Addiko Bank

Priporočila za varno internetno poslovanje

Addiko Bank d.d.

Addiko Bank

Priporočila za varno internetno poslovanje

Brezgotovinsko poslovanje je postalo sestavni del našega vsakdana in večina med nami si ne predstavlja več življenja brez plačilnih kartic ter nakupov preko spleta ter brez uporabe spletnega in mobilnega bančništva. Z vedno bolj razširjeno uporabo pametnih mobilnih telefonov in tablic so internet in digitalni kanali uporabnikom bolj dostopni, hkrati pa se povečuje tudi število zlorab pri poslovanju in komunikacijo preko digitalnih kanalov. Udobje brezgotovinskega poslovanja nam namreč lahko hitro da občutek lažne varnosti, kar zlonamerneži s pridom izkoriščajo. Za nekatere vrste zlorab se je uveljavilo poimenovanje "tatvina identitete", kjer se zlonamerneži izdajajo za drugo osebo, ki je na primer legitimni uporabnik plačilnega sredstva in se poizkusijo neupravičeno okoristiti. Tovrstna zloraba se lahko zgodi vsakemu od nas.

Radi bi vas opozorili na največje nevarnosti pri brezgotovinskem in spletnem poslovanju, hkrati pa podali napotke, kako se lahko pred njimi najučinkoviteje zavarujemo. Osredotočili smo se na največkrat uporabljane načine brezgotovinskega poslovanja, in sicer plačilne kartice, internetna plačila in plačila v okviru spletne in mobilne 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) in Safe.si (https://safe.si/), redno spremljate novice in napotke o varnosti.

Za informacije ali vprašanja iz področja varnosti poslovanja s plačilnimi karticami, spletnim ali mobilnim bančništvom nas lahko pokličete na telefonsko številko 01 580 40 00, ali nam pišete na e-poštni naslov varnost.si@addiko.com ali pošljete običajno pošto na naslov Addiko Bank d.d., Dunajska cesta 117, 1000 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 ali m-bančništva pa na +386 (0)1 580 43 00 (pomoč uporabnikom Addiko EBank in Addiko Mobile).

Najpogostejši načini zlorab

Najpogostejša načina zlorabe podatkov plačilnih kartic sta prestrezanje kartičnih podatkov s pomočjo lažnega predstavljanja ali ribarjenja (angl. *phishinga*). Zlonamerneži s pomočjo lažnih nagradnih iger in ugodnosti prejemnike vabijo k razkritju podatkov o plačilnih in kreditnih karticah. Ribarjenje izvajajo s komunikacijo preko sodobnih digitalnih kanalov, kot so elektronska pošta, socialna omrežja, spletne klepetalnice in tudi sporočil SMS. Prejemniki so napoteni na zlonamerne spletne vsebine, ki posnemajo znane legitimne spletne strani in kjer z navideznimi ugodnostmi obiskovalca prepričujejo k vnosu kartičnih podatkov. Na podlagi prejetih podatkov zlonamerneži bodisi v ozadju opravijo nakup težje izsledljive storitve, prodajo lažno blago ali storitev, ali pa podatke prodajajo naprej in posledice lahko nastopijo čez čas. Pridobljeni podatki na zalogo tako služijo zlonamerni uporabi plačilnih kartic, s katerimi se poizkuša izvesti zlorabe z uporabo na prodajnih mestih, kjer včasih zaradi neustreznih varnostnih zaščit niti ni potreben vnos varnostne kode za oddaljene nakupe.

Pri zlorabah v okviru spletnega bančništva so najpogostejši načini zlorabe prenakazovanje denarnih sredstev sumljivega izvora na račune zlonamernežev preko računov prenašalcev, ki so lahko fizične ali pravne osebe, imenovane tudi denarne mule. Te največkrat lahkomiselno računajo na hiter zaslužek s provizijo za prenakazilo, in prenos sredstev v tujino s pomočjo različnih storitev (npr. Western Union), kjer jih zlonamerneži z zvijačo dvignejo v banki posrednici, nato pa se za denarjem izgubi vsaka sled.

