahrbtno, saj se napad običajno zgodi brez kakršnega koli vsaj približno sumljivega obvestila. Napadalci vaš računalnik s pomočjo sistemskih sprememb za razreševanje domenskih imen preusmerijo na lažno spletno stran, ki na prvi pogled deluje pristno, običajno so drugačni le identifikacijski elementi (spletni certifikat) oziroma tega sploh ni. Tudi obiskovalci takih spletnih strani nepridipravom nevede sami posredujejo podatke o plačilnih karticah, uporabniških imenih in geslih za spletne trgovalne račune (npr. PayPal).

Škodljiva programska koda (angl. *Malware*)

Kriminalci lahko s pomočjo škodljive programske kode, predvsem trojanskih konjev, orodij za prevzem skrbniškega dostopa in programov, ki snemajo vse vaše pritiske tipk (angl. *Keylogger*) na tipkovnici, brez vaše vednosti pridobijo vse podatke, ki jih potrebujejo za oddaljene nakupe.

Lažne spletne trgovine

S pomočjo lažnih spletnih trgovin, ki po sumljivo ugodnih cenah ponujajo različne mikavne artikle, do katerih obiskovalec običajno pride prek spletnih povezav v neželeni e-pošti, lahko kriminalci dobijo vse podatke za izvedbo oddaljenih nakupov.

Hekerski vdor v baze podatkov spletnih trgovcev

Zaradi poznanih prednosti je vedno več uporabnikov spletnih trgovin. Nekateri trgovci pa zaradi nepoučenosti in nestrokovnosti po nepotrebnem shranjujejo njihove podatke o plačilnih karticah in s tem stranke v veliki meri izpostavljajo nevarnosti tatvine identitete. Velikokrat se je že pripetilo in zagotovo se še bo, da hekerji uspejo pridobiti neupravičen dostop do baz podatkov kupcev in plačilnih kartic, ki jih prekopirajo in prodajo, ali pa kar sami zlorabijo.

Domače zlorabe

Mobilne naprave, na katerih so plačilne kartice povezane z digitalnimi identitetami ali jih uporabniki uporabljajo za dostop do računov spletnih plačilnih posrednikov in storitev za prenos denarja, predstavljajo grožnjo predvsem tistim, ki te mobilne naprave delijo z drugimi uporabniki. Običajno so to osebe iz družinskega kroga, ki imajo zaradi okoliščin nemoten dostop do mobilne naprave. Če imajo uporabniki varnostna gesla za dostop do računov spletnih plačilnih posrednikov shranjena v napravi oziroma jih drugi uporabniki poznajo ali jih lahko ugotovijo, jih lahko tudi zlorabijo ter s tem uporabniku povzročijo škodo oziroma sebi pridobijo tudi neposredno finančno korist.

Addiko Bank

Nasveti za zaščito pred zlorabami:

- zaupajte le tistim spletnim mestom in prodajalcem, ki od vas zahtevajo varnostno številko kartice, sicer nakupa ne opravite; po možnosti kupujte le pri preverjenih trgovcih;
- ne opravljajte nakupov prek spletnih mest, do katerih ste prišli prek spletnih povezav v neželeni elektronski pošti, ali pa so vas poklicali po telefonu in vam želeli prodati neko storitev ali blago in od vas želeli podatke s kartice. Po potrebi spletni naslov v brskalnik vpišite ročno;
- na način, ki je opisan v poglavju "Spletno in mobilno bančništvo", preverite pristnost spletnega mesta;
- v nobenem primeru nikoli ne vpisujte ali ne povejte številke PIN, saj pri oddaljenih nakupih ni potrebna;
- nikomur ne zaupajte varnostnih gesel za dostop do računov spletnih plačilnih posrednikov in storitev za prenos denarja ter izvedbo plačil preko digitalnih identitet. Gesla za te račune oziroma izvajanje plačil naj bodo drugačna od gesel, ki jih uporabljate sicer in ste jih komu že zaupali;
- natisnite spletno stran z oddanim naročilom in pogoji poslovanja in dostave ter s kontaktnimi podatki prodajalca. Prodajalca je dobro tudi preveriti, vsaj obstoj njegovega naslova in stacionarne telefonske številke;
- pri izbiri spletnega trgovca dajte prednost tistim, ki omogočajo uporabo varnostne storitve MasterCard SecureCode, saj so ti nakupi varnejši že samo zato, ker podatke o plačilni kartici pošljete neposredno banki in jih trgovec niti ne dobi. Spletna mesta, ki so vključena v storitev MasterCard SecureCode, so označena z logotipom:

