Publicat pe (https://www.bnm.md)

23.07.2024

Cum să faci plăți online în condiții sigure și fără riscuri

Ce plăți online fac oamenii zi de zi și cât de răspândite sunt acestea

Odată cu creșterea digitalizării, consumatorii recurg tot mai des la comerțul online. Cele mai des întâlnite cumpărături online sunt cele de echipamente electronice și media digitale, cum ar fi: calculatoarele și telefoanele, jocurile, muzica și cărțile electronice. De asemenea, online se cumpără haine și încălțăminte, produse cosmetice și alimentare, servicii de transport și călătorie și multe altele. Plățile pentru diverse servicii guvernamentale, taxele instituțiilor de învățământ, facturile pentru servicii comunale, de asemenea, pot fi achitate online. Printre principalele motive din care oamenii preferă cumpărăturile online se numără ușurința și rapiditatea procesului care nu necesită deplasare la locul de vânzare, livrarea frecvent gratuită, promoțiile și reducerile, posibilitatea de a citi recenzii, comoditatea procesului de plată.

În Moldova, pe parcursul anului 2023, numărul de platforme de comerț electronic (soluții ce permit acceptarea plăților în mediul online) a crescut cu 57,0%, iar numărul și valoarea operațiunilor de plată fără numerar efectuate prin e-commerce a sporit respectiv cu 15,2% și 17,2%.

De asemenea, în aceeași perioadă, numărul plăților online în Moldova (fără prezența fizică a cardului) a crescut cu 12,5%, iar valoarea operațiunilor de plată online a sporit respectiv cu 25,6%. În prezent, un locuitor al Republicii Moldova efectuează lunar în medie o operațiune de plată online, iar valoarea medie lunară a plăților online per locuitor este de 764 lei.

Datorită avantajelor pe care le oferă, comerțul electronic va continua să crească. Conform estimărilor [1], la nivel mondial, în anul 2023 fiecare a cincea cumpărătură cu amănuntul a fost efectuată în mediul online, iar către anul 2026 se așteaptă că fiecare a patra cumpărătură se va face online.

Ce riscuri puteți întâlni atunci când faceți plăți online

Cu toate avantajele pe care le oferă plățile online, acestea pot avea și anumite riscuri. Ținând cont de faptul că lunar în Moldova sunt efectuate circa 15 milioane de operațiuni cu cardul, valoarea fraudelor înregistrate este nesemnificativă (0.01% din valoarea totală a operațiunilor cu cardul). Totuși este bine de știut cu ce tipuri de riscuri puteți să vă confruntați atunci când faceți plăți online și cum le puteți evita.

Tehnicile de fraudare în cadrul plăților online sunt variate, cele mai frecvente fiind următoarele:

1. Furtul elementelor de securitate ale victimei (phishing). De obicei, se face prin intermediul unei pagini de internet banking sau de inițiere plăți clonate (false), referința la care este trimisă victimei prin poștă electronică, SMS sau mesagerie. Într-un astfel de mesaj, victimei i se cere să deschidă referința sub pretextul necesității urgente de a face „actualizări" referitoare la datele contului bancar sau cele personale, primirea unui premiu, ridicarea unui colet poștal etc. Pe această pagină victima, crezând că accesează site-ul veritabil al băncii sau întreprinderii, introduce date.
2. Imitarea autorităților sau a persoanelor de încredere (inginerie socială). În acest tip de fraude escrocul nu fură datele cardului, ci manipulează victima, astfel încât ea însăși să-i transfere banii. De exemplu, escrocul se poate prezenta (telefonic sau prin mesaj) drept rudă sau prieten care a nimerit într-un accident sau o altă situație urgentă și să-i ceară victimei un transfer de bani pentru a evita arestul sau pentru a plăti servicii medicale. Cu posibilitățile pe care le oferă în prezent inteligența artificială, escrocul poate imita destul de convingător vocea rudei. Sau, de exemplu, răufăcătorul se poate prezenta drept angajat al băncii și să-i spună că în contul victimei a avut loc o tranzacție suspectă și că este nevoie de transferat urgent banii pe un alt cont specificat de el, pentru a-i „proteja". Uneori escrocii se prezintă drept angajați ai poliției sau ai guvernului, cunosc IDNP-ul, data de naștere și alte date personale ale victimei și sunt convingători. Ei îi cer victimei să plătească „impozite" sau „amenzi" în anumite conturi controlate de ei. O variație a acestui tip de fraude reprezintă facturile false pentru diferite servicii (comunale ș.a.), în care sunt indicate conturile escrocului în loc de conturile prestatorului real al serviciilor.
3. Fraude cu plată (comision/taxă) anticipată. În acest tip de fraude victimei i se cere să facă o mică plată în avans pentru a primi ulterior o sumă mare de bani. De exemplu, victima este anunțată că a câștigat un premiu, dar pentru a intra în posesia acestuia trebuie mai întâi să plătească un impozit sau taxa de livrare. Sau un presupus „avocat" anunță victima că este moștenitoarea unei averi după decesul unei rude îndepărtate de peste hotare și că trebuie să transfere o anumită sumă de bani pentru servicii notariale/bilete de avion sau altceva.
4. Vânzarea de produse/servicii fictive. Uneori, după ce ați făcut o comandă online și ați achitat-o, bunul comandat nu este livrat sau serviciul nu este prestat. Se întâmplă și la magazine veritabile din cauza unor erori tehnice sau umane și în acest caz un apel la administrația magazinului ar trebui să ajute. Câteodată însă administrația nu poate fi contactată și nu se cunoaște nimic despre soarta bunului/serviciului comandat.
5. Atacuri prin acces la distanță (malware). Navigând pe internet puteți „prinde" un virus care instalează fără știința dvs. aplicații malițioase pentru interceptarea datelor transmise sau obținerea de drepturi de administrare asupra stației de lucru. Ca variantă, escrocul se poate prezenta drept un membru al echipei de asistență/suport tehnic și să convingă victima să instaleze un instrument de acces la distanță, cum ar fi aplicația AnyDesk sau altele asemănătoare, ca să acceseze calculatorul victimei și contul ei de internet banking, pentru a sustrage banii.

Ce măsuri puteți lua pentru a face plăți online în condiții sigure și fără riscuri

Reguli generale

Banca dvs., cu siguranță, deja a implementat unele soluții de securitate pentru a proteja banii dvs. de eventualele fraude, cum ar fi: sistemele de monitorizare a tranzacțiilor suspecte, limitele presetate pentru operațiuni etc. Cu toate acestea, responsabilitatea principală îi revine clientului deținător de card, care trebuie să respecte anumite reguli de securitate chiar din momentul în care primește cardul de la bancă:

- Când primiți cardul, citiți atent condițiile contractului care este eliberat odată cu înmânarea cardului. Contractul oferă siguranță și protecție împotriva fraudei prin definirea responsabilităților, stabilirea limitelor și a altor condiții generale;
- După primirea cardului, notați numărul de telefon al centrului de suport al băncii dvs., indicat pe versoul cardului, pentru a putea anunța imediat cazul de furt sau pierdere a cardului. Dacă apar suspiciuni legate de fraudă, sunați imediat la bancă anume la acest număr sau blocați cardul direct din aplicația instalată pe dispozitivul mobil.
- Schimbați-vă PIN-ul generat automat pe un PIN ușor de memorizat pentru dvs., dar greu de ghicit pentru persoane terțe. Dacă nu puteți memoriza PIN-ul și sunteți nevoit/ă să-l notați undeva, nu-l păstrați în același loc cu cardul;
- Când creați un PIN nou, evitați combinațiile evidente, cum ar fi data nașterii, ultimele cifre ale numărului de telefon etc.
- Dacă aveți mai multe carduri, nu setați același PIN pe acestea.
- Schimbați periodic codurile PIN ale cardurilor și parolele pentru online banking (sau aplicația mobilă a băncii sau versiunea sa web).
- Nu dați cardul dvs. altor persoane să îl utilizeze, nici chiar membrilor familiei. Păstrați cardul în condiții care exclud pierderea sau furtul lui, sau al datelor indicate pe card;
- În alegerea parolei pentru internet banking sau banking-ul mobil, evitați expresii ușor de determinat de către alte persoane și nu comunicați nimănui parola;
- Nu divulgați codul PIN, CVV, codurile de confirmare de unică folosință nimănui, nici măcar personalului băncii. Schimbați-vă parolele la orice suspiciune că alte persoane le-ar putea ști;
- Nu dezvăluiți detaliile complete ale cardului (numărul, data expirării și codul CVC2), codul PIN, parola pentru online banking sau orice alte parole și coduri trimise prin SMS.
- Abonați-vă la servicii de SMS alert prin care să fiți notificați despre orice tranzacție în conturile dvs.;
- Folosiți serviciul de 3-D Secure pentru plățile online cu cardul. Acesta adaugă o etapă suplimentară de autentificare (în doi factori) ce permite comercianților și băncilor să verifice suplimentar dacă cel care efectuează plata este într-adevăr titularul cardului. Astfel, deținătorul de card trebuie să introducă un cod de confirmare furnizat de bancă pentru fiecare tranzacție, cel mai adesea, printr-un mesaj SMS trimis la numărul de telefon mobil asociat cardului;
- Monitorizați frecvent ceea ce se întâmplă în contul dvs., verificați chitanțele de la magazine şi comparați-le cu datele din istoria tranzacțiilor, astfel încât să puteți identifica erorile sau transferurile neautorizate;
- Este recomandabil să stabiliți limite maxime pentru diverse tipuri de operațiuni în contul dvs. (de exemplu, prin aplicația de mobile banking), pentru a reduce pierderile în cazul în care cardul şi PIN-ul au fost furate;
- Atunci când accesați internet banking-ul, evitați utilizarea terminalelor publice (de exemplu, computere publice la biblioteci). Dacă totuși aveți nevoie să folosiți un terminal public, asigurați-vă că nimeni nu vede datele de acces şi că ați făcut log-out la sfârșitul sesiunii de utilizare;
- Atunci când cumpărați ceva online, asigurați-vă că adresa web a magazinului începe cu: https://. Litera „s” în https:// vă informează că pagina web este securizată;
- Citiți notificările băncii privind noile metode de fraudare;
- Instalați sistemele antivirus și efectuați la timp actualizările de software la dispozitivele utilizate;

— Dacă bănuiți vreo activitate frauduloasă, anunțați imediat banca.

Cum combateți o tentativă de phishing

— În primul rând, trebuie să știm, cum să deosebim mesajele phishing de mesajele normale ale băncilor sau magazinelor. Ele au un șir de trăsături specifice: email-urile falsificate sunt, de regulă, impersonale (nu menționează concret numele dvs.) şi ajung de cele mai multe ori în mapa Spam. Mesajele phishing încearcă să vă dea un sentiment de primejdie și urgență, de exemplu: „URGENT! Dacă nu actualizați datele în 24 de ore, contul dumneavoastră va fi blocat!". Băncile nu practică așa ceva, ele nu solicită niciodată transmiterea/actualizarea datelor personale online și nu au nevoie să le spuneți datele confidențiale ale cardului sau codurile de confirmare de unică folosință primite prin SMS;
— Nu accesați link-uri necunoscute expediate prin email sau mesaje și nu completați datele bancare personale pe site-uri dubioase;
— Accesați pagina web a băncii direct, nu printr-un link primit. Culegeți adresa pe bara de căutare sau salvați pagina web a băncii ca favorită;
— Pentru a face o plată cu cardul într-un magazin online nu este nevoie niciodată să introduceți codul PIN pe niciuna dintre paginile web.