Sledijo zlorabe povezane s plačili navideznih stroškov za fiktivne kredite, zapuščinske postopke, ljubezenske prevare, stroške nakupov preko spleta mimo uradih trgovskih in turističnih platform ter špekulativne naložbe z visokimi obljubljenimi donosi, pri čemer so najpogosteje žrtve fizične osebe. Pri pravnih osebah najpogosteje zaznavamo prevare v obliki nakazil zaposlenih na račune zlonamernežev, ki se izdajajo za vidne oziroma vodilne predstavnike podjetja, ali pa ponaredijo račune oškodovanemu podjetju znanih dobaviteljev ali izvajalcev, pri čemer navedejo transakcije račune, do katerih imajo dostop zlonamerneži.

Zlonamerneži lahko v svojih poizkusih izvedbe prevar pridobijo širok nabor osebnih in plačilnih podatkov, namenjenih nadaljnjim zlorabam. Sem štejemo podatke o plačilnih in kreditnih karticah, prestrezanje podatkov in verifikacijskih elementov potrebnih za izvedbo transakcij (npr. pri spletni banki), ter osebnih podatkov, kot so davčna številka ali EMŠO, datum rojstva, prebivališče in podobno. Z zbranimi podatki se lahko zlonamerneži zlahka izdajajo za drugo osebo. Tatvina identitete je lahko za lastnika zlorabljenih podatkov hud finančni udarec, saj zlikovcu lahko omogoči zlorabo plačilne kartice, sklepanje kreditnih pogodb, uporabo spletne banke in drugo.

V nadaljevanju na kratko navajamo najpogostejše nevarnosti, ki so izhodišče opisanih zlorab. Svetujemo, da razmislite, ali nevarnosti znate prepoznati oziroma se o njih in njihovi zaznavi dodatno poučite na strokovnih spletnih straneh (slovenske smo navedli v uvodu) ter redno spremljajte to tematiko.

Nevarnosti za uporabnike

Lažno predstavljanje ali ribarjenje (angl. *Phishing*)
Pri lažnem predstavljanju zlonamerneži pošiljajo lažna e-poštna sporočila tako preko elektronske pošte, kot drugih spletnih storitev, klepetalnic in tudi sporočil SMS . Sporočila na prvi pogled delujejo avtentična in vas želijo prepričati k uporabi spletne povezave, vključene v sporočilu. Ta vodi do lažne spletne strani banke, plačilne ustanove ali znanega ponudnika storitev. Spletna stran, na kateri naj bi obiskovalec potrdil oziroma obnovil svoje varnostne podatke, ali pa opravil plačilo za na videz zanj ugodno storitev, je seveda ponarejena in ni prava, , a na prvi pogled lahko deluje pristno. Obiskovalec take spletne strani nepridipravom nevede dejansko sam posreduje podatke o plačilni kartici ali druge podatke, ki bi nepridipravom lahko omogočili izvedbo zlonamernih transakcij .

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 okužijo z zlonamerno kodo, ki vas samodejno preusmeri 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*)
Zlonamerneži lahko s pomočjo škodljive programske kode, predvsem trojanskih konjev, orodij za prevzem skrbniškega dostopa in programov, ki snemajo uporabnikove pritiske tipk (angl. *Keylogger*) na tipkovnici brez njegove vednosti, ter tako pridobijo vse podatke, ki jih potrebujejo za oddaljene nakupe. S škodljivo programsko kodo naprave najpogosteje okužimo z nameščanjem nelegalne programske opreme, snemanjem programske opreme in vsebine iz sumljivih spletnih strani ter preko okuženih priponk v elektronski pošti. O varnosti priponk oziroma prenesenih datotek in programov se lahko brezplačno prepričamo s spletnimi pregledovalniki sumljivih datotek, kot je storitev Virustotal (https://www.virustotal.com/), ki s pomočjo priznanih orodij pregleda datoteke ali programe, ki jih ocenimo kot sumljive.