MasterCard SecureCode

Storitev MasterCard SecureCode omogoča, da uporabnik vsak spletni nakup potrdi z enkratnim geslom, ki ga v obliki sporočila SMS prejme na mobilno telefonsko številko, ki jo je predhodno sporočil banki:

Za uporabo storitve MasterCard SecureCode, ki je za uporabnika brezplačna, se mora uporabnik registrirati. Za to poleg številke kartice potrebuje še davčno številko, datum rojstva in mobilno telefonsko številko. Ob registraciji uporabnik v spletno aplikacijo vnese davčno številko, medtem ko mobilno telefonsko številko, če je ta prikazana, zgolj potrdi in zatem na isto številko prejme potrditveno sporočilo SMS. Če številka ni prikazana, se mora uporabnik osebno oglasiti v eni izmed poslovalnic Addiko Bank d.d.

Addiko Bank

- Če oddaljene nakupe pogosto opravljate, je smiselno samo za te nakupe uporabljati drugo, predplačniško plačilno kartico MasterCard Addiko banke.

Spletno in mobilno bančništvo

Razvoj in dostopnost sodobnih informacijskih tehnologij mnogim omogočata poslovanje z banko z računalnikom ali mobilno napravo, ki je povezana v splet. Mobilna banka Addiko Mobile deluje kot komplement spletne banke Addiko EBank ter vključuje najpogosteje uporabljene funkcionalnosti spletne banke. Stranke lahko do mobilne banke Addiko Mobile dostopajo na 2 različna načina in sicer preko aplikacije na svojih pametnih mobilnih telefonih ali tabličnih računalnikih (na voljo za Android in iOS sisteme) oziroma preko brskalnika (**https://mobile.addiko.si**). Funkcionalnosti obeh verzij mobilne banke so identične z izjemo storitev, ki so vezane na opremo mobilnih telefonov oziroma tablic (npr. geolokacijske storitve, plačilo s slikanjem), zaradi česar jih različica preko brskalnika ne vključuje.

Vsega tega se zavedajo tudi kriminalci, ki poskušajo prek uporabnikov priti do tistih podatkov, ki bi jim omogočili tatvino oziroma prenos sredstev na druge račune. Pri tem so dokaj uspešni, tudi v Sloveniji. Napadi na spletno bančništvo, ki uporablja dinamična oziroma enkratna gesla, kot je v uporabi tudi v Addiko banki, so praviloma zelo težko izvedljivi, niso pa nemogoči, zato se tako bančništvo smatra za bolj varno. Uporabniki se še vedno premalo zavedamo, da moramo za svojo varnost najprej poskrbeti sami, seveda pa ob tem upoštevati tudi varnostna navodila, ki jih dobimo od banke.

Nevarnosti za uporabnike

Med največje nevarnosti za uporabnike spletnega bančništva in spletnih trgovalnih računov sodijo zgoraj predstavljeni lažno predstavljanje (angl. *Phishing*), zvabljanje (angl. *Pharming*) in škodljiva programska koda (angl. *Malware*), saj lahko napadalec z njihovo pomočjo pridobi vaša uporabniška imena in gesla. Spletno bančništvo, kjer uporabnik za prijavo uporablja enkratna gesla, je pred zlorabami veliko bolj varno, ne pa povsem, zato smo v Addiko banki za večjo varnost uvedli še dodatno potrditev nekaterih plačil in sprememb podatkov z dodatnim enkratnim varnostnim geslom, ki jih uporabniki prejmejo preko sporočil SMS na njihove mobilne telefone.

