Concepte de afaceri în IT

Săptămâna 9

Dosescu Tatiana-Corina

Universitatea Titu Maiorescu

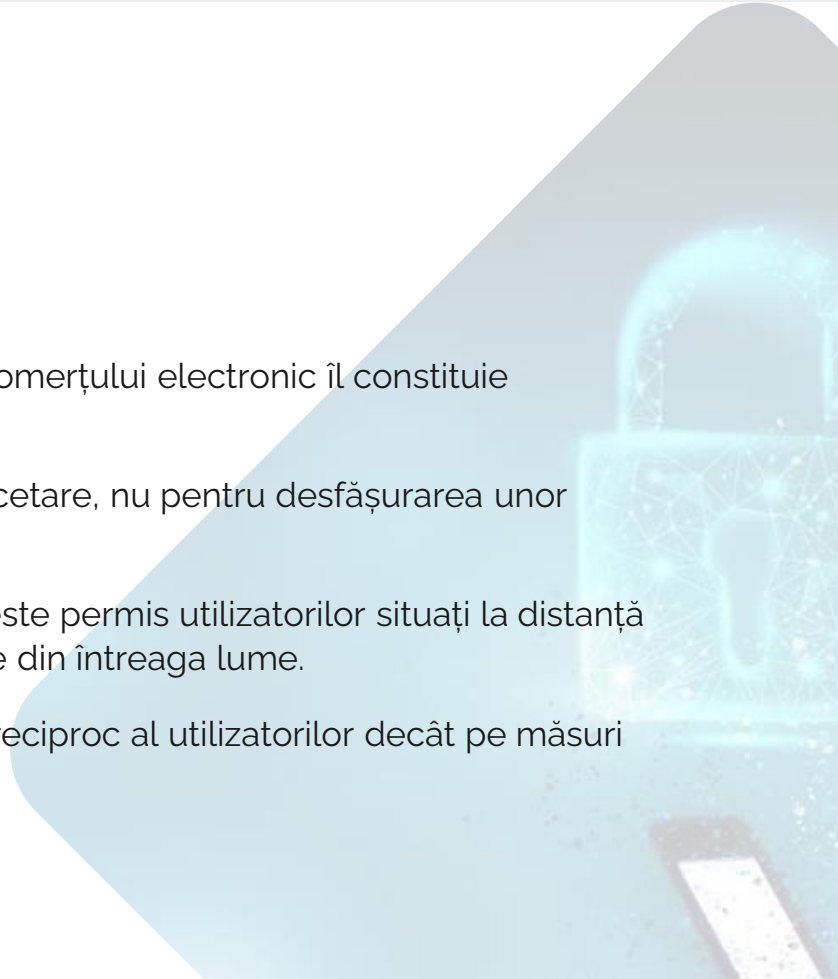
Securitatea în mediul online

Un factor principal care frânează oarecum dezvoltarea comerțului electronic îl constituie insecuritatea.

Inițial, serviciile din Internet au fost proiectate pentru cercetare, nu pentru desfășurarea unor tranzacții comerciale.

Internetul operează într-un mediu de încredere, în care este permis utilizatorilor situați la distanță să acceseze fișierele și resursele critice de pe computere din întreaga lume.

La început, securitatea era lăsată mai mult pe respectul reciproc al utilizatorilor decât pe măsuri tehnice și administrative.

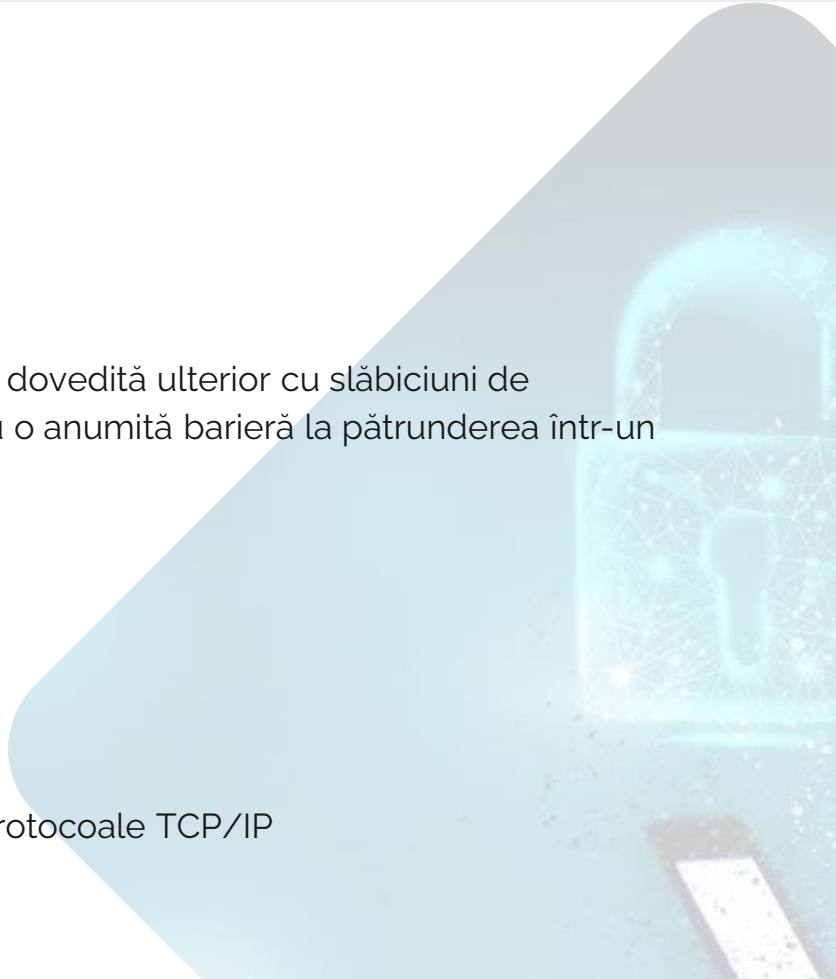


Securitatea în mediul online

O protecție minimă, considerată mult timp suficientă, dar dovedită ulterior cu slăbiciuni de concepție, au constituit-o sistemele de parole care creau o anumită barieră la pătrunderea într-un sistem aflat la distanță.

Toate atacurile online speculează:

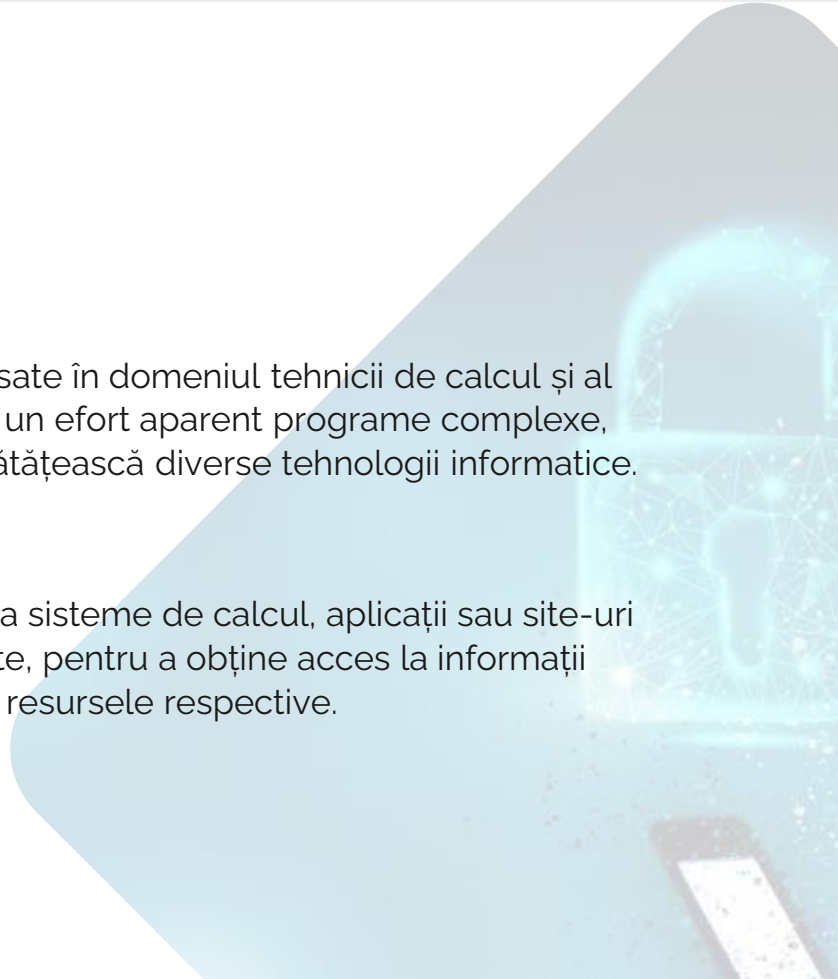
1. proasta configurare a unor sisteme
2. erorile în scrierea programelor
3. administrarea neglijentă a unor rețele
4. neglijența unor utilizatori autorizați
5. lipsa totală de servicii de securitate în ierarhia de protocoale TCP/IP



Securitatea în mediul online

- **Hacker** - persoană care are cunoștințe foarte avansate în domeniul tehnicii de calcul și al programării, reușește să scrie sau să înțeleagă fără un efort aparent programe complexe, precum și să proiecteze, să dezvolte sau să îmbunătățească diverse tehnologii informatice.