Lažne spletne trgovine
S pomočjo lažnih spletnih trgovin, ki po sumljivo ugodnih cenah ponujajo različne privlačne izdelke, do katerih obiskovalec običajno pride prek spletnih povezav v neželeni e-pošti, lahko zlonamerneži dobijo vse podatke za izvedbo oddaljenih nakupov. Ob super ponudbah na nam nepoznaih in nepreverjenih spletnih straneh, je priporočljivo preveriti njihovo legitimnost, še posebej če so cene bistveno nižje, kot pri večini drugih, širše znanih trgovcih. Pri preverjanju legitimnosti spletnih trgovin priporočamo uporabo storitev, ki so namenjene recenziji spletnih trgovcev in spletnih strani, kot sta na primer Trustpilot (https://www.trustpilot.com/), ki nudi uporabniške ocene in opise spletnih ponudnikov, ter Sucuri (https://sucuri.net/), ki naredi varnostni pregled spletne strani. Obe storitvi sta v angleškem jeziku.

Hekerski vdor v baze podatkov spletnih trgovcev
Zaradi poznanih prednosti je vedno več uporabnikov spletnih trgovin. Nekateri trgovci zaradi nepoučenosti in nestrokovnosti po nepotrebnem shranjujejo podatke strank 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.

Nigerijske in loterijske prevare
Scenarijev je več, na primer zadetek na loteriji, odkrili so skrite račune na bankah, prejemnik je dedič ogromnega premoženja, a osnovni mehanizem goljufije ostaja enak - zlonamerneži želijo prejemniku sporočila nakazati večjo vsoto denarja. Z zelo privlačno ponudbo goljufi vzpostavijo komunikacijo (to je lahko preko elektronske pošte, spletnih oglasnikov, Facebooka itd.), nato avtor prevare sporoči, da je potrebno zaradi tega ali onega postopka v naprej poravnati minimalno vsoto, čemur kmalu sledijo pozivi po poravnavi dodatnih stroškov, kot na primer strošek odprtja novega računa, plačilo davkov, stroški vodenja računa, stroški odvetnika itd. Ko uporabnik preneha s plačevanjem (izmišljenih) stroškov in zahteva obljubljeno nagrado, se komunikacija prekine.

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.

Direktorske prevare
Zlonamerneži prek lažnih elektronskih naslovov, ki so na videz podobni naslovom vodilnih v podjetju, kontaktirajo pooblaščene osebe za izvajanje plačil v podjetju, z namenom, da jih zavedejo, da gre za legitimno zahtevo vodstva in ti izvršijo plačila na lažne bančne račune.

Vsiljevanje v poslovno komunikacijo
Zlonamerneži vdirajo v e-poštne sisteme podjetij, od koder lahko spremljajo njihovo elektronsko komunikacijo s strankami. Ko pridobijo dovolj pomembnih informacij o poslovnih procesih, lahko v ključnem trenutku aktivno posežejo v komunikacijo in kupcu pošljejo lažno sporočilo o spremembi transakcijskega računa. Tako preusmerijo plačevanje računov in drugih stroškov na svoje lažne bančne račune.

Addiko Bank

Pomembni kartični podatki in verifikacijski elementi

Med najpomembnejšimi podatki na plačilni kartici so podatki o uporabniku, številka kartice oziroma PAN (angl. *Primary Account Number*) in veljavnost kartice, ki so odtisnjeni na sprednji strani kartice. Na večini plačilnih kartic je na hrbtni strani kartice vtisnjena varnostna številka kartice, ki se uporablja pri oddaljenih nakupih. Na debetnih in kreditnih karticah Mastercard Addiko banke je ta zapisana v obliki 3-mestnega števila, ki se imenuje CVC oziroma CVC2 (angl. *Card Verification Code*). Izdajatelji plačilnih kartic varnostno številko (angl. *Card Security Code – CSC*) za oddaljene nakupe poimenujejo različno: CVC, CVC2, CVV, CVV2, CAV, CVD, CID itd, kar naj vas ne zmoti, saj gre za isto stvar.