Cum să nu cădeți victimă a ingineriei sociale

— Dacă în conversația telefonică vi se spune că „pentru a primi premiul trebuie să plătiți impozit", „pentru a proteja banii pe card, trebuie să-i transferați în alt cont" etc., nu credeți: este un semnal de fraudă. Nu transferați bani nimănui dacă vi se cere prin telefon. Angajații băncii nu cer niciodată aceasta.
— Nu oferiți persoanelor neautorizate și nu publicați pe rețele sociale informații personale despre dvs. (fotografiile buletinului de identitate, IDNP, data nașterii, numărul actului de identitate, adresa, informații despre membrii familiei etc.), pentru că escrocii ar putea să le utilizeze cu scopul de a mima rudele tale sau angajații statului;
— Fiți vigilenți și tratați cu suspiciune orice apel sau mesaj prin care vi se solicită datele personale sau să faceți un transfer, chiar dacă numărul de telefon sau adresa de email este similară cu cea a băncii. Spuneți persoanei care vă sună că veți reveni singur/ă cu un apel, găsiți numărul de contact oficial al băncii/agenției guvernamentale și sunați la el;
— Dacă primiți un apel de la o rudă/prieten aflat în dificultate financiară, închideți și sunați dvs. ruda la numărul ei/lui obișnuit;
— De regulă, băncile nu-și contactează clienții pe Viber, WhatsApp sau alte mesagerii. Dacă primiți un mesaj sau un apel de la bancă pe aceste canale, contactați banca la numărul ei oficial;

Cum evitați fraudele cu plată anticipată

Feriți-vă de propuneri și promisiuni nerealiste. Nu puteți câștiga un premiu într-o tombolă sau un concurs la care nici nu ați participat și, cel mai probabil, nu sunteți moștenitorul unui milionar de peste hotare. Minuni se întâmplă, dar chiar și așa, ar trebui să vă pună în gardă solicitarea de a efectua o plată în avans.

Ce faceți dacă ați achitat online pentru produse care nu au fost livrate

— Asigurați-vă că știți și aveți încredere în comerciantul de la care cumpărați marfa/serviciul. Dacă magazinul nu vă este cunoscut, alegeți opțiunea de plată după livrare sau nu cumpărați deloc;
— Dacă ați așteptat destul și livrarea nu s-a efectuat, încercați să contactați administrația magazinului sau să inițiați o dispută pe platforma comercială respectivă;
— Dacă nici așa nu ați reușit să soluționați problema, puteți încerca să vă recuperați banii cu ajutorul băncii dvs. printr-o procedură de chargeback. Chargeback este o procedură de contestare a unei plăți cu cardul bancar cu care clientul nu este de acord. Ea este utilizată în cazul în care un vânzător de bunuri sau un furnizor de servicii nu și-a îndeplinit obligațiile.

Atenție! Dacă ați trimis din greșeală banii către o altă persoană, i-ați transferat de bună voie către escroci sau i-ați investit fără succes, chargeback-ul nu va funcționa!. Procedura are loc în felul următor. Cumpărătorul nemulțumit își contactează banca și solicită un chargeback. Banca evaluează dacă este posibil să inițieze o procedură de rambursare. În cazul în care este posibil, aceasta transmite cererea cumpărătorului către sistemul de plată, care o trimite băncii vânzătorului. La rândul ei, banca află dacă clientul său este într-adevăr obligat să returneze banii. Dacă este cazul, debitează suma necesară din contul vânzătorului și o trimite băncii cumpărătorului. Procedura de rambursare este, de obicei, gratuită pentru client, deși băncile pot stabili un comision pentru ea.

Cum vă protejați de atacurile prin acces la distanță

- Evitați accesarea internet banking-ului prin conectarea la rețele wi-fi nesecurizate sau prin terminale publice. Datele dvs. de logare pot fi puse în pericol;
- Instalați pe dispozitivul tău un program antivirus și anti-spyware și actualizați-l frecvent;
- Descărcați aplicații numai din surse sigure;
- Nu deschideți link-uri sau atașamente din email-urile unor persoane pe care nu le cunoașteți.

Ce faceți dacă totuși ați devenit victima unei fraude

- Contactați imediat banca dvs. pentru blocarea cardului, atunci când codurile PIN sau parolele au fost dezvăluite persoanelor terțe, în cazul în care cardul a fost pierdut sau furat, sau dacă au fost efectuate tranzacții frauduloase;
- Sesizează autoritățile cu privire la frauda sau tentativa de fraudă cu cardul tău (de exemplu, serviciul 112).