- **Cracker** - persoană care obține acces neautorizat la sisteme de calcul, aplicații sau site-uri Web, trecând peste măsurile de securitate existente, pentru a obține acces la informații confidențiale sau pentru a utiliza în diverse scopuri resursele respective.



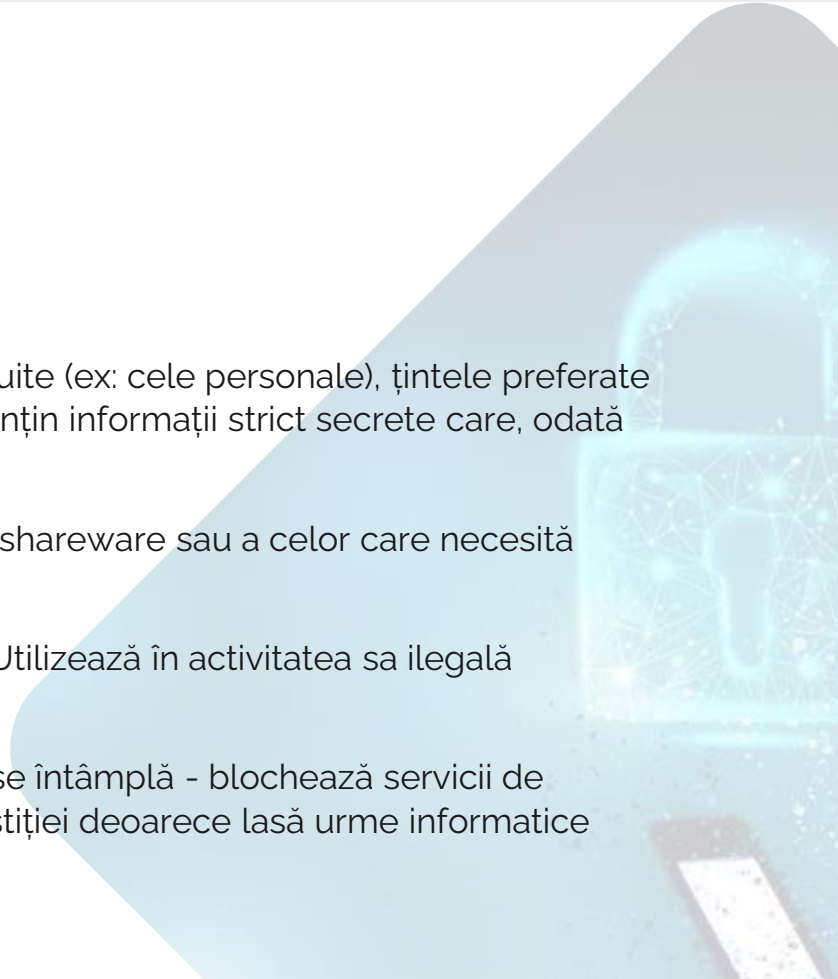
Securitatea în mediul online

Crackerii care se respectă nu distrug paginile Web obișnuite (ex: cele personale), țintele preferate fiind site-urile importante care au protecții avansate și conțin informații strict secrete care, odată obținute, sunt publicate pe Internet.

Mulți crackeri sunt specializați în spargerea programelor shareware sau a celor care necesită introducerea unui cod serial.

Haxor - cracker amator, fără cunoștințe de programare. Utilizează în activitatea sa ilegală programe create de alții.

În mod obișnuit, haxorii care - din dorința de a vedea ce se întâmplă - blochează servicii de utilitate publică (ex: motoare de căutare), ajung în fața justiției deoarece lasă urme informatice care îi deconspiră.



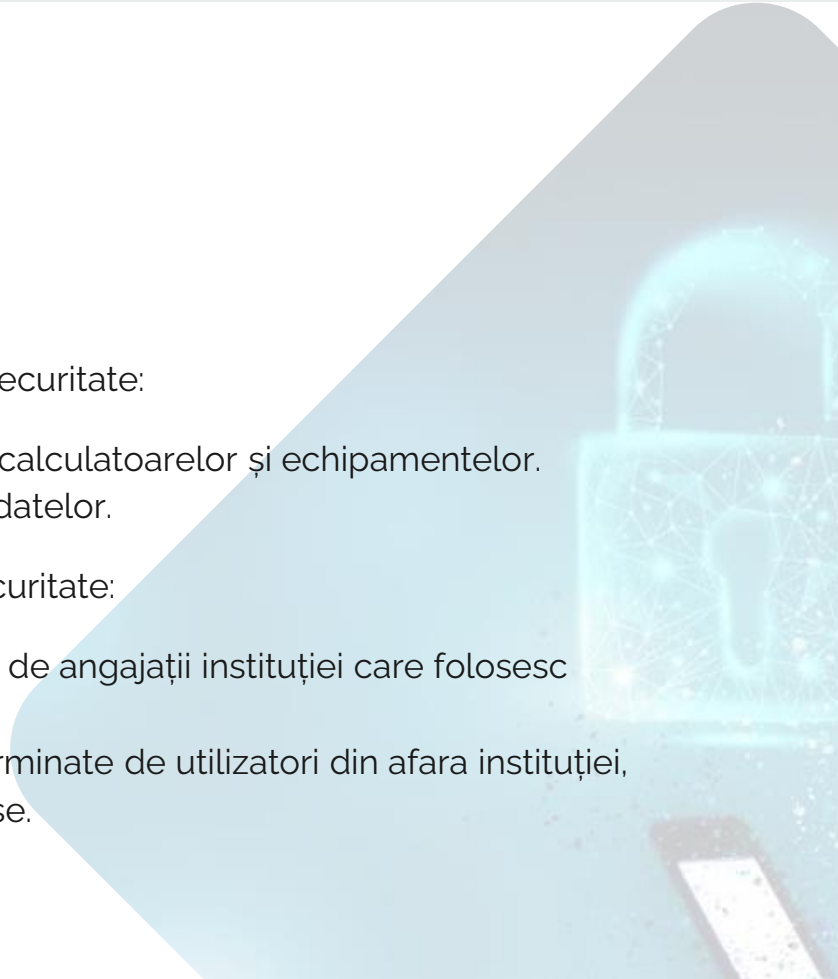
Securitatea în mediul online

În funcție de nivelul la care se produc, există atacuri de securitate:

- **la nivelul fizic**: furtul, distrugerea sau deteriorarea calculatoarelor și echipamentelor.
- **la nivelul datelor**: ștergerea, coruperea sau furtul datelor.

În funcție de localizarea atacatorilor, există atacuri de securitate:

- **interne** (sau locale [local attack]): sunt determinate de angajații instituției care folosesc rețeaua și pot fi intenționate sau neintenționate.
- **externe** (sau la distanță [remote attack]): sunt determinate de utilizatori din afara instituției, care nu au acces autorizat la date sau la alte resurse.



Securitatea în mediul online

În funcție de consecințele asupra rețelei, atacurile de securitate fac parte din următoarele categorii:

- **atacuri pasive**: au ca scop furtul informațiilor, nu distrugerea/deteriorarea acestora.
- **atacuri active**: au ca scop furtul, coruperea sau distrugerea informațiilor.

