

Zloupotreba platnih kartica na internetu ili moto prodajnim mjestima

Pod internet prodajnim mjestom podrazumijeva se onlajn prodavnica koja omogućava naplatu unosom podataka sa platne kartice u odgovarajući web formular, dok se pod MOTO prodajnim mjestima podrazumijeva prodavnica koja omogućava udaljenu prodaju koja se vrši naplatom putem platne kartice na način da se prethodno navedeni podaci o kartici dostave trgovcu putem pošte, elektronske pošte ili izdiktiraju telefonom.



Tip prevare i način rada

Podaci odštampani na platnoj kartici – broj platne kartice, datum važenja i trocifreni sigurnosni broj sa pozadine kartice (CVC ili CVV) se neautorizovano koriste od strane trećeg lica za obradu transakcija na internet ili MOTO prodajnim mjestima.

Do podataka na platnoj kartici može se doći na različite načine:

- kupovinom kartičnih podataka na "crnom" tržištu
- uvidom u samu platnu karticu na nekom od prodajnih mjesta na kojima je vlasnik koristio karticu
- korišćenjem fišing napada
- krađom podataka putem javne wi-fi mreže
- hakovanjem sistema onlajn prodavnica
- do kompromitacije podataka sa platne kartice može da dođe i od strane članova porodice ili prijatelja, što je na žalost čest slučaj u praksi.

Nakon što se prikupe podaci o kartici, oni se koriste za plaćanje na Internet ili MOTO prodajnim mjestima na teret vlasnika kartice.



Mjere predostrožnosti za sigurniju internet kupovinu

- Kartica uvijek mora biti samo u vašem posjedu, nikada je ne pozajmljujte i ne ustupajte drugim licima na korišćenje
- Pažljivo posmatrajte izvršenje transakcija kada god je to moguće, kako biste izbjegli kompromitovanje odštampanih podataka sa platne kartice od strane zaposlenih na prodajnom mjestu
- Neposredno prije plaćanja, potrebno je da pročitate sva obavještenja o vašoj porudžbini i upoznate se sa uslovima kupovine koje u tom momentu prihvatate
- Koristite Vašu platnu karticu isključivo na sajtovima koji zadovoljavaju Visa i Mastercard sigurnosne standarde (Verified by Visa i Mastercard Secure Code) koristeći 3D secure opciju
- Povjerljive podatke ukucajte samo na sajtovima koji počinju sa https://. Veb stranice koje počinju sa https:// omogućavaju siguran prenos podataka koje ste unijeli na vašem pretraživaču do strane koja prikuplja podatke.
- Ako vam sajt nije poznat od ranije, potrudite se da preko veb pretraživača saznate nešto više o izabranom trgovcu, kako biste utvrdili da li je dovoljno pouzdan za kupovinu
- Nikada ne koristite istu lozinku za različite naloge. Elektronsku poštu, profile društvenih mreža, korisničke profile povezane sa uslugama elektronskog bankarstva, kreditnim karticama, finansijskim proizvodima, uvijek zaštitite različitim lozinkama

- Provjerite da li računar sa kojeg obavljate kupovinu ima ažurne verzije operativnog sistema, antivirus softvera i internet pretraživača
- Redovno provjeravajte promet i izvode računa platne kartice kako biste pravovremeno identifikovali sumnjive transakcije
- Ukoliko sumnjate u regularnost neke od transakcija procesuirane vašom platnom karticom, odmah se obratite banci
- Ažurirajte pravovremeno vaše kontakt podatke kako bi Vas banka mogla uspješno kontaktirati u cilju identifikovanja sumnjivih transakcija
- Molimo Vas da u najkraćem roku banci prijavite svaki gubitak, krađu, zloupotrebu, promjenu ili gašenje mobilnog pretplatničkog broja ili tableta preko koga koristite sredstva za identifikaciju (autentifikaciju) i OTP uslugu mobilnog bankarstva
- Nikada ne plaćajte onlajn preko javne wi-fi mreže i ne pristupajte mrežama koje prethodno ne zahtijevaju prijavu
- Kada ste konektovani na neku javnu mrežu, svi podaci koji se prenose sa vašeg uređaja su dostupni svim ostalim korisnicima te iste mreže. Na uređaju sa kojeg pristupate mreži, isključite bilo kakvo dijeljenje privatnih podataka, datoteka i lokacije
- Četvorocifreni PIN broj nikada nemojte nositi zajedno sa karticom i nemojte ga unositi na internet ili saopštavati drugoj osobi
- Nikada ne šalјite fotografije platne kartice ili jednokratnu lozinku. Broj IBAN-a je jedina informacija koju druga osoba treba znati kako bi Vam uplatila novac
- Koristite opciju promjene internet limita kroz CKB GO aplikaciju. Savjetujemo da internet limit uvijek podesite na 0 eura osim u momentima kada trebate izvršiti plaćanje

NAPOMENA:

Banka primjenjuje najsavremenije tehnologije i najviše bezbjedonosne standarde u cilju prevencije svih oblika zloupotreba, kako bi obavljanje transakcija na internetu bilo sigurno i jednostavno. Banka je svim svojim korisnicima omogućila najveći stepen zaštite za kupovinu preko interneta kroz program dodatne identifikacije Mastercard Secure Code i Verified by VISA. Uz pomoć 3D secure password-a (lozinke) klijenti na siguran način plaćaju preko interneta i zaštićeni su od potencijalne zloupotrebe podataka sa kartice. U momentu obrađivanja internet transakcije, klijent putem SMS-a dobija jednokratnu lozinku (OTP) kojom potvrđuje i finalizuje transakciju.