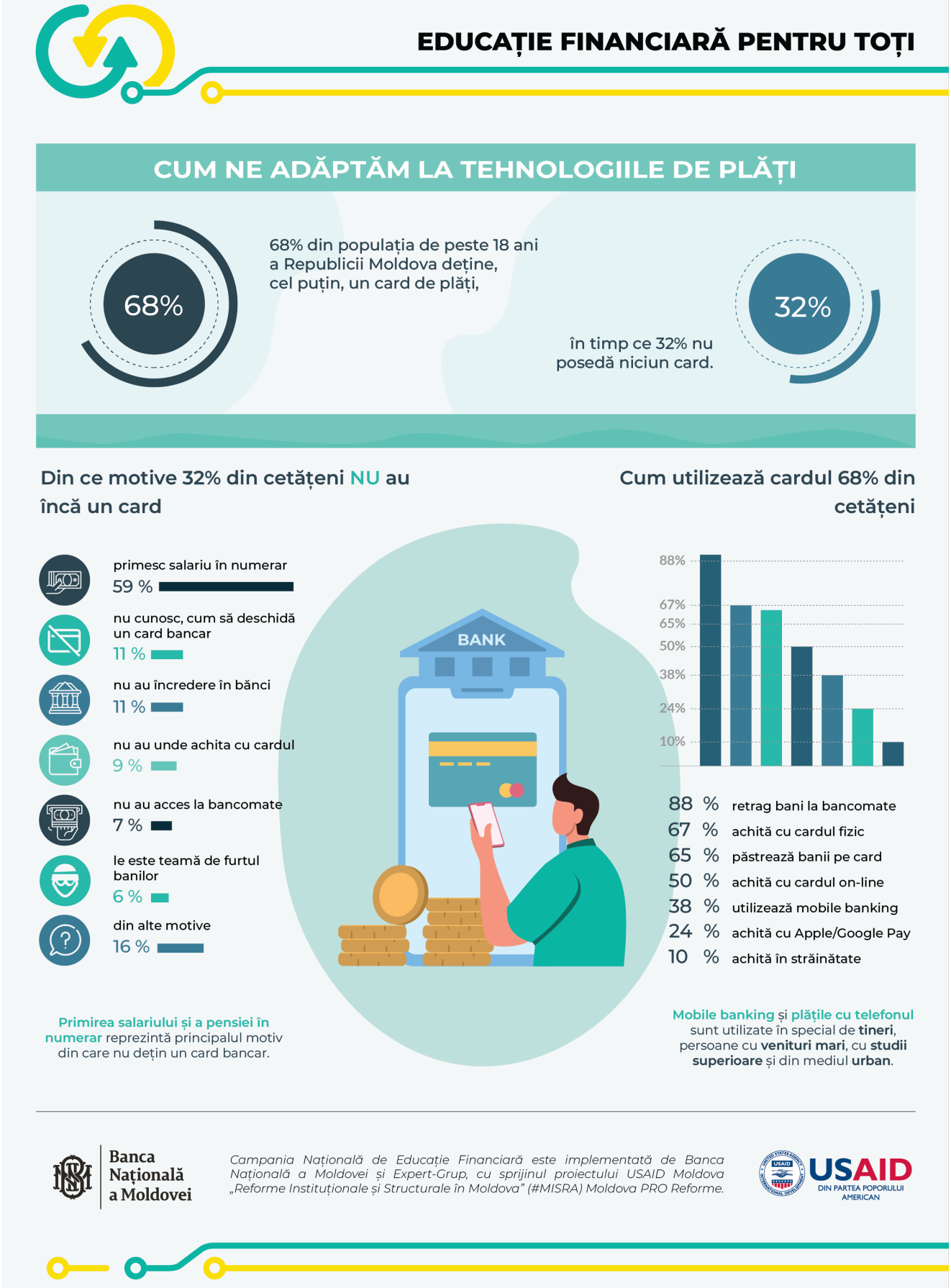
Ce drepturi aveți în calitate de consumator al serviciilor de plată online

