TRANZACȚII ONLINE ÎN SIGURANȚĂ

Sfaturi esențiale pentru tineri

2025

Disclaimer: Într-o lume tot mai digitalizată, în care plățile și cumpărăturile online au devenit parte din viața de zi cu zi, siguranța tranzacțiilor tale este esențială. Acest ghid are scopul de a te ajuta să înțelegi cum funcționează plățile online, care sunt riscurile asociate și ce măsuri poți lua pentru a-ți proteja datele și fondurile. Vei descoperi bune practici pentru utilizarea cardurilor, platformelor de plată și magazinelor online, precum și metode de recunoaștere a site-urilor și ofertelor nesigure.

Materialul are un rol exclusiv educațional și nu oferă recomandări financiare personalizate. Reglementările și tehnologiile din domeniul plăților digitale pot suferi modificări, așa că îți recomandăm să verifici periodic informațiile și să consulți surse oficiale sau specialiști în domeniu.

ASE și Raiffeisen Bank promovează educația financiară și digitală responsabilă, încurajând tinerii să efectueze tranzacții online în mod conștient, sigur și informat.

Cuprins

În contextul accelerării transformării digitale și al extinderii ecosistemului de plăți către aplicații mobile, portofele electronice, platforme de e-commerce și fintech, tinerii – nativi digital – devin simultan cei mai activi utilizatori și o categorie vulnerabilă la riscuri cibernetice și financiare emergente. Expunerea la scheme sofisticate de inginerie socială (phishing, smishing, vishing, impersonare pe rețele sociale), fraudă de plăți autorizate (APP), utilizarea necritică a linkurilor și codurilor QR, precum și gestionarea deficitară a datelor personale și a autentificării pe dispozitive multiple, amplifică probabilitatea compromiterii conturilor, a identității și a fondurilor.

În acest peisaj, **alfabetizarea financiară și igiena cibernetică** devin competențe de bază, comparabile ca relevanță cu cele digitale generale, aplicarea unor recomandări pentru efectuarea în siguranță a tranzacțiilor financiare online, fundamentate pe bune practici internaționale și pe cerințe de reglementare relevante (de exemplu, autentificare puternică a clientului conform PSD2/PSR, protecția datelor cu caracter personal, reziliența operațională DORA) contribuind la prevenție.

Abordarea îmbină perspectiva tehnică (configurarea securizată a dispozitivelor, gestionarea credențialelor, recunoașterea indicatorilor de compromitere) cu cea comportamentală (decizii informate în situații de presiune temporală, validarea identității interlocutorilor, igienă informațională pe rețele sociale) și cu elemente de protecție juridică și financiară (drepturi ale consumatorilor, proceduri de raportare și recuperare a fondurilor).

Dezvoltarea de competențe operaționale ușor de aplicat, cultivarea unei atitudini critice față de riscurile digitale contribuie la creșterea autonomiei și a rezilienței în gestionarea banilor în mediile online.

1.Verificarea site-urilor și a platformelor de plată

Evaluarea credibilității comercianților și a intermediarilor de plată este premisa fundamentală a tranzacțiilor sigure. Legitimitatea se confirmă printr-o combinație de indicatori tehnici, juridici și reputaționali, iar incongruențele între aceste elemente constituie un risc major.

Indicatori tehnici: utilizați doar site-uri cu conexiune criptată (https), verificați certificatul digital (emis de o autoritate recunoscută, numele domeniului corespunde mărcii), evitați domeniile cu substituții vizuale (ex.: rn în loc de m) sau extensii atipice pentru branduri consacrate.

Exemple: site-ul oficial al unei bănci ar trebui să fie pe domeniul băncii (ex.: banca.ro), nu pe subdomenii generice (ex.: banca-secure-pay.xyz).

Trasabilitate și conformitate: existența unor politici clare de retur, termeni și condiții, identificare fiscală (CUI), adrese și canale de contact verificabile; pentru procesatorii de plăți, mențiuni privind conformitatea Payment Card Industry Data Security Standard (PCI DSS) și listarea publică a partenerilor (Visa, Mastercard).

Exemplu: platformele mari de e-commerce afișează politicile de protecție a cumpărătorului și procedurile de dispută.

Reputație și istoric: consultați recenzii independente și scoruri pe multiple surse (ex.: Google Reviews, forumuri de consumatori, comparatoare de preț), cu atenție la conturile nou-înființate, recenzii identice sau excesiv de laudative postate într-un interval scurt.

Exemplu: un magazin apărut recent cu sute de recenzii aproape identice poate fi indiciu de manipulare.

Comportament la checkout: site-urile legitime nu cer credențiale bancare complete prin e-mail/mesagerie; redirecționează către ferestre securizate ale procesatorului de plăți. Evitați formulare care solicită PIN, parole de internet banking sau coduri OTP pentru „verificare cont".

Mediile de tranzacționare: când accesați marketplace-uri, optați pentru plățile prin mecanisme de escrow/protecție cumpărător, evitați transferurile directe la presiunea vânzătorului („trimite banii prin link de curier").