Addiko Bank

Nasveti za zaščito pred zlorabo:

- spletni naslov vaše banke vedno vnesite ročno, nikoli pa do spletne strani ne dostopajte prek spletne povezave v elektronskem sporočilu;
- vedno preverite digitalni certifikat spletne banke, kakor tudi mobilne banke, če jo obiščete z mobilnim brskalnikom. Nekateri spletni brskalniki ujemanje spletnega naslova z digitalnim certifikatom opravljajo že samodejno. Naši spletni banki Addiko EBank in Addiko Mobile uporabljata digitalni certifikat z razširjenim preverjanjem veljavnosti, kar uporabnik opazi tako, da se na začetku ali koncu naslovne vrstice v spletnem brskalniku naziv naše banke v zeleni barvi izpiše v celoti.
- pri preverjanju digitalnega certifikata bodite še zlasti pozorni na prstni odtis digitalnega certifikata (angl. *Thumbprint*), ki ima unikatno vrednost, ki je ni mogoče ponarediti. Vrednosti SHA1 in SHA-256 prstnega odtisa za digitalni certifikat za spletno stran **https://www.addiko.si/addiko-ebank** sta objavljeni na spletni povezavi https://www.addiko.si/addiko-ebank.
- vrednosti SHA1 in SHA-256 prstnega odtisa za digitalni certifikat za spletno stran **https://mobile.addiko.si** sta objavljeni na spletni povezavi https://www.addiko.si/addiko-mobile.
- preverjanje vrednosti prstnega odtisa je različno glede na brskalnik, ki ga uporabljate:
  Microsoft Internet Explorer:
  Kliknete na ključavnico oziroma tekst Addiko Bank d.d. [SI] ob naslovni vrstici. Odpre se pogovorno okno, v katerem kliknete "Ogled potrdil" in s tem odprete dodatno okno, v katerem izberete zavihek "Podrobnosti". Z drsnikom se premaknete do dna okna, kjer vidite rubriki: "Algoritem za razpoznavni odtis" z vrednostjo SHA1 in "Razpoznavni odtis", v katerem je vpisana zgornja vrednost.
  Google Chrome:
  Kliknete na ključavnico oziroma tekst Addiko Bank d.d. [SI] ob naslovni vrstici. Odpre se pogovorno okno, v katerem kliknete "Povezava" in nato "Informacije o potrdilu". S tem odprete dodatno okno, v katerem izberete zavihek Podrobnosti in se z drsnikom premaknete do dna okna, kjer vidite rubriki: "Algoritem za razpoznavni odtis" z vrednostjo SHA1 in "Razpoznavni odtis", v katerem je vpisana zgornja vrednost.
  Mozilla Firefox:
  Kliknete na ključavnico oziroma tekst Addiko Bank d.d. (SI) zraven naslovne vrstice in nato "Več Podatkov". Odpre se pogovorno okno, v katerem kliknete na "Preglej Certifikat" in s tem odprete dodatno okno, kjer v spodnjem delu okna vidite vrednosti obeh prstnih odtisov;

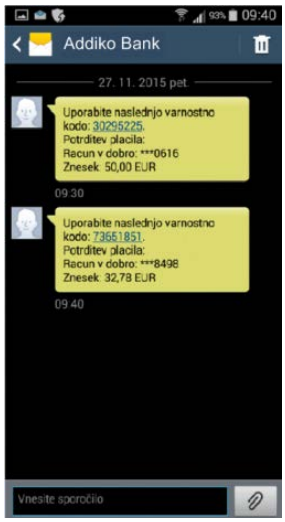
- v primeru, da se med obiskom spletne banke pričnejo odpirati pojavna okna, ki jih prej niste nikoli opazili, se nemudoma odjavite iz spletne banke in o tem obvestite banko, v pojavna okna pa ne vnašajte svojih podatkov ali podatkov o plačilnih karticah, uporabniških imen ali gesel;
- Addiko banka nikoli ne pošilja e-poštnih ali sporočil SMS s spletnimi povezavami na prijavno stran Addiko EBank ali Addiko Mobile. Prosimo vas, da o prejemu takega sporočila nemudoma obvestite banko na e-poštni naslov varnost.si@addiko.com;
- banka od vas preko e-pošte nikoli ne bo zahtevala osebnih podatkov, podatkov o vaših uporabniških imenih, geslih ali plačilnih karticah, saj z njimi že razpolaga. Prosimo vas, da tudi o prejemu takega sporočila nemudoma obvestite banko na e-poštni naslov varnost.si@addiko.com;
- nastavite oziroma aktivirajte in uporabljajte vse zaščitne funkcionalnosti, ki jih omogoča ponudnik elektronskega bančništva (npr. uporabo dodatnih gesel za potrjevanje nakupov, obvestilo o vstopu v spletno bančništvo po e-pošti ali SMS);

- pazite, da ne postanete denarna mula - ne nasedajte ponudbam s hitrim zaslužkom s provizijo, ki naj bi jo dobili, če boste gotovino, ki naj bi jo prejeli na vaš račun z nekega tretjega računa, posredovali v tujino. Ta denar običajno izvira iz zlorabljenih e-bančnih računov.

