BANK

HYPO GROUP
ALPE ADRIA

Varna uporaba plačilnih kartic in e-bančništva

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 spletnega bančništva. Udobje brezgotovinskega poslovanja vas 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, zato smo skupaj z Zvezo potošnikov Slovenije pripravili brošuro o varni uporabi plačilnih kartic in e-bančništva.

Radi bi vas opozorili na največje nevarnosti pri brezgotovinskem poslovanju, hkrati pa podali napotke, kako se pred njimi najučinkoviteje zavarujete. Osredotočili smo se na največkrat uporabljane načine brezgotovinskega poslovanja, in sicer plačilne kartice, e-trgovino in e-bančništvo. Dodali smo tudi napotke o tem, kaj storiti, ko zlorabo odkrijete.

Najpogostejši načini zlorab podatkov

Najpogostejša načina zlorabe podatkov s plačilnih kartic sta izdelava ponarejenih magnetnih plačilnih kartic in zloraba podatkov pri oddaljenih nakupih prek spleta. Oddaljeni nakupi so tisti, kjer kupec in prodajalec nista hkrati na istem kraju oziroma kupec ni pri prodajalcu. Sem spadajo vsi spletni nakupi, telefonski nakupi, kataloški nakupi ... Ponarejene magnetne plačilne kartice zlikovci 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 in prenos sredstev v tujino. Kriminalci denar najraje na svoje račune prenašajo preko računov prenašalcev (imenovanih tudi denarne mule), ki največkrat lahkomiselno računajo na hiter zaslužek s provizijo za prenakazilo. Denarna sredstva lahko v tujino pošljejo kriminalci sami ali pa jim pri tem pomagajo denarne mule. Oboji pri tem uporabljajo storitve kot je na primer Western Union, pri kateri kriminalci sredstva 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 e-bančništvu), 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 e-bančništva in drugo.

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 natisnjeni na sprednji strani kartice. Na nekaterih plačilnih karticah je vtisnjena varnostna številka kartice, ki se uporablja pri oddaljenih nakupih. Ta je v obliki 3- ali 4-mestnega števila pri večini izdajateljev zapisana na zadnji strani kartice (npr. MasterCard, Visa), pri nekaterih pa na sprednji strani (npr. American Express). Izdajatelji varnostno številko (angl. Card Security Code – CSC) za oddaljene nakupe poimenujejo različno: CVC2, CVV2 in CID, kar vas ne sme zmotiti, saj gre za isto stvar.

Čipne kartice, kot jih izdaja Hypo Alpe-Adria-Bank d.d., so pri uporabi na terminalih POS ali bankomatih od magnetnih varnejše le v primeru, da so 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

tujini se torej še vedno soočate s starimi tveganji, zato previdnost na takih prodajnih mestih ni odveč.

Splošni napotki za povečanje varnosti:

- Nove kartice takoj podpišite.
- V mobilni telefon si shranite telefonske številke za 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 nepravilnostih pa takoj obvestite Hypo Alpe-Adria-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.
- Vključite storitev obveščanja o uporabi kartice prek sporočil SMS. To je še posebej primerno, ko potujete v države, kjer so zlorabe pogoste.

Nevarnosti za uporabnike

Snemanje magnetnega zapisa (angl. skimming)
Snemanje magnetnega zapisa se najpogosteje dogaja na bankomatih in terminalih POS, lahko pa tudi na samopostrežnih kioskih, kot so npr. na bencinskih črpalkah. S primernim čitalnikom magnetnih kartic lahko to izvedejo vsi, ki imajo vašo kartico ob plačilu blaga ali storitev v rokah. Za zlorabo kartice potrebujejo poleg magnetnega zapisa ponavadi 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). Snemanje magnetnega zapisa s čipnih kartic na bankomatih in terminalih POS, ki so skladni z EMV standardom, ni mogoče. 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.

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.
- Številko 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 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, o tem takoj obvestite banko, lahko pa tudi policijo.
- 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.

Hypo Alpe-Adria-Bank d.d. lahko obvestite osebno ali z elektronsko pošto na naslov varnost@hypo.si ali običajno pošto na naslov Dunajska cesta 117 v Ljubljani.

