**Co je kód CVV a kód CVC**

Vznik internetových plateb nejen zjednodušil životy uživatelů, ale také zhoršil osobní finance. Zklamání ze statistik naznačují, že 80% případů podvodného krádeže finančních prostředků je spácháno online. Bankovní zákazníci často ztrácejí peníze, neboť kvůli nevědomosti či nedbalosti sdělují podvodníkům soubor důvěrných údajů: číslo, dobu platnosti bankovní karty a kód CVV2 / CVC2.

Co je kód CVC nebo CVV? Jedná se o digitální heslo plastové nebo virtuální karty, která umožňuje identifikaci bankovního zákazníka, když provádí platbu na internetu. Na rozdíl od jednorázových hesel, které jsou vždy generovány k potvrzení platební transakce, kód CVC2 / CVV2 je trvalý, je vytvořen jednou při vystavení karty. Každá karta má bezpečnostní kód CVV / CVC, ať již kreditní nebo debetní.

V závislosti na tom, do kterého platebního systému patří klientská karta, se bezpečnostní kód nazývá CVC nebo CVV.

## Co je CVV a kde ho najdete

CVV znamená hodnotu ověření karty nebo doslovně: ověřovací skóre karty. Jedná se o třímístný kód ověřování karty, který se týká platebního systému VISA. Digitální kombinace je aplikována na zadní straně plastového nosiče v poli pro podpis klienta. Nedaleko jsou poslední čtyři číslice čísla karty a přímo samotný kód, oddělený mezerou.

Není-li šifra mapována nebo přepsána s časem, můžete ji rozpoznat v bance. Zkontrolujte možnost obnovení třímístného hesla prostřednictvím vzdáleného bankovního systému. Chcete-li to provést, musíte na svém osobním účtu odeslat žádost a kód přiloží zprávu na číslo kontaktu vašeho telefonu. Stejným způsobem můžete zjistit kombinace čísel pro virtuální kartu.

## Co je kód CVC a kde je napsáno?

Podobně identifikační heslo v platebním systému Mastercard se nazývá CVC. Doslovně znamená Card Validation Code - ověřovací kód karty. Stejně jako CVV, CVC se skládá ze tří číslic a nachází se na zadní straně plastového nosiče.

**Co znamená číslice 2 v kódu CVV2 / CVC2**

Proč někdy kód CVV / CVC obsahuje číslo 2 v názvu? To znamená, že se jedná o druhý kód bankovní karty. První kód je vytištěn na magnetickém proužku a slouží k ověření bezpečnosti při provádění plateb v obchodě nebo v bankomatu.

## Bezpečnostní požadavky

Je možné hlásit kód CVV karty někomu a uvést ji na stránkách pro provádění plateb a dalších operací? CVV karty jsou stejné důležité informace pro virtuální transakce jako PIN kód pro platby za skutečné karty. Proto není nutné vykazovat kódy vašich karet cizím osobám přesně stejně jako platit kartou na podezřelých místech.

Většina internetových obchodů a služeb neuchovává kódy CVV / CVC ve svých databázích, ale tyto informace používají pouze k ověření držitele karty. Když klient získá půjčku v VC, budete muset zadat třímístný kód CVV, aby jste svázali kartu s profilem a obdrželi peníze. K tomu by mělo být ve fázi vyplňování žádosti uvedeno:

* 16 číslicové číslo karty;
* příjmení, jméno majitele;
* doba platnosti hranice karty ve formátu měsíce a roku;
* třímístný kód CVV / CVC2 v příslušném poli.

Je zcela bezpečné zadat kód CVV karty na webové stránce VC, protože totožnost klienta je ověřována nejen trojciferným trvalým heslem, ale také technologií 3D-Secure. Hesla nejsou uložena v databázi VC. Po zadání kódu a potvrzení operace s jednorázovým heslem bude na kartě rezervováno libovolné množství až do 1 UAH. Služba chce tedy:

а) ujistěte se, že karta, na kterou budou peníze převedeny, patří dlužníkovi;

b) Zabránit možným podvodům.

Po uplynutí doby splácení úvěru nebudete muset data znovu zapisovat, pokud budete platit kartou prostřednictvím osobního účtu. Pokud si klient přeje zaplatit dluh, obejde si osobní účet, na webových stránkách některých platebních služeb budete muset znovu zadat platební údaje včetně karty CVV odesílatele platby.

## Jak podvodníci mohou používat CVV a CVC

Stejně jako jakékoliv jiné osobní heslo by CVV bankovní karty měla být pečlivě uchovávána od neznámých osob. Kód CVV nelze zjistit pouze číslem karty. S celkovými údaji, jako je číslo karty, doba platnosti a kód CVV2, mohou útočníci platit s penězi ostatních lidí na internetu bez znalosti vlastníka. Je pravda, že použití technologie 3D-Secure, když potřebujete zadat jednorázové heslo ze zprávy SMS pro potvrzení operace, komplikuje krádež fondů. Avšak ne všechny internetové obchody a ne všechny banky používají tento protokol ochrany, takže stojí za to pamatovat si pravidla osobní finanční bezpečnosti:

1. 1. Neposílejte fotografie přední a zadní strany plastového nosiče na internetu a pokud je potřeba pořídit fotografii obratu
2. karty, kód CVV by měl být uzavřen.
3. 2. Pod žádnou záminkou nekomunikujte telefonem nebo osobní korespondencí současně s číslem karty, kódem CVV a jednorázovými hesly.
4. 3. Pokud CVV přišla do klienta v SMS, je lepší si zapamatovat kombinaci čísel a vymazat zprávu. Pokud máte dobrou paměť, můžete ji přehrát bezpečně a vymazat třímístnou šifru z plastového nosiče.
5. 4. Bez zvláštních potřeb neukládejte data platebních karet na různých místech. Zvláště pokud web nemá logo Verified by Visa / MasterCard Secure Code. Dokonce i velké stránky se mohou stát předmětem hackerského útoku a důvěrné údaje - padnou do rukou podvodníků.
6. 5. Pro platby na internetu si dejte samostatnou kartu, na které si ponecháte malou částku.
7. 6. Připojte SMS upozornění na změnu stavu vašeho účtu nebo kontrolu zůstatku prostřednictvím internetové banky.

## Omezení CVV2

Z bezpečnostních důvodů může emitent uložit určitá omezení transakcí pomocí kódu CVV. Například vyžadovat zavedení kódu pro jakoukoli platbu v síti. V případě pravidelných plateb nelze kartu použít. Tento problém je zpravidla řešen vytvořením samostatného virtuálního platebního operátora a stanovením limitů. Nebo můžete dočasně vypnout zámek CVV2.

Použití karty pro online transakce nejenže otevírá spoustu příležitostí, ale také ohrožuje peníze. Nezanedbávejte pravidla základního finančního zabezpečení. Nezveřejňujte údaje o kartách externím uživatelům a používejte pouze spolehlivé weby a služby.