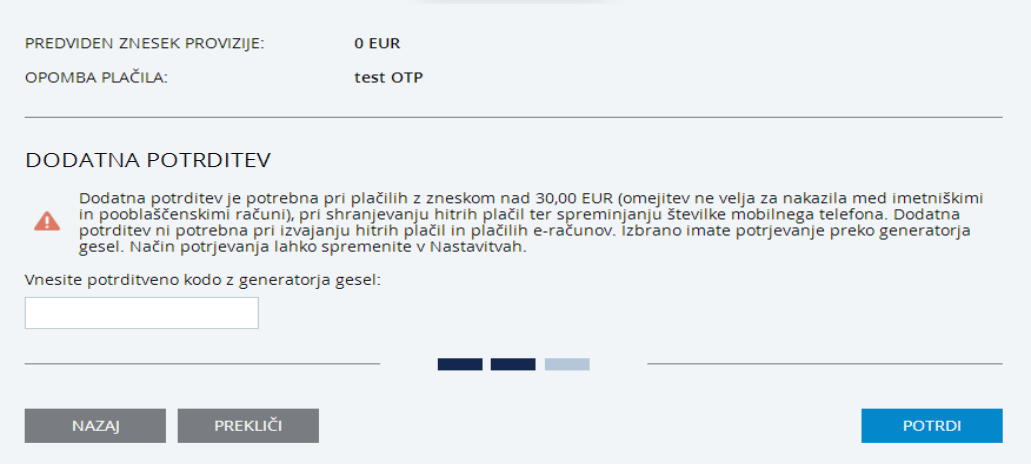
Postopek potrjevanja transakcij

Pri plačilih in naročilih, kjer je potrebno dodatno potrjevanje z varnostno kodo, se po kliku gumba »Naprej« na prvem koraku plačila oziroma naročila prikaže pojavno okno z naslovom »Dodatna potrditev«. Način potrjevanja je mogoče spremeniti na strani »Nastavitve«.

Če uporabnik v »Nastavitvah« izbere možnost potrjevanja s SMS sporočilom na številko mobilnega telefona, bo na svoj mobilni telefon prejel SMS sporočilo s potrditveno kodo, ki jo bo vpisal v za to predvideno polje na vnosni maski Addiko EBanka v naslednjem koraku ter s tem plačilo/naročilo tudi formalno potrdil.



Če uporabnik v »Nastavitvah« izbere možnost potrjevanja z geslom generatorja gesel, mora kodo generirati prek generatorja gesel in jo nato vpisati v za to predvideno polje na vnosni maski Addiko EBanka ter s tem plačilo/naročilo tudi formalno potrditi.



Addiko Bank

Splošni napotki za varnejše elektronsko poslovanje z računalniki in mobilnimi napravami:

Za varne spletne nakupe in elektronsko bančništvo je potrebno upoštevati osnovna pravila varne uporabe interneta:

- nakupujte le na spletnih straneh, ki omogočajo varno (https) povezavo, prav tako pa vedno preverite digitalni certifikat spletnih strani (kdo ga je izdal, komu ga je izdal, njegovo veljavnost). To preverite s klikom na ključavnico, ki se pojavi ob naslovni vrstici;
- takoj izbrišite elektronsko pošto, v kateri pošiljatelj sprašuje po uporabniških imenih, geslih, številkah kartic in drugih občutljivih podatkih ter pogosto vsebuje povezavo na neko spletno mesto, katerega prikazani naslov je enak ali podoben kot naslov Addiko EBank ali Addiko Mobile;
- redno nameščajte varnostne popravke za operacijski sistem in ostalo programsko opremo;
- ne nameščajte datotek, katerih izvora in namena delovanja ne poznate oziroma izvirajo iz neuradnih virov;
- na računalnikih nastavite in za vsakodnevno delo uporabljajte omejen uporabniški profil, ki onemogoča nameščanje programske opreme in spremembe sistemskih nastavitev računalnika;
- uporabo računalnika, pametnega telefona ali tablice omogočite samo osebam, ki jim dejansko zaupate;
- uporabljajte lokalni požarni zid, ki ga je potrebno redno posodabljati;
- uporabljajte programsko opremo za zaščito pred internetnimi nevarnostmi in jo redno posodabljajte;
- preverite in prilagodite varnostne nastavitve vašega brskalnika tako, da ta ne bo hranil vaših uporabniških imen in gesel, kot tudi ne vsebine šifriranih povezav;
- varnost lahko povečate tudi z uporabo navideznih računalnikov, ki so namenjeni samo spletnim nakupom in spletnemu bančništvu;
- po končanemu spletnem nakupu in bančništvu se vedno odjavite iz spletne trgovine/banke in zaprite zavihek v brskalniku, prav tako pa po potrebi ponovno zaženite spletni brskalnik;
- pametno kartico ali ključ USB z nameščenim kvalificiranim digitalnim potrdilom po uporabi vedno takoj odstranite iz čitalca ali računalnika;
- ne uporabljajte istih uporabniških imen in gesel (za operacijski sistem, za spletne trgovine in banke), prav tako pa geslo redno spreminjajte, razen seveda, če storitev omogoča uporabo enkratnih gesel, kot to omogočata spletna banka Addiko EBank in mobilna banka Addiko Mobile;
- mobilne naprave pred neupravičeno uporabo zaščitite najmanj z zaklepanjem zaslona z vzorcem ali številko PIN, ki je drugačna od številke PIN za Addiko Mobile;
- po izhodu iz Addiko EBank ali Addiko Mobile se program oziroma brskalnik v ozadju še naprej izvajata. Z vgrajenimi menijskimi ukazi ustavite program ali storitev po navodilih proizvajalca (postopek je različen v odvisnosti od operacijskega sistema in uporabljene naprave). Le tako se bodo iz delovnega pomnilnika računalnika ali mobilne naprave v celoti izbrisali zasebni podatki.

Addiko Bank

Bankomati in terminali POS

Nevarnosti za uporabnike so:

Snemanje magnetnega zapisa (angl. *skimming*):
Snemanje magnetnega zapisa se najpogosteje dogaja na bankomatih, redkeje na terminalih POS, lahko pa tudi samopostrežnih kioskih, kot so npr. na bencinskih črpalkah. S primernim čitalnikom magnetnih kartic lahko to izvedejo tudi vsi, ki imajo vašo kartico ob plačilu blaga ali storitev v rokah. Za zlorabo kartice potrebujejo poleg magnetnega zapisa največkrat še varnostno in/ali številko PIN, kar jim omogoča tudi izdelavo ponarejene plačilne kartice. Varnostno številko s kartice enostavno prepišejo, medtem ko številko PIN pridobijo na več načinov. Največkrat tako, da vas opazujejo med vpisovanjem številke, ali s pomočjo pripomočkov, ki jih namestijo na bankomat (video kamera, lažna tipkovnica). Kopiranje podatkov s čipa na bankomatih in terminalih POS, ki so skladni z EMV standardom, ni mogoče, medtem ko je snemanje magnetnega zapisa možno vedno, ne glede na vrsto kartice. Sodobnejši bankomati in terminali POS namreč onemogočajo dodajanje naprav za snemanje magnetnega zapisa, oziroma na prisotnost take naprave opozorijo oskrbnika.

Libanonska zanka
Libanonska zanka je posebna naprava, ki se vstavi v režo bankomata in onemogoči izmet plačilne kartice uporabniku. Uporabniki ne morete do svoje kartice, kriminalec, ki se nahaja v bližini bankomata, pa vam ponudi pomoč, seveda s ciljem, da izve številko PIN. Ko po neuspelih poskusih, da bi prišli do kartice, odidete, jo zlikovec izvleče in s pomočjo pridobljene številke PIN tudi enostavno zlorabi. Sodobnejši bankomati tovrstne naprave praviloma zaznajo.