În contextul comerțului electronic, atacurile la securitate se manifestă, cu precădere, astfel:

- **Ascultarea comunicațiilor**: poate conduce la furtul unor informații importante ale clienților (ex: nr. cardului de plată, nr. contului bancar, etc).
- **Furtul parolelor**: permite accesul la sisteme care stochează date importante.
- **Modificarea datelor**: determină alterarea mesajelor prin modificare, inserare sau ștergere.
- **Refuzul serviciului**: o entitate nu-și poate îndeplini propria funcție sau face acțiuni care împiedică o altă entitate să-și îndeplinească propria funcție.
- **Repudierea serviciului**: o entitate refuză să recunoască un serviciu efectuat de o altă entitate.

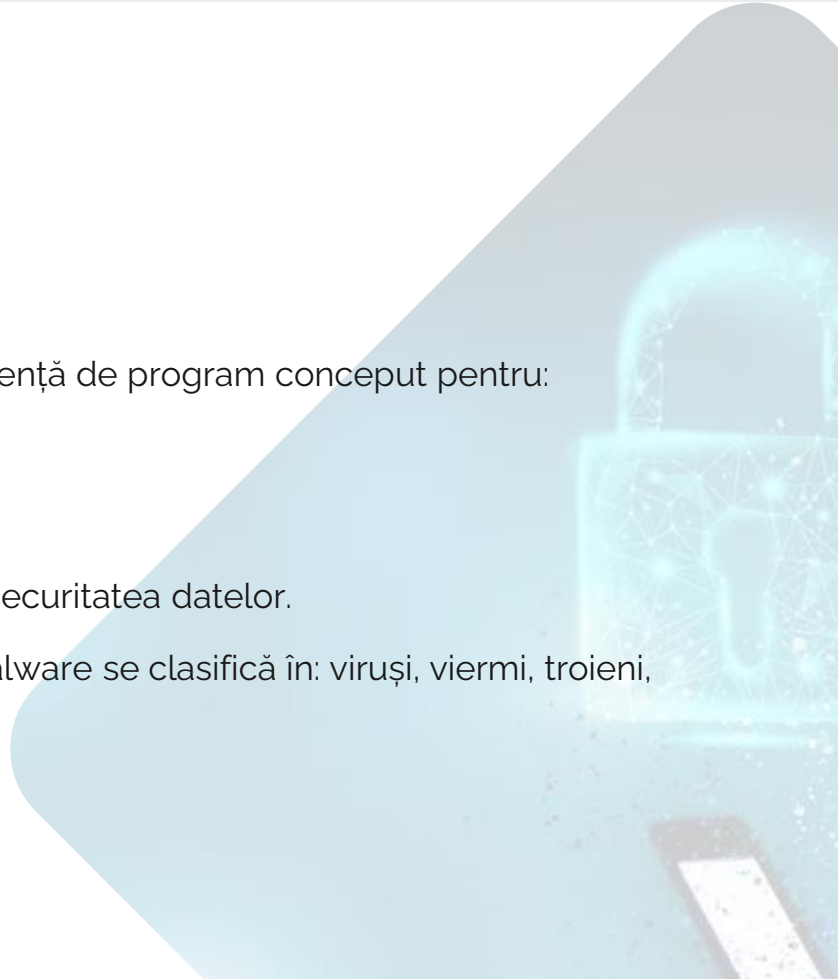
Malware

Un software de tip **malware** este un program sau o secvență de program conceput pentru:

- a perturba funcționarea corectă a unui calculator
- a aduna informații confidențiale
- a obține acces neautorizat la resursele sistemului.

Reprezintă una dintre cele mai grave amenințări pentru securitatea datelor.

În funcție de acțiunea determinată, software-ul de tip malware se clasifică în: viruși, viermi, troieni, bombe, spoofere, căi ascunse, etc.

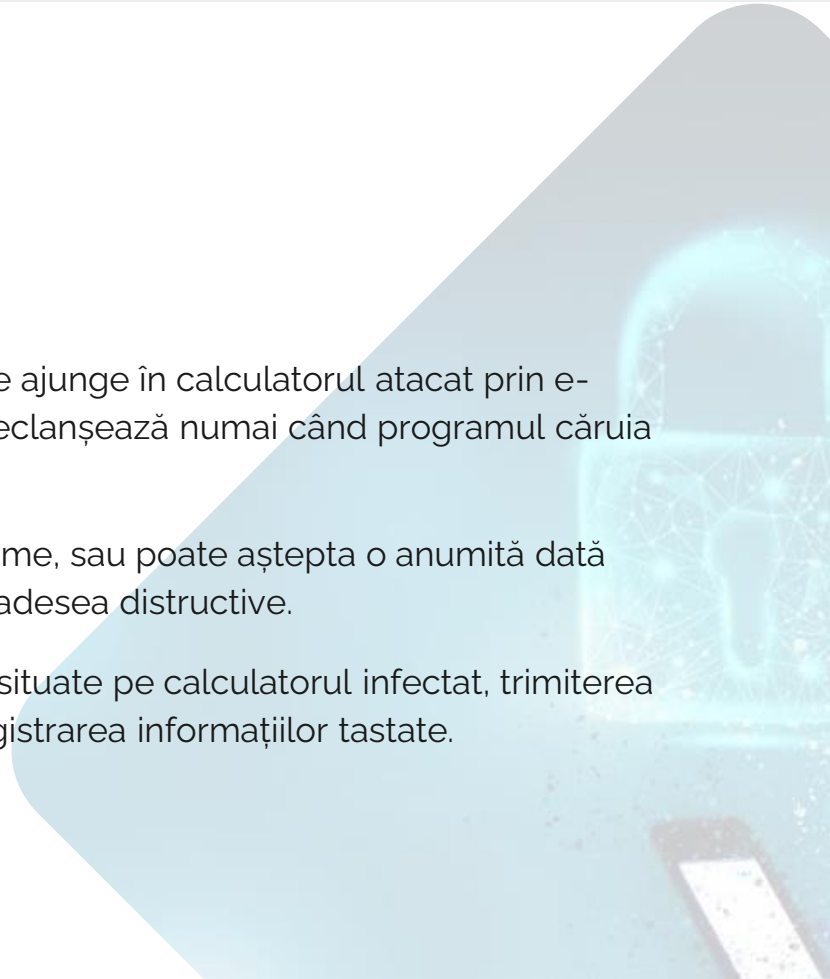


Malware

Virus - program dependent de un alt program, care poate ajunge în calculatorul atacat prin e-mail, transfer de fișiere sau mesaje și a cărui acțiune se declanșează numai când programul căruia îi este atașat este lansat în execuție.

Virusul se poate reproduce imediat, infectând alte programe, sau poate aștepta o anumită dată sau un anumit eveniment, realizând acțiuni neautorizate, adesea distructive.

Consecințe ale acțiunii unui virus: ștergerea unor fișiere situate pe calculatorul infectat, trimiterea unor mesaje e-mail către toate adresele existente în înregistrarea informațiilor tastate.



Malware

Un virus informatic are un ciclu de viață:

Creare → de către un programator

Multiplicare → virusul se copiază de la un calculator la altul

Activare → virusul se lansează în execuție

Detectare → virusul este descoperit, începe studierea acestuia

Asimilare → producătorii de software antivirus includ semnătura noului virus în tabelul de semnături