Brezstične čipne kartice, ki jih izdaja Addiko banka, so pri uporabi na terminalih POS ali bankomatih od magnetnih varnejše le v primeru, da so te naprave skladne s standardom EMV, saj uporaba brezstične funkcionalnosti oziroma 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.

Vse plačilne kartice, ki jih izdajamo v Addiko banki, imajo vgrajeno najsodobnejšo tehnologijo za brezstično poslovanje, ki je enako varna kot čipna tehnologija. Te kartice imajo natisnjen znak:

Prodajna mesta in bankomati, kjer je možno brezstično poslovanje, so označena z znakom:

Brezstično poslovanje pomeni, da sta tako terminal POS oziroma bankomat kot tudi kartica opremljena s tehnologijo za brezstično poslovanje.

Pri brezstičnem plačevanju na terminalih POS, se PIN uporablja le za nakupe, vredne več kot 25 evrov (velja za Slovenijo; v drugih državah so lahko omejitve drugačne). Za nakupe nižjih vrednosti pa je dovolj, da kartico k terminalu le prislonite.
Pri brezstičnem dvigu gotovine na bankomatih, je PIN potrebno vnesti ob vsakem dvigu gotovine ali ob izvedbi katere druge transakcije, ki jo bankomat omogoča (kot na primer vpogled v stanje, zamenjava PIN-a, ipd).

Dodatna varnost pri zaporednih brezstičnih transakcijah brez vnosa PIN-a
Po več zaporednih brezstičnih transakcijah brez vnosa PIN-a s skupnim zneskom nad 50 EUR je potrebno izvesti transakcijo z vnosom PIN-a.

Plačevanje z brezstično kartico Mastercard je enako varno, kot plačevanje z običajno, to je stično, 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 mora biti kartica zelo blizu, največ nekaj centimetrov oddaljena od terminala POS oziroma bankomata z zgornjim simbolom;
- na brezstičnem čipu ni vašega imena, naslova in varnostnega števila CVC2, temveč zgolj številka kartice in datum veljavnosti, ob vsakem plačilu oziroma dvigu gotovine 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 oziroma bankomata dotaknili večkrat, bo obračunan zgolj en nakup oziroma plačilo oziroma dvig gotovine.

Splošni napotki za povečanje varnosti pri uporabi plačilnih in kreditnih kartic

- novo kartico takoj podpišite;
- v mobilni telefon si shranite telefonsko številko klicnega centra za pomoč uporabnikom in preklic plačilnih kartic (+386 (0)1 583 41 83, Bankart, d.o.o.);
- pri plačilih oziroma dvigih gotovine imejte plačilno kartico vedno pri sebi, ne izročajte je nikomur, temveč jo sami prislonite na terminal POS oziroma bankomat ali vstavite v terminal POS oziroma bankomat ali jo potegnite prek čitalnika magnetnega zapisa na terminalu POS;
- PIN kode ne delite z nikomer in je nikoli ne razkrivajte;
- ne omogočajte dostopa do verifikacijskih elementov za spletna kartična plačila in povezanih verifikacijskih (avtentikacijskih in avtorizacijskih) podatkov ne posredujte nikomur, uporabljate (vnašajte) jih le pri spletnih trgovcih, ki omogočajo storitve Mastercard SecureCode ali Mastercard Identity Check (storitev je podrobneje opisana v poglavju Nasveti za zaščito pred zlorabami);
- redno pregledujte bančne izpiske in preverite zabeležene transakcije, o morebitnih nepravilnostih pa takoj obvestite Addiko banko;
- plačilne kartice, bančne izpiske in drugo občutljivo dokumentacijo po uporabi varno uničite (z rezalnikom, s sežiganjem);
- plačilne kartice, ki niso več veljavne, uničite tako, da jih prerežete prek čipa in magnetne steze in delce odvrzite v ločene smeti in
- vključite storitev obveščanja o uporabi kartice prek sporočil SMS, to je še posebej primerno, ko potujete v države, kjer so zlorabe pogoste.