Past za gotovino (angl. *Cash Trapping*)
Past za gotovino je način zlorabe, pri katerem kriminalci na odprtino za izdajanje gotovine namestijo dodatno, običajno lepljivo, letev, ki prepreči izdajo gotovine in povzroči zagozditev gotovine v reži. V ozadju celotni postopek sicer poteka nemoteno in bankomat tudi pozove uporabnika, naj vzame gotovino, vendar pa to zaradi ovire pred režo ni mogoče. Uporabniki običajno sumijo na tehnično napako na bankomatu in ne preverijo vzroka ter odidejo. Storilci zatem past z bankomata odstranijo in si denar nezakonito prilastijo.

Izguba in tatvina plačilne kartice
Vsakodnevno se dogajajo tako tatvine kot tudi izgube plačilnih kartic, ki jih je možno do preklica zlahka zlorabiti za oddaljene nakupe. Če pa je kartici priložena še številka PIN, pa so možnosti zlorabe kartice seveda še mnogo širše.

Podatki o plačilnih karticah na potrdilih o nakupu
Kljub strogim zahtevam varnostnih standardov se podatki o številki kartice, njeni veljavnosti in celo imetniku kartice še vedno občasno pojavljajo na potrdilih o nakupu, še zlasti v nerazvitem svetu. Tudi te podatke je mogoče zlorabiti za oddaljene nakupe, saj povsod ne zahtevajo tudi podatka o varnostni številki.

Dvakratno odčitavanje plačilnih kartic
Nekateri trgovci zaradi zahtev blagajniškega poslovanja podatke s plačilne kartice odčitajo dvakrat: na terminalu POS, kjer odčitajo podatke z magnetne steze ali čipa, in na lastnem bralniku, ki

(nekatere) podatke z magnetnega zapisa prenese v računalniški program blagajne. Tu so podatki izpostavljeni varnostnemu tveganju, saj jih lahko zaposleni, hekerji in drugi zlorabijo za oddaljene nakupe na tistih prodajnih mestih, kjer ne zahtevajo varnostne številke.

Lažni prodajalci blaga po telefonu
Nič vas ne bi smel presenetiti telefonski klic lažnivega neznanca, ki naj bi opravljal neposredno trženje prek telefona, saj nepridipravi tudi na tak način poskušajo priti do podatkov, ki jim omogočajo oddaljene nakupe. Za take napade so ranljive tako magnetne kot čipne plačilne kartice, vendar za slednje obstajajo dodatne zaščite, ki take napade preprečijo.

Kako se zaščititi pred zlorabo?
- Pri vnosu številke PIN stopite bližje k napravi in številčnico prekrijte s prosto roko ali pa se nadnjo nagnite s telesom;
- številke PIN nikoli nikamor ne zapišite in je v nobenem primeru nikomur ne povejte (niti policiji, niti bančnim uslužbencem);
- ob prejemu nove številke PIN to spremenite, če vam kombinacija številk ne ustreza (možno samo na Maestro BA karticah);
- če na bankomatu ali terminalu POS opazite karkoli nenavadnega (poškodbe, dodatke), prekinite transakcijo in o tem obvestite prodajalca, banko ali policijo;
- pri uporabi brezstične kartice bodite pozorni na to, da k terminalu POS ne prislanjate denarnice, če imate v njej več brezstičnih kartic, temveč iz denarnice izvlecite tisto kartico, s katero želite plačati;
- ob nakupih manjvrednih stvari od uličnih ali naključnih prodajalcev, ki bi vam ponujali možnost nakupa z brezstično kartico, se odločite za nakup z gotovino;
- pri uporabi plačilne kartice nikoli ne sprejemajte pomoči neznancev;
- po opravljeni transakciji denar, potrdilo in kartico pospravite takoj, šele nato odidite;
- ko bankomat iz neznanega razloga zadrži kartico ali ne izplača denarja, o tem takoj obvestite Bankart d.o.o., Ljubljana (+386 (0)1 583 41 83), banko (+386 (0)1 580 40 00), lahko pa tudi policijo (v Sloveniji je telefonska številka 113);
- ne dovolite, da bi trgovec kartico preko terminala ali celo tipkovnice potegnil več kot enkrat, oziroma za vsak neuspešen poskus zahtevajte potrdilo o neuspeli transakciji.