Eradicare → programele antivirus elimină virusul

Securitatea în mediul online

Trap Doors

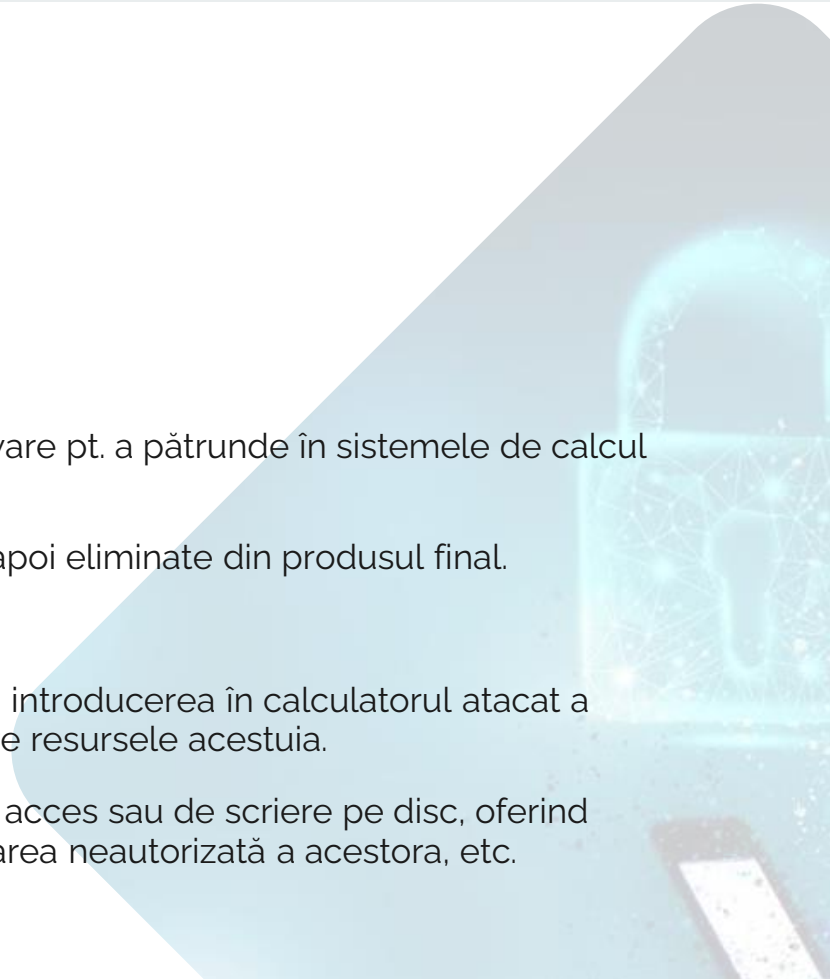
Sunt mecanisme de acces create de proiectanții de software pt. a pătrunde în sistemele de calcul prin ocolirea mecanismelor de protecție.

Sunt folosite în perioada de testare a software-ului, fiind apoi eliminate din produsul final.

Back Doors

Sunt, de obicei, create cu ajutorul troienilor, presupunând introducerea în calculatorul atacat a unui program care, ulterior, va deschide căi de acces către resursele acestuia.

Mecanismul **Back Door** permite încălcarea restricțiilor de acces sau de scriere pe disc, oferind posibilitatea violării confidențialității informațiilor, modificarea neautorizată a acestora, etc.



Securitatea în mediul online

Programele de tip adware

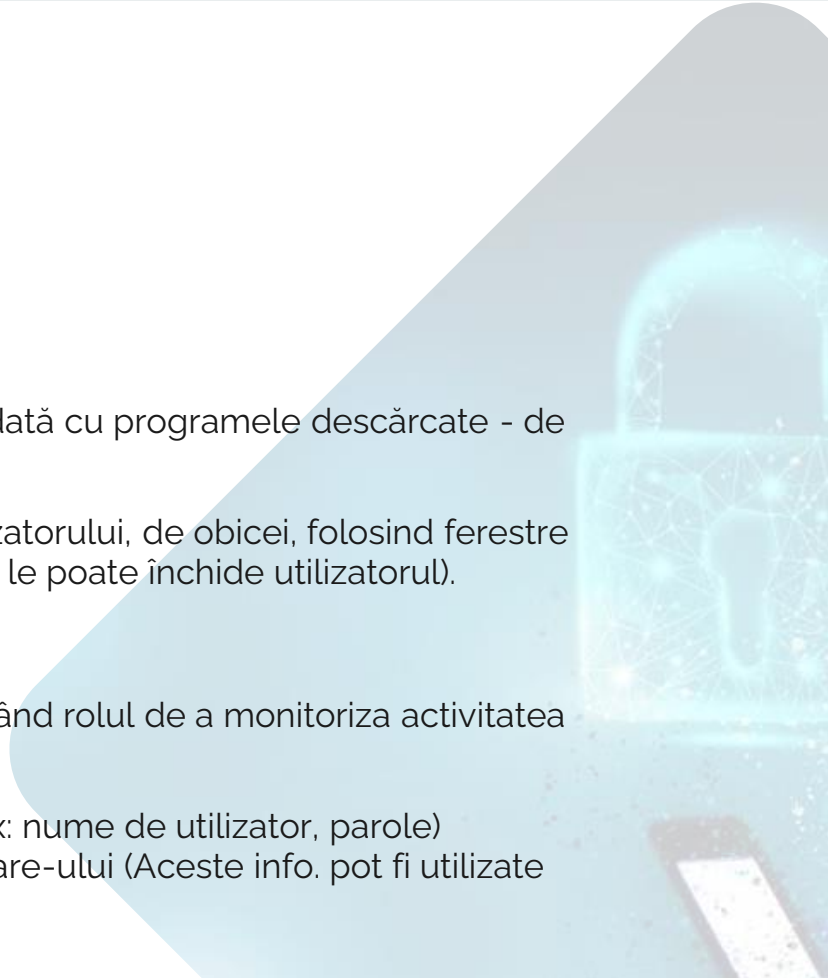
Sunt distribuite, fără cunoștința și acordul utilizatorului, odată cu programele descărcate - de obicei, gratuit - de pe Internet.

Au rolul de a afișa mesaje publicitare pe calculatorul utilizatorului, de obicei, folosind ferestre pop-up (Acestea sunt deschise adesea mai repede decât le poate închide utilizatorul).

Programele de tip spyware

Sunt distribuite fără cunoștința și acordul utilizatorului, având rolul de a monitoriza activitatea acestuia.

Transmit informațiile legate de activitatea utilizatorului (ex: nume de utilizator, parole) organizației/persoanei responsabile cu distribuirea spyware-ului (Aceste info. pot fi utilizate ulterior pt. atacarea calculatorului respectiv).

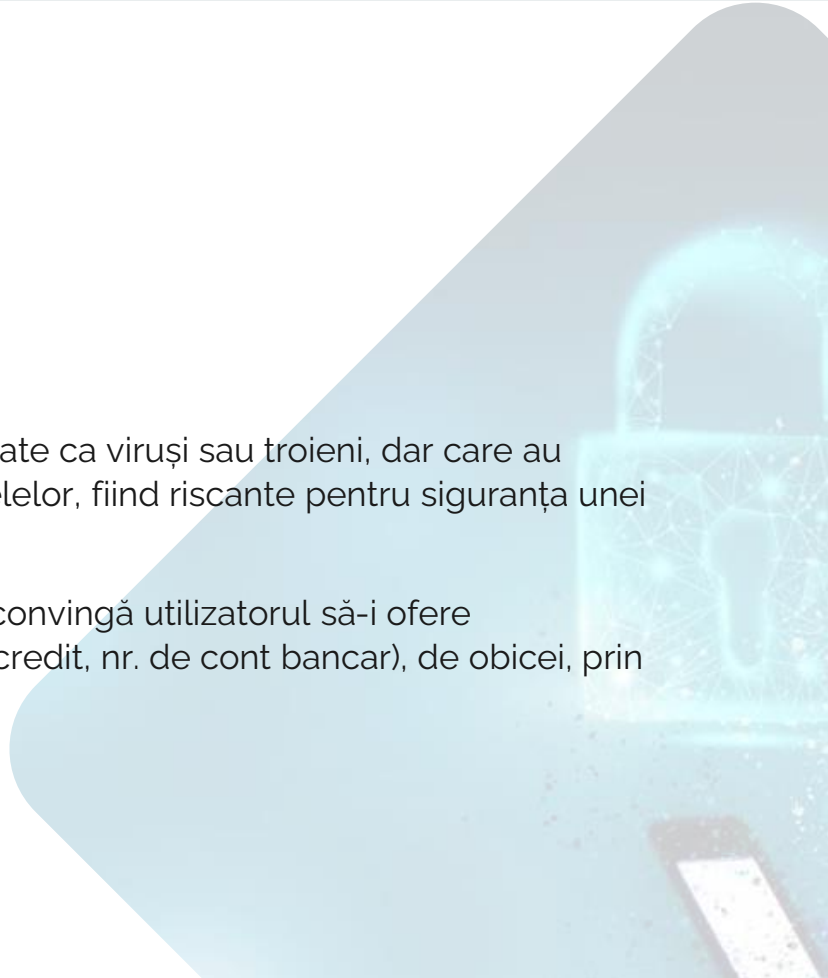


Securitatea în mediul online

Grayware

Termenul se referă la aplicații/fișiere care nu sunt clasificate ca viruși sau troieni, dar care au scopul de a afecta performanța calculatoarelor sau a rețelelor, fiind riscante pentru siguranța unei organizații.