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 kupujete 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 ‖ mastercard ID Check

- plačilne kartice, ki jih izdaja Addiko banka, za uporabo storitve Mastercard SecureCode ali Mastercard Identity Check ni potrebno predhodno registrirati;
- če oddaljene nakupe pogosto opravljate, je smiselno samo za te nakupe uporabljati drugo, predplačniško plačilno kartico Mastercard Addiko banke.

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, Apple Pay ter povezav plačilnih kartic z osebnimi računi oziroma spletnimi digitalnimi identitetami kot so Facebook, Apple ID, Google račun, slovenska rešitev Rekono račun in drugi. 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, kot je npr. vklop dvo-faktorske verifikacije, pri čemer velja poudariti, da jo vse prej navedene storitve omogočajo.

Spletno in mobilno bančništvo

Razvoj in dostopnost sodobnih informacijskih tehnologij mnogim omogočata poslovanje z banko z računalnikom ali mobilno napravo, ki je povezana v internet. Mobilna banka Addiko Mobile deluje kot komplement spletne banke za fizične osebe, Addiko EBank, ter vključuje najpogosteje uporabljene funkcionalnosti spletne banke. Dodatno je na voljo mobilna aplikacija Flik Pay, preko katere lahko uporabnik izvaja takojšnja (instantna) plačila z drugimi fizičnimi osebami, ki imajo transakcijski račun pri kateri od slovenskih bank, ki sodelujejo v slovenski shemi za takojšnja plačila Flik. Mobilni aplikaciji sta dostopni za naprave Android in iOS. Funkcionalnosti na obeh operacijskih sistemih 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 zlonamerneži, 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 in preventivni ukrepi

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 in elektronska banka za pravne osebe imajo vpeljane varne prijavne verifikacijske elemente na ločenih kanalih:

- spletna banka za fizične osebe Addiko EBank: uporabniško ime in enkratno geslo z uporabo programskega ali strojnega generatorja v kombinaciji z vnosom PIN, pri čemer je programski generator del mobilne banke za fizične osebe;
- spletna banka za pravne osebe Addiko Business EBank: uporaba elektronske identitete z uporabo računa Rekono;
- elektronska banka za pravne osebe Halcom Addiko Business EBank: PIN in kvalificirano digitalno potrdilo na pametni kartici oziroma USB ključu.

Uporaba spletnega bančništva je z opisanimi načini prijave varna. Dodatni verifikacijski element pri potrditvi plačil je uporaba dinamične kode, ki je izračunana iz plačilnih podatkov in plačniku s povratnim sporočilom omogoča pregled prejetih plačilnih podatkov v zalednih sistemih banke pred potrditvijo plačila. Kakršnakoli sprememba plačilnih podatkov s strani napadalcev naredi kodo neveljavno oziroma spremembo opazi tudi uporabnik sam pred končno potrditvijo plačila. Uporabnik dinamično kodo prejme v obliki:

- spletna banka za fizične osebe Addiko EBank: enkratna geslo v obliki sporočila SMS oziroma potisnega sporočila v mobilni banki za fizične osebe;
  Iz potrjevanja z dinamično kodo so izvzeta nakazila med lastnimi in pooblaščenim računi ter plačila e-računov in predloge, ki jih je uporabnik kreiral z uporabo prijavnih verifikacijskih elementov.
- spletna banka za pravne osebe Addiko Business EBank: potisno sporočilo v mobilno aplikacijo OnePass;
- elektronska banka za pravne osebe Halcom Addiko Business EBank: dinamična koda se zagotavlja v okviru podpisa z digitalnim kvalificiranim potrdilom.