Kako ukrepati, če ste žrtev zlorabe

Predstavljene zlorabe plačilnih kartic oziroma občutljivih (tudi osebnih) podatkov se med seboj očitno razlikujejo. Zato so napotki za ukrepanje, ko postanete žrtev zlorabe, razdeljeni na tri sklope: splošni napotki, ki veljajo v vseh primerih zlorab, napotki, ki veljajo v primeru, ko je bila zloraba izvedena na "klasičnem" prodajnem mestu (npr. v trgovini, v gostinskem obratu) in napotki, ki veljajo pri zlorabah preko interneta.

Splošni napotki za ukrepanje:
- o ugotovljeni zlorabi takoj obvestite banko, še zlasti takrat, ko je zloraba posledica nekega predhodnega kaznivega dejanja;
- z banko sodelujte pri razjasnitvi okoliščin zlorabe, saj bo le skupen napor dosegel želene rezultate. Vsako zlorabo plačilne kartice ali spletne banke morate prijaviti policiji;

- zabeležite si vse postopke obveščanja in prijav, saj vam to lahko pomaga pri povrnitvi nastale škode;
- banki napišite pooblastilo, da dovoljujete posredovanje podatkov policiji, sicer bo morala policija pridobiti odredbo sodišča, kar pa običajno traja dlje časa in je za uspešnost preiskave lahko usodno;
- za lažjo povrnitev odtujenih sredstev bo včasih pomagal tudi verodostojen alibi, s katerim boste dokazali, da sporne transakcije niste naredili sami, temveč ste bili v kritičnem času v službi, ste govorili po telefonu daleč stran in podobno. Te podatke boste morali priskrbeti sami.

Ukrepanje ob zlorabi, ki je bila povzročena na "klasičnem" prodajnem mestu:

- takoj prekličite veljavnost zlorabljene plačilne kartice;
- od banke čim prej pridobite vse podatke o spornih transakcijah (kdaj in kje so se zgodile) in jih izročite policiji oziroma za to pooblastite banko, da bo lahko policija hitro nadaljevala s preiskovanjem, saj je hitrost bistvenega pomena;
- poskusite sami ugotoviti morebitne nenavadne situacije, kjer bi pri uporabi plačilne kartice lahko prišlo do odtujitve podatkov ali celo kartice.

Ukrepanje ob zlorabi, ki je bila povzročena preko interneta:

- takoj prekličite veljavnost zlorabljene plačilne kartice, uporabniškega imena ali digitalnega certifikata za spletno banko ter za čas do razjasnitve okoliščin onemogočite uporabo vašega spletnega bančništva oziroma spletnih trgovalnih računov (npr. PayPal);
- od banke čim prej pridobite vse dnevniške datoteke o spornih transakcijah (kdaj so se zgodile, naslov IP napadalčevega računalnika) in jih izročite policiji oziroma za to pooblastite banko, da bo lahko policija hitro nadaljevala s preiskovanjem, saj je hitrost bistvenega pomena;
- v primeru, ko pride do zlorabe spletne banke, napadalci podatke najpogosteje pridobijo z oškodovančevega računalnika, to pa je možno tudi pri zlorabi plačilne kartice, zato takrat, ko je to nujno potrebno, omogočite forenzični pregled računalnika in sodelujte pri njem, da se ugotovi okoliščine zlorabe in odkrije storilca;
- poskusite sami ugotoviti morebitne nenavadne situacije, kjer bi pri uporabi interneta lahko prišlo do odtujitve podatkov ali celo kartice. Ugotovitve posredujte banki skupaj z morebitnimi pojasnili.

Pomen kratic:

1. PIN (angl. *Personal Identification Number*): osebno geslo
2. PAN (angl. *Primary Account Number*): številka kartice
3. CSC (angl. *Card Security Code*): trimestna varnostna številka, vtisnjena na hrbtni strani plačilne kartice
4. CVC2 (angl. *Card Verification Code*): trimestna varnostna številka, vtisnjena na hrbtni strani plačilne kartice
5. Terminal POS (angl. *Point of Sale*): je naprava, ki omogoča plačevanje s plačilnimi karticami in običajno delujejo kot razširitev osnovne blagajne ali kot nadomestek plačilnega sistema
6. EMV: standard čipne tehnologije uporabljene pri plačilnih karticah