Multe atacuri **grayware** sunt de tip phishing: încearcă să convingă utilizatorul să-i ofere atacatorului acces la informații personale (ex: nr. card de credit, nr. de cont bancar), de obicei, prin intermediul unor formulare online.



Prevenirea fraudelor în comerțul electronic

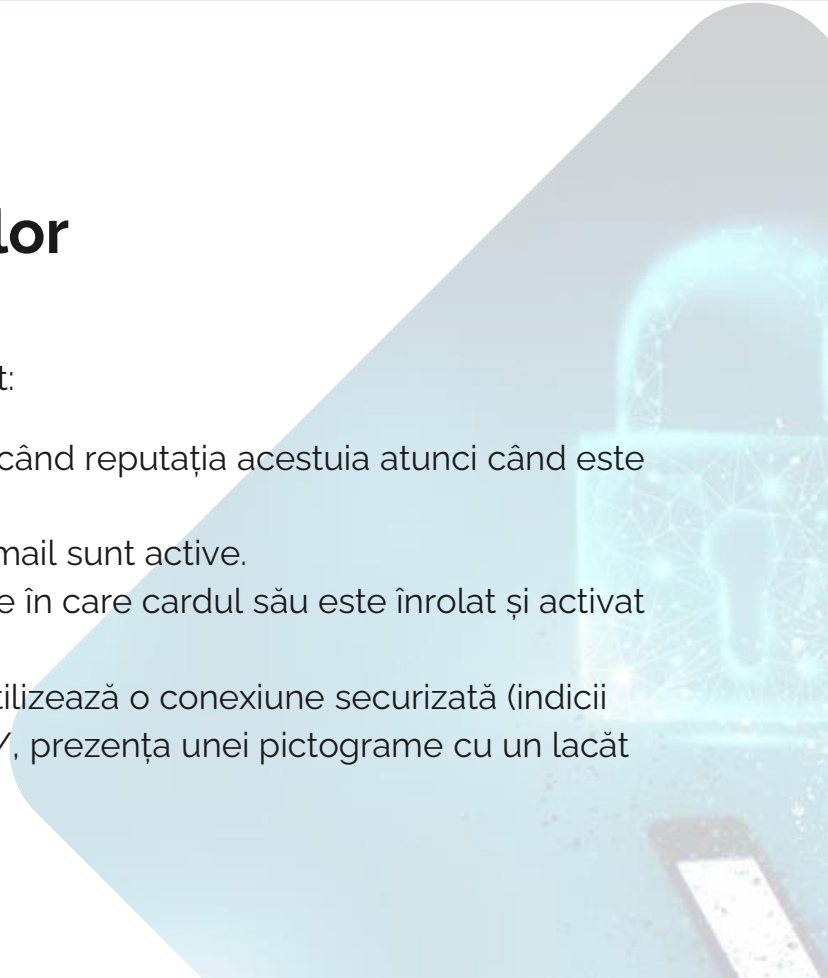
Câteva dintre fraudele cu care pot lua cunoștință clienții magazinelor electronice și măsurile necesare pentru evitarea lor:

- Frauda prin nelivrarea produselor
- Frauda cu cărți de credit
- Furtul de identitate (Phishing)

Fraudă prin nelivrarea produselor

Pentru a evita o astfel de fraudă, este necesar ca un client:

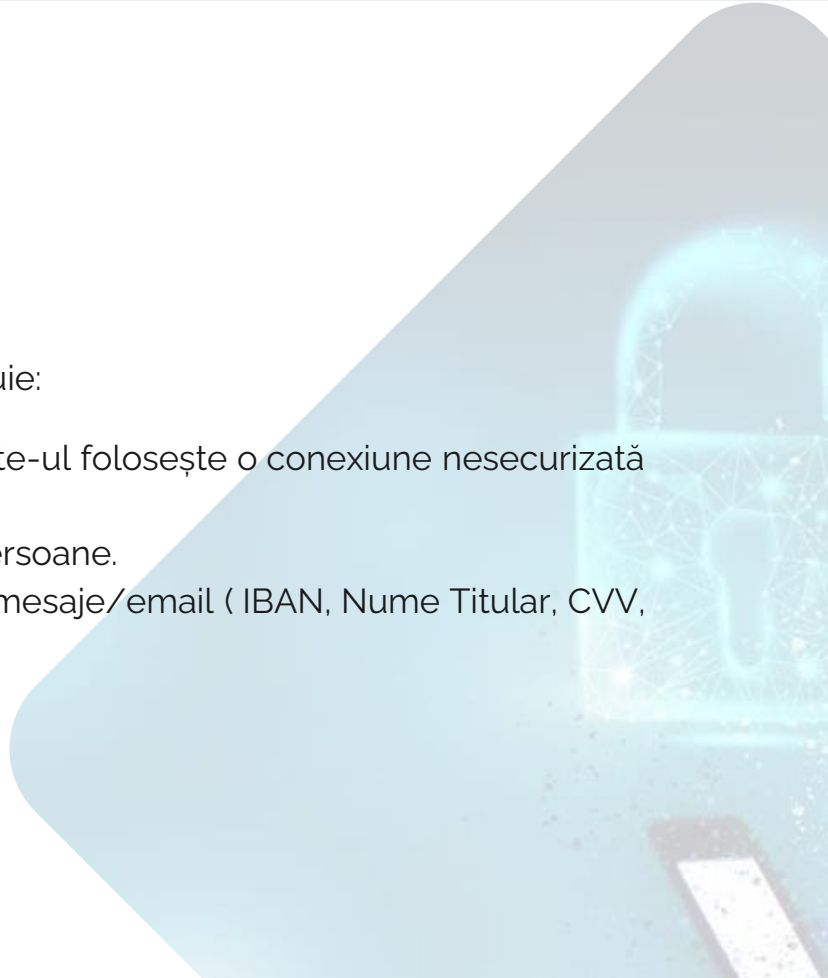
- să se asigure că vânzătorul este de încredere, verificând reputația acestuia atunci când este posibil.
- să verifice dacă numărul de telefon și adresa de e-mail sunt active.
- să tranzacționeze în sistemul **3D Secure**, în condițiile în care cardul său este înrolat și activat în acest sistem.
- să se asigure că site-ul pe care se face tranzacția utilizează o conexiune securizată (indicii ale unei pagini securizate: adresa începe cu https://, prezența unei pictograme cu un lacăt închis în fereastra browserului).



Frauda cu cărțile de credit

Pentru a nu fi victima unei astfel de fraude, un client trebuie:

- să nu ofere niciodată informații despre card dacă site-ul folosește o conexiune nesecurizată sau dacă reputația acestuia este îndoielnică.
- să nu ofere informații referitoare la card nici unei persoane.
- să nu ofere informațiile bancare la telefon sau prin mesaje/email (IBAN, Nume Titular, CVV, etc)

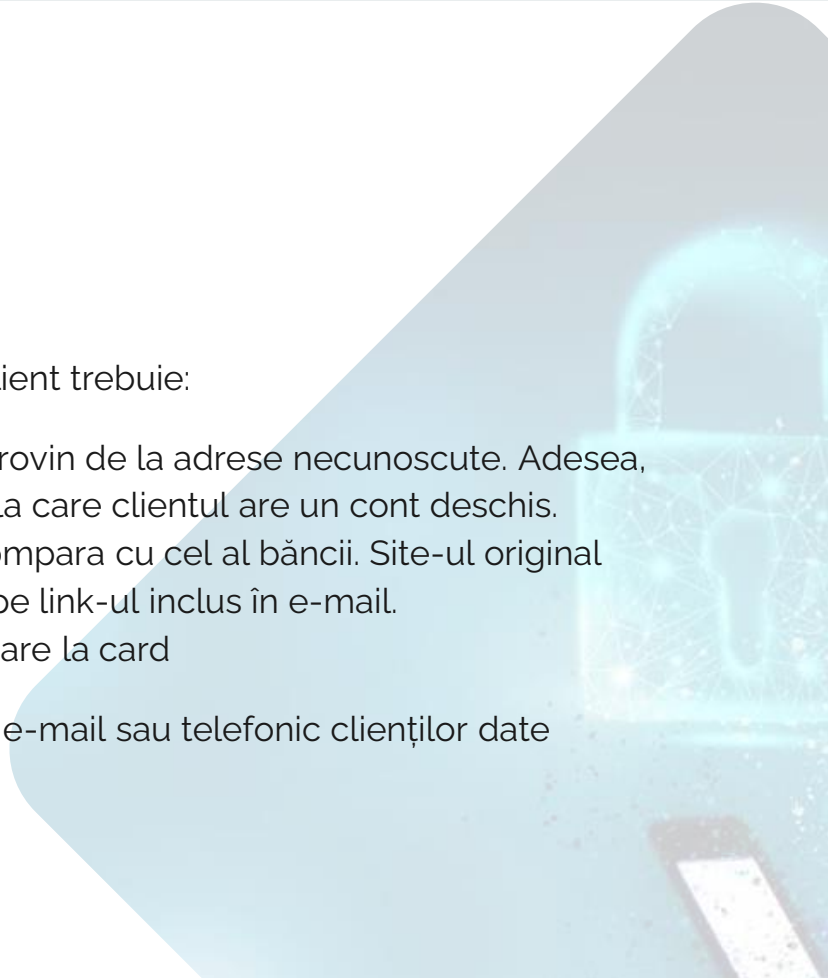


Furtul de identitate (Phishing)