În Republica Moldova, drepturile și obligațiile utilizatorilor serviciilor de plată sunt stabilite prin Legea cu privire la serviciile de plată şi moneda electronică [2]. În ceea ce privește securitatea plăților, aceasta prevede următoarele:

- Prestatorul de servicii de plată (banca) trebuie să-i informeze pe clienți cu privire la cerinţele de protejare şi măsurile de siguranţă a plăților: (1) cum să păstreze siguranţa cardului şi modalităţile de notificare a prestatorului în cazul pierderii sau furtului cardului, sau al oricărei utilizări neautorizate a acestuia; (2) procedura de notificare a clientului de către prestator în cazul suspiciunilor de fraudă sau al unei fraude reale, ori în cazul unor amenințări la adresa securității asociate serviciilor de plată;
- Utilizatorul serviciilor de plată are următoarele obligaţii: (a) să utilizeze cardul în conformitate cu condiţiile de emitere şi de utilizare a acestuia; (b) să-l informeze pe prestatorul său de servicii de plată, de îndată ce ia cunoştinţă despre cazurile de pierdere, furt sau de utilizare neautorizată a acestuia; (c) să întreprindă toate măsurile rezonabile pentru a păstra în siguranţă elementele de securitate personalizate;
- În cazul în care clientul nu a păstrat siguranţa elementelor de securitate personalizate ale cardului, el suportă pierderile legate de orice operaţiune de plată neautorizată până la mărimea maximă convenită între el și prestator, dar nu mai mult de 2500 de lei. Clientul suportă toate pierderile legate de orice operaţiune neautorizată dacă aceste pierderi rezultă din fraudă ori din nerespectarea intenţionată, sau din neglijenţă gravă a uneia sau a mai multor obligaţii care îi revin. În astfel de cazuri, suma maximă menţionată mai sus nu se aplică;
- Prestatorul emitent, la primirea înștiinţării de la deţinătorul cardului despre producerea unei situaţii de

urgenţă (pierderea, furtul cardului, tranzacţie neautorizată, blocarea cardului etc.), trebuie să ia toate măsurile necesare pentru oprirea imediată a oricăror tranzacţii prin intermediul cardului în cauză;

- Prestatorul emitent este obligat să stabilească, cel puţin, următoarele modalităţi speciale de comunicare: linie telefonică, adresă e-mail, prin care deţinătorii de carduri de plată să poată solicita explicaţii privind soluţionarea problemelor survenite la utilizarea cardurilor de plată.
- Prestatorul emitent este obligat să asigure informarea deţinătorului de card cu privire la măsurile ce pot fi întreprinse de către acesta în scopul prevenirii cazurilor de fraudă, actualizate în funcţie de evoluţia şi diversificarea tipurilor de fraudă.



[3]

Tag-uri

Cum să faci plăți online în condiții sigure și fără riscuri [4]

educație financiară pentur toți [5]
campania de educatie financiara [6]
campanie de educație financiară [7]
campania de educatie financiar [8]
Educație financiară pentru toți [9]
Educația financară pentru toți [10]

Sursa URL:
https://www.bnm.md/ro/content/cum-sa-faci-plati-online-conditii-sigure-si-fara-riscuri

Legături conexe:

[1] https://www.insiderintelligence.com/content/worldwide-ecommerce-forecast-update-2022 [2] https://www.legis.md/cautare/getResults?doc_id=139642&lang=ro [3] https://www.bnm.md/files/6_Info1-3_1.png [4] https://www.bnm.md/ro/search?hashtags[0]=Cum să faci plăți online în condiții sigure și fără riscuri [5] https://www.bnm.md/ro/search?hashtags[0]=educație financiară pentur toți [6] https://www.bnm.md/ro/search?hashtags[0]=campania de educatie financiara [7] https://www.bnm.md/ro/search?hashtags[0]=campanie de educație financiară [8] https://www.bnm.md/ro/search?hashtags[0]=campania de educatie financiar [9] https://www.bnm.md/ro/search?hashtags[0]=Educație financiară pentru toți [10] https://www.bnm.md/ro/search?hashtags[0]=Educația financară pentru toți