Spletne trgovine in drugi oddaljeni nakupi

Poslovanje preko spletnih trgovin pomeni nižje stroške za trgovce, za uporabnike pa večje udobje. Varnost spletnih trgovin je običajno dobra, a vseeno slabša od spletnih bank, kljub temu pa na uporabnike preži kar nekaj pasti. Razlika v varnosti nastopi zaradi tega, ker v spletni trgovini lahko nakupuje kdorkoli, medtem ko je pri spletni banki uporabnik že v naprej znan in mu banka zato lažje določi varnostne elemente.

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. Za take napade so ranljive tako magnetne kot čipne plačilne kartice, vendar za slednje obstajajo dodatne zaščite, ki lahko take napade preprečijo.

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). Prav tako tudi v teh primerih za čipne kartice obstajajo dodatne zaščite, ki lahko tovrstne napade onemogočajo.

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. keyloggers) na tipkovnici, brez vaše vednosti pridobijo vse podatke, ki jih potrebujejo za oddaljene nakupe. Tudi tukaj so čipne kartice varnejše od magnetnih, popolna varnost pa ni zagotovljena.

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. Tudi za te napade so magnetne kartice ranljivejše od čipnih.

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.

Hekerski vdor v baze podatkov spletnih trgovcev
Zaradi poznanih prednosti je vedno več uporabnikov spletnih trgovin, žal pa nekateri trgovci 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. Kot v vseh primerih oddaljenih nakupov obstajajo varnostne rešitve za čipne kartice, medtem ko za magnetne žal ne.

Kako se zaščititi pred zlorabo?

- 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.
- V nobenem primeru nikoli ne vpisujte ali ne povejte številke PIN, saj pri oddaljenih nakupih ni potrebna.
- 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.
- Plačilno kartico je zelo priporočljivo registrirati za uporabo varnostnih storitev SecureCode MasterCard SecureCode za nakupe prek spleta. Pri izbiri trgovca dajte prednost tistim, ki omogočajo uporabo teh storitev, saj so ti nakupi varnejši že samo zato, ker podatke o plačilni kartici pošljete neposredno banki in ne trgovcu.
- Če oddaljene nakupe pogosto opravljate, je smiselno samo za te nakupe uporabljati ločeno plačilno kartico.

Spletno bančništvo in spletni trgovalni računi

Razvoj in dostopnost sodobnih informacijskih tehnologij mnogim omogočata poslovanje z banko za domačim računalnikom, ki je povezan v splet. Tega se zavedajo tudi kriminalci, ki poskušajo prek uporabnikov domačih računalnikov priti do tistih podatkov, ki bi jim omogočili tatvino oziroma prenos sredstev na druge račune. In pri tem so dokaj uspešni, tudi v Sloveniji. Napadi na spletno bančništvo, ki uporablja dinamična oziroma enkratna gesla, kot je v uporabi tudi v Hypo Alpe-Adria-Bank d.d., so praviloma zelo težko izvedljivi, zato se tako bančništvo smatra za bolj varno. Uporabniki se še vedno premalo zavedajo, da morajo za svojo varnost najprej poskrbeti sami, seveda pa ob tem upoštevati tudi varnostna navodila, ki jih dobijo od banke.

Nevarnosti za uporabnike

Med največje nevarnosti za uporabnike spletnega bančništva in spletnih trgovalnih računov sodijo 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.

Kako se zaščititi pred zlorabo?

- 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.
- V nobenem primeru nikoli ne vpisujte ali ne povejte številke PIN, saj pri oddaljenih nakupih ni potrebna.
- 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. Spletni naslov vaše banke ali spletnega trgovalnega računa vedno vnesite ročno, nikoli pa do spletne strani ne dostopajte prek spletne povezave v elektronskem sporočilu.
- Vedno preverite digitalni certifikat spletne banke ali spletnega trgovalnega računa. Nekateri spletni brskalniki ujemanje spletnega naslova z digitalnim certifikatom opravljajo že samodejno.
- Pri preverjanju digitalnega certifikata bodite še zlasti pozorni na prstni odtis digitalnega certifikata (angl. Thumbprint), ki ima unikatno vrednost in je ni mogoče ponarediti. Vrednost prstnega odtisa za digitalni certifikat za spletno stran https://www.hyponet.net je objavljena na spletni povezavi

http://www.hypo-alpe-adria.si. Preverjanje vrednosti prstnega odtisa je različno glede na brskalnik, ki ga uporabljate:

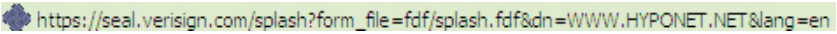
Microsoft Internet Explorer:

Kliknete na ključavnico ob naslovni vrstici. Odpre se pogovorno okno, v katerem kliknete "Ogled potrdil" in 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" in "Razpoznavni odtis":

Mozilla Firefox:

Kliknete v barvni okvir v orodni vrstici in nato "Več podatkov" ali pa na ključavnico desno spodaj. Odpre se pogovorno okno, v katerem kliknete na "Preglej certifikat" in s tem odprete dodatno okno, kjer v spodnjem delu okna vidite vrednosti prstnih odtisov.