Pentru a nu cădea pradă unei tentative de **phishing**, un client trebuie:

- să nu acceseze link-urile incluse în mesajele care provin de la adrese necunoscute. Adesea, aceste mesaje de e-mail par că provin de la banca la care clientul are un cont deschis.
- să verifice în browser numele site-ului pentru a-l compara cu cel al băncii. Site-ul original trebuie accesat direct, nu prin efectuarea unui clic pe link-ul inclus în e-mail.
- să nu divulge niciodată datele confidențiale referitoare la card

Trebuie reținut că, prin politica lor, băncile nu solicită prin e-mail sau telefonic clienților date confidențiale.



Protocolul de securitate 3D Secure

Lansat în România în feb. 2004, **3D Secure** este un sistem antifraudă dezvoltat de Visa și de MasterCard.

Permite creșterea securității tranzacțiilor online prin solicitarea unei parole la fiecare plată.

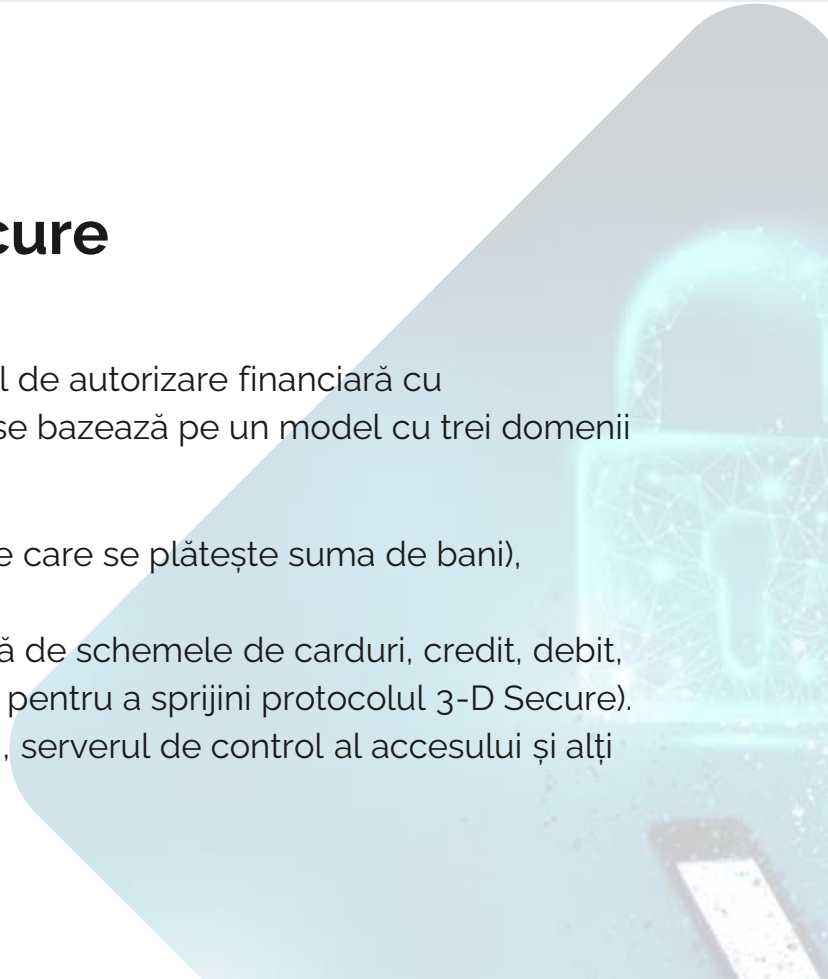
În site-urile care afișează logourile **Verified by Visa** și **MasterCard SecureCode**, utilizatorul este solicitat să se autentifice la fiecare tranzacție, păstrând astfel controlul asupra cumpărăturilor efectuate.

Procesul de autentificare nu necesită instalarea vreunei aplicații speciale pe calculatorul clientului și nici nu îngreunează navigarea.

Protocolul de securitate 3D Secure

Conceptul de bază al protocolului este de a lega procesul de autorizare financiară cu autentificarea online. Această autentificare suplimentară se bazează pe un model cu trei domenii (de unde şi "**3-D**" în nume). Cele trei domenii sunt:

1. **Domeniul achizitorului** (banca și comerciantul către care se plătește suma de bani),
2. **Domeniul emitentului** (emitentul cardului),
3. **Domeniul interoperabilității** (infrastructura furnizată de schemele de carduri, credit, debit, carduri preplătite sau alte tipuri de carduri de plată, pentru a sprijini protocolul 3-D Secure). Acesta include internetul, plug-in-ul comerciantului, serverul de control al accesului și alți furnizori de software.



Protocolul de securitate 3D Secure

În cazul în care un card înrolat în **3D Secure** este furat, acesta nu poate fi folosit de alte persoane pt. cumpărături online.

Prin folosirea acestui sistem de tranzacționare s-a observat o reducere a disputelor din fraudele rezultate din tranzacțiile online cu cel puțin 80%.

Pe măsură ce tot mai multe magazine virtuale împreună cu băncile lor și tot mai multe bănci emitente de carduri aderă la acest serviciu, crește încrederea tuturor părților implicate în tranzacțiile pe Internet și, implicit, volumul acestora, scăzând concomitent riscul de fraudă.

Protocolul de securitate 3D Secure

Beneficiile serviciului **3D Secure**:

- Securitate sporită pentru tranzacțiile online.
- Asigurarea că doar posesorul cardului poate tranzacționa online.
- Cardul înrolat în **3D Secure** va fi recunoscut automat în toate magazinele înrolate în acest sistem.
- Reducerea riscului de fraudă atât pt. comercianți, cât și pt. posesorii de carduri înrolate.
- Creșterea calitativă a serviciilor oferite.
- Reducerea tranzacțiilor disputate și a costurilor aferente.

Sisteme electronice de plată

Cele mai multe activități de comerț electronic implică schimbul unor forme de bani pentru bunuri și servicii. În acest context, o funcție importantă a site-urilor de comerț electronic este gestionarea plăților prin Internet.

În general, în comerțul electronic B2B, companiile folosesc **EFT** (**E**lectronic **F**unds **T**ransfer) și **EDI** (**E**lectronic **D**ata **I**nterchange) financiar pt. a efectua plăți online.