Mobilna banka za fizične osebe, Addiko Mobile, za prijavo uporablja PIN, ki ga uporabnik nastavi ob registraciji oziroma uporabnikove biometrične podatke, kjer je to omogočeno.
Dodatni verifikacijski element pri potrditvi plačil je uporaba dinamične kode, ki je izračunana iz plačilnih podatkov in plačniku omogoča pregled prejetih plačilnih podatkov v zalednih sistemih banke pred potrditvijo plačila. Kakršnakoli sprememba plačilnih podatkov s strani napadalcev, naredi kodo neveljavno oziroma spremembo opazi tudi uporabnik sam pred končno potrditvijo plačila. Plačnik dinamično kodo prejme v obliki potisnega sporočila v aplikaciji, ki vsebuje povzetek nakazila. Plačilo potrdi z vnosom PIN, oziroma vnosom biometričnih podatkov, kjer je to omogočeno.
Dodatno je integriteta mobilne aplikacije in plačil zaščitena s sistemom za prepoznavo zlonamerne kode, kot so na primer beleženje pritiskov tipk (angl. Keylogger), zaznava prekrivanja aplikacij, okrnjene integritete mobilne aplikacije ali omogočenih pravic korenskega dostopa na napravi (angl. Jailbreak/Root). V primeru zaznanih navedenih tveganj, je uporaba mobilne banke onemogočena. Prav tako je onemogočen programski generator enkratnih gesel, za vstop v spletno banko za fizične osebe.

Mobilna aplikacija Flik Pay za prijavo uporablja PIN, ki ga uporabnik nastavi ob registraciji oziroma uporabnikove biometrične podatke, kjer je to omogočeno.
Dodatni verifikacijski element pri potrditvi plačil je uporaba dinamične kode, ki je izračunana iz plačilnih podatkov, in plačniku omogoča pregled poslanih plačilnih podatkov v zaledne sisteme banke pred potrditvijo. Kakršnakoli sprememba plačilnih podatkov s strani napadalcev naredi kodo neveljavno oziroma spremembo opazi tudi uporabnik sam pred končno potrditvijo plačila. Uporabnik dinamično kodo prejme v obliki pojavnega sporočila v aplikaciji, kjer je povzetek nakazila. Plačilo potrdi z vnosom PIN, oziroma vnosom biometričnih podatkov, kjer je to omogočeno.
Dodatno je integriteta mobilne aplikacije in plačil zaščitena s sistemom za prepoznavo varnostnih tveganj, okrnjene integritete mobilne aplikacije ali omogočenih pravic korenskega dostopa na napravi (angl. Jailbreak/Root). V primeru zaznanih navedenih tveganj je uporaba mobilne aplikacije onemogočena.

Dodatni nasveti za zaščito pred zlorabo

- naslov spletne banke vedno vnesite ročno, ali prek zaznamka, ki si ga ustvarite ob prvem obisku. Nikoli do spletne strani ne dostopajte prek spletnih povezav v elektronskih sporočilih;
- 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 spletnih bank. 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 spletnega 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.

Splošni napotki za varnejše elektronsko poslovanje z računalniki in mobilnimi napravami

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

- nakupujte le na spletnih straneh, ki omogočajo varno (https) povezavo, prav tako vedno preverite digitalni certifikat spletnih strani (kdo ga je izdal, komu ga je izdal in 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 spletnih ali mobilne banke;
- redno nameščajte varnostne popravke za operacijski sistem in ostalo programsko opremo na računalniku, pametnem telefonu ali tablici;
- 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;
- na javnih površinah imejte računalnik, pametni telefon ali tablico vedno pod nadzorom;