- Na vstopni spletni strani banke poiščite znak  in s klikom nanj preverite, da ste dejansko na spletni strani spletne banke HYPOnet. Prikazati se mora novo okno, ki ima v naslovi vrstici besedilo:

  v orodni vrstici pa tudi ključavnico z besedilom VeriSign, Inc. (US). 

- 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.
- Hypo Alpe-Adria-Bank d.d. nikoli ne pošilja e-poštnih sporočil s spletnimi povezavami na prijavno stran HYPOnet. Prosimo vas, da o prejemu takega sporočila nemudoma obvestite banko na e-poštni naslov varnost@hypo.si.
- Spletno bančništvo, ki uporablja tehnologijo enkratnih gesel je za povprečnega uporabnika praviloma bolj varno od tistega, ki uporablja digitalne certifikate.
- Nastavite oziroma aktivirajte vse zaščitne funkcionalnosti, ki jih omogoča ponudnik elektronskega bančništva (npr. pozdravno sporočilo ali sliko na vstopni strani, uporabo navideznih tipkovnic, 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

Uporabniki so bili ob pojavu elektronskega poslovanja nezaupljivi, saj jih je skrbela varnost. Redki so se zavedali, da lahko za varnost največ storijo sami, saj so domači računalniki običajno neprimerno slabše zaščiteni od poslovnih informacijskih sistemov.

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

Kako se zaščititi pred zlorabo?

- 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  , ki se pojavi ob naslovni vrstici ali v spodnji statusni vrstici.
- Takoj izbrišite elektronsko pošto, v kateri pošiljatelj sprašuje po uporabniških imenih, geslih, številkah kartic in drugih občutljivih podatkih.
- Redno nameščajte varnostne popravke za operacijski sistem in ostalo programsko opremo.
- Uporabljajte lokalni požarni zid, ki ga je potrebno redno posodabljati.
- Uporabljajte protivirusno programsko opremo in redno posodabljajte virusne definicije.
- Uporabljajte protivohunsko programsko opremo in jo redno posodabljajte.
- Preverite in prilagodite varnostne nastavitve vašega brskalnika tako, da ta ne bo hranil vaših uporabniških imen in gesel, kot tudi vsebine šifriranih povezav.
- Varnost lahko povečate tudi z uporabo navideznih računalnikov, ki so namenjeni samo spletnim nakupom in spletnemu bančništvu.
- Po končanemu spletnemu nakupu in bančništvu se vedno odjavite iz spletne trgovine/banke, prav tako pa po potrebi ponovno zaženite spletni brskalnik.
- 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 omogoča spletna banka HYPOnet.

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 prek računalnika.

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.
- 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 kvaliteten 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, da bo lahko 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 prek računalnika

- Takoj prekličite veljavnost zlorabljene plačilne kartice, uporabniškega imena ali digitalnega certifikata za e-bančništvo 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, da bo lahko hitro nadaljevala s preiskovanjem, saj je hitrost bistvenega pomena.
- V primeru, ko pride do zlorabe e-bančništva, 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.

Pomembne telefonske številke:

- Preklic plačilnih kartic: 01 583 41 83
- Nadzor mreže bančnih avtomatov: 01 583 41 84
- Pomoč uporabnikom POS-terminalov: 01 583 41 13
- Pomoč pri uporabi HYPOneta: 01 580 43 00, 01 580 43 01 ali 01 580 43 02

Hypo Alpe-Adria-Bank d.d. lahko obvestite tudi osebno, z elektronsko pošto na naslov varnost@hypo.si ali običajno pošto na naslov Dunajska cesta 117 v Ljubljani.

BANK

HYPO GROUP
ALPE ADRIA

www.hypo-alpe-adria.si