În comerțul electronic B2C, câteva dintre alternativele pt. plăți online sunt:

- cardurile de plată (de debit, de credit)
- banii electronici
- portofelele electronice
- cardurile cu valoare stocată

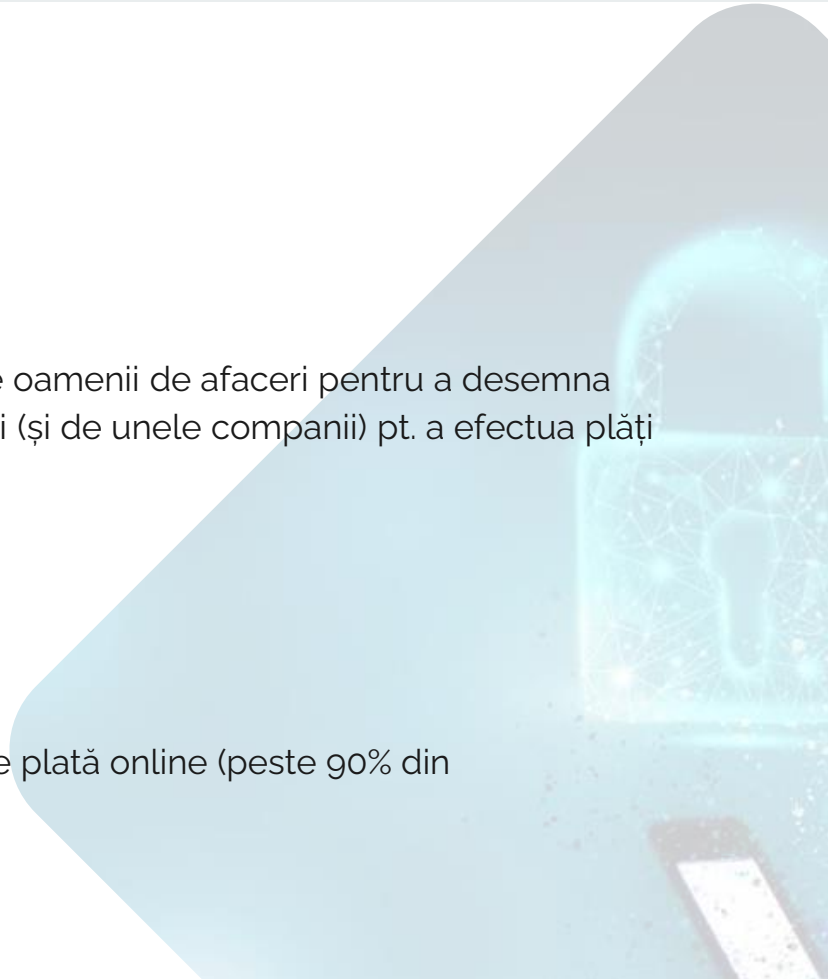
Sisteme electronice de plată

Card de plată [Payment card] = termen general utilizat de oamenii de afaceri pentru a desemna toate tipurile de carduri de plastic folosite de consumatori (și de unele companii) pt. a efectua plăți în procesul de cumpărare.

Principalele categorii de carduri de plată:

- card de credit
- card de debit

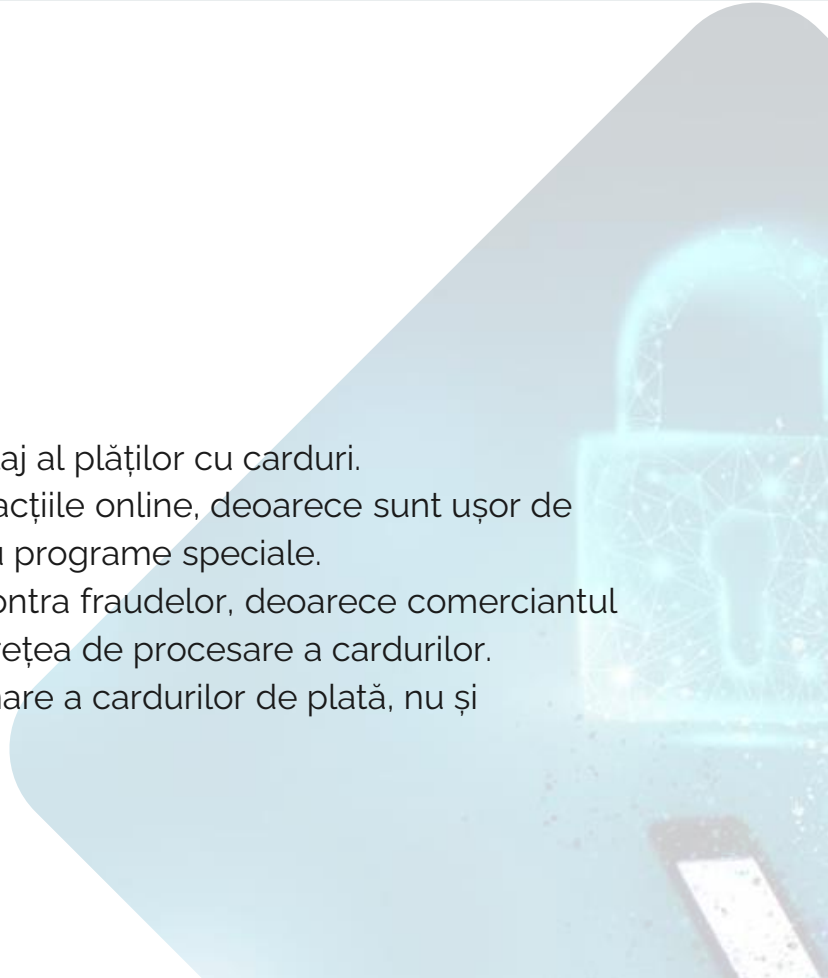
Cardurile de plată reprezintă cea mai populară metodă de plată online (peste 90% din cumpărăturile pe Internet, peste 95% în S.U.A.).



Sisteme electronice de plată

Avantaje:

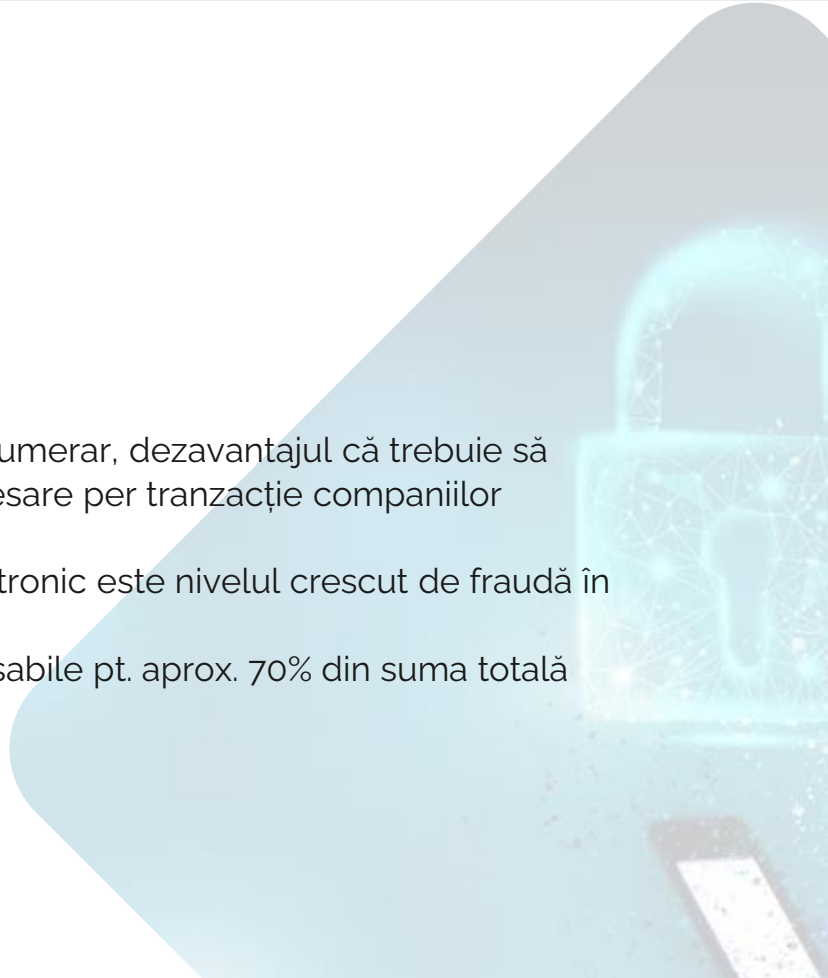
- Acceptarea globală este, poate, cel mai mare avantaj al plăților cu carduri.
- Cardurile de plată sunt foarte potrivite pentru tranzacțiile online, deoarece sunt ușor de folosit, neavând nevoie de dispozitive hardware sau programe speciale.
- Cardurile de plată oferă comerciantului protecție contra fraudelor, deoarece comerciantul poate autentifica și autoriza o tranzacție folosind o rețea de procesare a cardurilor.
- Clientul plătește, de obicei, numai o taxă de gestionare a cardurilor de plată, nu și comisioane per tranzacție.