- plačilne storitve ne izvajajte, ko ste priklopljeni na javna brezžična omrežja, saj lahko pride do prestrezanja podatkov;
- po prenehanju uporabe računalnika, pametnega telefona ali tablice, napravo vedno zaklenite;
- na računalniku uporabljajte lokalni požarni zid, ki ga je potrebno redno posodabljati;
- na računalniku uporabljajte programsko opremo za zaščito pred internetnimi nevarnostmi in virusi ter 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 po potrebi ponovno zaženite spletni brskalnik;
- pametno kartico ali ključ USB z nameščenim kvalificiranim digitalnim potrdilom ter kakšen drug verifikacijski USB element, kot je na primer varnostni ključ FIDO, po uporabi vedno takoj odstranite iz čitalca ali računalnika in shranite na varno mesto;
- mobilne naprave pred neupravičeno uporabo zaščitite najmanj z zaklepanjem zaslona s številko PIN ali geslom, ki je drugačna od številke PIN, ki jih uporabljate za vstop v mobilne aplikacije banke;
- na mobilni napravi hranite le lastne biometrične podatke – banka nima dostopa do biometričnih podatkov, temveč se ti hranijo in obdelujejo zgolj na napravi v okviru operacijskega sistema;
- na mobilni napravi ne omogočajte skrbniških pravic (angl. Jailbreak/Root);
- mobilne aplikacije nameščajte le iz uradnih trgovin, kot sta Google Play in Apple App Store;
- po izhodu iz spletnih, elektronske in mobilne banke se brskalnik in aplikacija v ozadju še naprej izvajata. Z vgrajenimi menijskimi ukazi ustavite program ali storitev po navodilih proizvajalca (postopek je različen v odvisnosti od programa, operacijskega sistema in uporabljene naprave). Le tako se bodo iz delovnega pomnilnika računalnika ali mobilne naprave v celoti izbrisali zasebni podatki;
- 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;
- prijavnih podatkov, verifikacijskih elementov, avtentikacijskih in avtorizacijskih kod ne razkrivajte, jih ne posredujte naprej oziroma ne omogočajte njihove uporabe drugi osebi.

Bankomati in terminali POS

Nevarnosti za uporabnike

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 morejo do svoje kartice, zlonamernež, ki se nahaja v bližini bankomata, pa uporabniku ponudi pomoč, seveda s ciljem, da izve številko PIN. Ko uporabnik po neuspelih poskusih, da bi prišel do kartice, odide, jo zlonamernež 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 zlonamerneži na bankomatu 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 uporabniku 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 tudi čipne in brezstične plačilne kartice, vendar za slednji dve obstajajo dodatne zaščite, ki take napade preprečijo.

Dodatni ukrepi zaščite 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;
- 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 na bankomatu denar, potrdilo in kartico pospravite takoj, šele nato odidite;

- ko bankomat iz neznanega razloga zadrži kartico ali ne izplača denarja, o tem takoj obvestite klicni center 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 ali suma zlorabe

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

Splošni napotki za ukrepanje

- o ugotovljeni zlorabi ali sumu zlorabe 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 ali sumu zlorabe, 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 ali sumu zlorabe, ki je bila povzročena preko interneta:

- takoj prekličite veljavnost zlorabljene plačilne kartice ter za čas do razjasnitve okoliščin onemogočite uporabo vašega spletnega in mobilnega bančništva oziroma spletnih plačilnih 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.

Addiko Bank

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
7. Biometrični podatki - so podatki o posameznikovih fizičnih karakteristikah, kot so na primer prstni odtis, obrazne lastnosti, lastnosti roženice, ki jih mobilna naprava, v kolikor to omogoča, zajame s pomočjo vgrajenih senzorjev in lahko predstavljajo dodatno avtentikacijsko metodo. Biometrični podatki so hranjeni le na mobilni napravi in Banka do njih nima dostopa;
8. Varno spletno nakupovanje – s pojmom "varno spletno nakupovanje" poimenujemo spletno nakupovanje na prodajnih mestih, ki uporabljajo storitev Mastercard SecureCode ali Mastercard Identity Check
9. Rekono storitev: digitalna identiteta, ki se uporablja:
   - za vstop in verifikacijo aktivnosti v spletni banka za pravne osebe Addiko Business Ebank;
   - za uporabo storitve varnega spletnega nakupovanja nove generacije (poimenovan tudi 3D Secure 2.0)
10. Verifikacijski elementi uporabnika – s tem pojmom poimenujemo uporabnikove osebne varnostne elemente (generatorje enkratnih gesel, osebna gesla, biometrične podatke in podobne elemente), ki jih uporabnik uporablja za vstop v digitalne kanale banke in verifikacijo določenih aktivnosti znotraj kanalov ter izvajanje plačilnih transakcij
11. Takojšnje plačilo je elektronsko plačilo, na voljo ves dan, vse dni v tednu, s takojšnjo ali skoraj takojšnjo izvršitvijo oz. odobritvijo sredstev na računu prejemnika plačila in posredovanjem potrditve plačniku.