Sisteme electronice de plată

Dezavantaje:

- Pentru comerciant există, comparativ cu plățile în numerar, dezavantajul că trebuie să plătească taxe de procesare lunare și taxe de procesare per tranzacție companiilor furnizoare de servicii legate de cardurile de plată.
- O altă problemă pe care o întâmpină comerțul electronic este nivelul crescut de fraudă în tranzacțiile online.
- Tranzacțiile online cu carduri de credit sunt responsabile pt. aprox. 70% din suma totală fraudată în toate tranzacțiile cu cărți de credit.



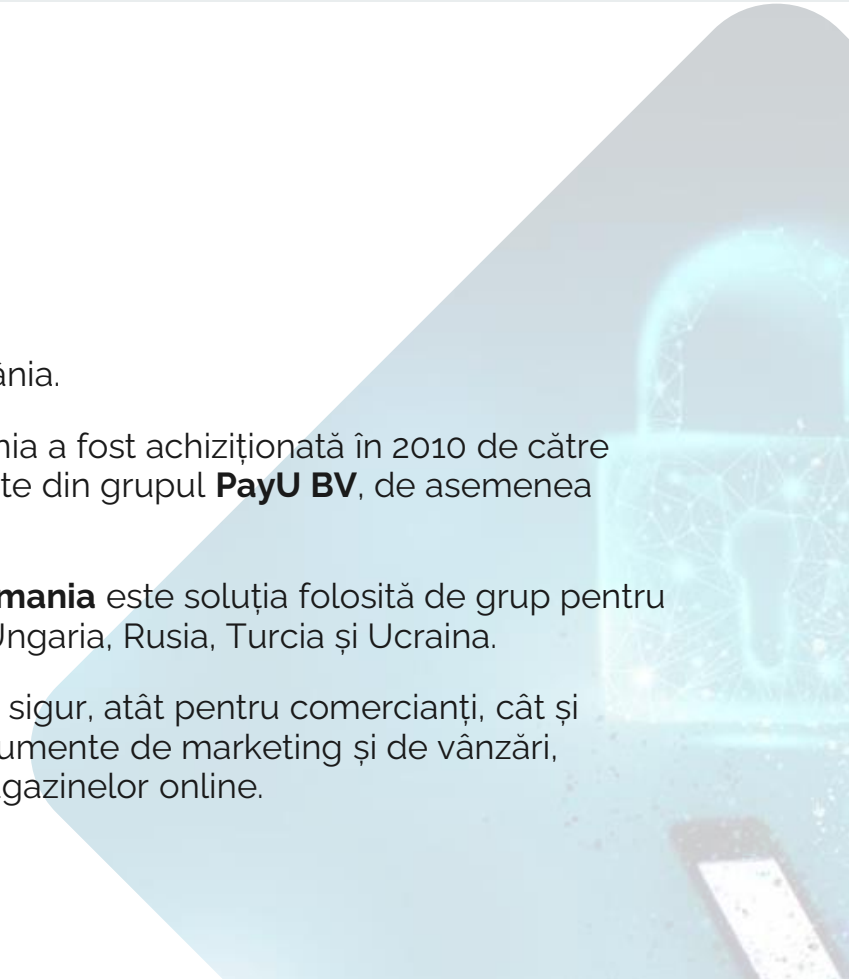
Sisteme electronice de plată

PayU este principalul integrator de plăți online din România.

Lansată în 2004, sub numele **GeCAD ePayment**, compania a fost achiziționată în 2010 de către grupul media internațional Naspers, iar din 2011 face parte din grupul **PayU BV**, de asemenea deținut de Naspers.

Din 2010, platforma dezvoltată și întreținută de **PayU Romania** este soluția folosită de grup pentru extinderea pe piața internațională, fiind operațională în Ungaria, Rusia, Turcia și Ucraina.

PayU oferă un sistem de plată online simplu de folosit și sigur, atât pentru comercianți, cât și pentru utilizatori, un sistem antifraudă la proprietar, instrumente de marketing și de vânzări, precum și multiple funcționalități pentru dezvoltarea magazinelor online.



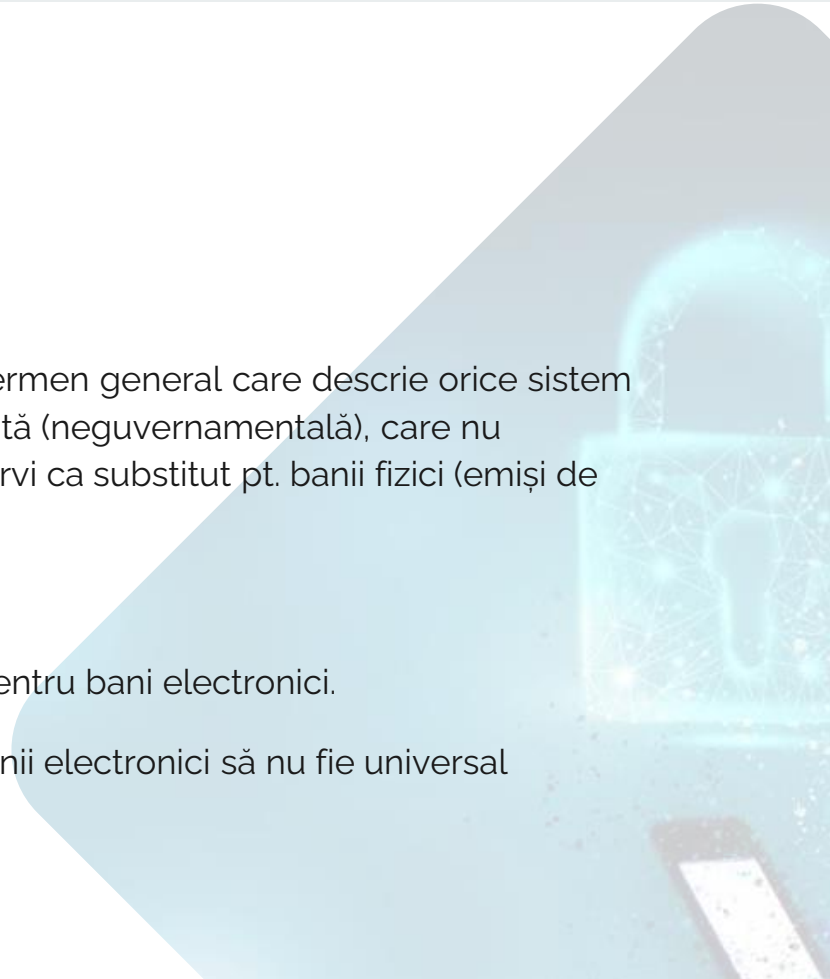
Sisteme electronice de plată

Bani electronici [Electronic cash, e-cash, digital cash] = termen general care descrie orice sistem de stocare și de schimb de valori creat de o entitate privată (neguvernamentală), care nu folosește bancnote și/sau monede fizice și care poate servi ca substitut pt. banii fizici (emiși de instituțiile guvernamentale).

Banii electronici pot fi schimbați în bani fizici, la cerere.

În prezent, nu există o standardizare general acceptată pentru bani electronici.

Fiecare emitent are propriul standard, ceea ce face ca banii electronici să nu fie universal acceptați.



Sisteme electronice de plată

Portofel electronic [electronic wallet, e-wallet] = aplicație software care îndeplinește funcții asemănătoare cu ale unui portofel fizic, adică stochează numere de carduri de plată, bani electronici, date de identificare a proprietarului, informații de contact pt. proprietar, adrese de livrare, etc. și furnizează automat aceste informații site-urilor de comerț electronic în momentul plății (la check-out).

Sisteme electronice de plată

Există două categorii de portofele electronice:

- **Server-side**: informațiile sunt stocate pe un server la distanță.

Avantaje: nu trebuie instalat software e-wallet la client, iar portofelul este disponibil întotdeauna.

Dezavantaj: probleme de securitate.

- **Client-side**: informațiile sunt stocate pe calculatorul clientului.

Avantaj: securitatea.

Dezavantaj: trebuie instalat software e-wallet la client.

Sisteme electronice de plată

Carduri cu valoare stocată [Stored-value cards] = carduri care stochează informații pe o bandă magnetică sau într-un microcip.

Tipuri de carduri cu valoare stocată:

- Carduri cu bandă magnetică [Magnetic stripe cards]
- Carduri inteligente [Smart cards]

Exemple: carduri pt. transport în comun (metrou, autobuz, etc.); carduri pt abonamente la sală; cartele telefonice preplătite, etc.