Exemple: fraudele „curierul" pe platforme de anunțuri folosesc linkuri false care imită pagini de plată.

2. Importanța protejării datelor personale și bancare

Datele personale și financiare au valoare economică directă pentru infractori, fiind utilizate pentru autentificări frauduloase, deschiderea de conturi, împrumuturi sau tranzacții neautorizate. Principiile de minimizare și control al difuzării datelor reduc suprafața de atac.

Minimizați divulgarea: nu partajați CNP, adresa completă, copii de acte sau IBAN în spații publice; furnizați doar datele strict necesare tranzacției. Exemplu: pentru livrare e suficientă adresa și telefonul curierului, nu și CNP-ul.

Segregați identitățile digitale: utilizați e-mailuri dedicate pentru plăți, aliasuri și numere virtuale acolo unde serviciul permite; limitați conectările prin conturi social media la comercianți necunoscuți (reduceți riscul de „account linking" abuziv).

Protejați datele cardului: preferați tokenizarea (Apple Pay/Google Wallet), carduri virtuale sau de unică folosință și limite de cheltuire. Exemplu: setați un card virtual cu plafon zilnic mic pentru abonamente online.

Gestionarea parolelor și a secretelor: folosiți un manager de parole, parole unice și complexe, activați autentificarea multifactor (MFA); nu stocați coduri 3D Secure/OTP în aplicații de notițe necriptate.

Controlul permisiunilor: acordați aplicațiilor bancare doar permisiunile necesare; fiți atenți la solicitări de acces la accesibilitate sau ecran, asociate cu viruși de tip trojan bancar.

Exemple: o aplicație de „scanare documente" care cere acces la SMS poate intercepta coduri OTP, solicitarea de a instala aplicații de remote control pe device motivând necesitatea acordării suportului tehnic.

Drepturi și protecție: cunoașteți drepturile GDPR (acces, ștergere) și politicile băncii privind răspunderea în caz de tranzacții neautorizate; raportați imediat breșele suspectate pentru a limita prejudiciul

3. Semnale de alarmă (phising, oferte false, investiții, aplicații periculoase)

Identificarea precoce a indicatorilor de fraudă reprezintă un element critic al igienei cibernetice, în special în contexte în care atacatorii mizează pe presiune temporală, autoritate aparentă și disimularea canalelor oficiale.

Din perspectivă analitică, semnalele de alarmă pot fi grupate în patru categorii principale: (a) phishing/inginerie socială, (b) oferte comerciale nerealiste, (c) oportunități de investiții "garantate", (d) aplicații malițioase. Fiecare categorie se caracterizează printr-un set recurent de indicatori tehnici și comportamentali.

Phishing / inginerie socială: apel la urgență („cont blocat", „verificare imediată"), solicitarea datelor sensibile (PIN, parole, coduri 3D Secure/OTP), linkuri scurtate sau către domenii care imită brandul, atașamente executabile, spoofing de identitate (nume afișat sau Caller ID fals). Canalele folosite includ SMS, e-mail, mesagerie instant sau apeluri telefonice cu scenarii prestabilite.

Oferte comerciale nerealiste: reduceri excesive, presiuni de tip "numai azi", cerere de plată în afara platformei sau prin link necunoscut, lipsa politicilor de retur/protecție a cumpărătorului. Se exploatează în special marketplace-urile și rețelele sociale.

Investiții „garantate": randamente fixe ridicate, lipsa riscului declarat, promisiuni de retrageri imediate, presiunea de a depune „taxe de deblocare" sau comisioane în avans; deseori implică criptomonede sau platforme nereglementate.

Aplicații periculoase:

Android Package Kit (APK-uri) distribuite în afara magazinelor oficiale, aplicații care cer permisiuni necorelate (Accesibilitate, SMS, ecran), clone ale aplicațiilor bancare sau „actualizări" livrate prin link; includ și fleeceware (abonamente ascunse, costuri recurente greu de anulat).

Exemple de mesaje frauduloase (simulări educaționale)

Notă: *exemplele de mai jos sunt fictive și oferite exclusiv în scop de instruire. Nu urmați astfel de instrucțiuni, nu accesați linkurile și nu divulgați date.*

1.Pretins „de la bancă" – SMS de blocare cont

Text: [Banca]: Contul dvs. a fost SUSPENDAT pentru activitate neobișnuită. Verificați imediat datele: https://banca-verificare-secure.com

Semnale de alarmă

- Domeniu care nu corespunde domeniului oficial al băncii (formă compusă, cuvinte precum „secure", „verify").
- Apel la urgență + sancțiune iminentă.
- Solicitare de „verificare" ce va conduce la pagini care cer date de card sau coduri OTP.

Cum verificați?

- Intrați pe site-ul oficial al băncii sau sunați la numărul de pe site-ul oficial.
- Băncile nu cer niciodată PIN/OTP prin SMS sau linkuri.

2. Pretins „e-mail de securitate" al băncii –atalament malițios

Subiect: Acțiune necesară – extras PDF securizat
Conținut: Stimate client, pentru a preveni suspendarea internet banking-ului, deschideți documentul atașat "Extras_Securizat.zip" și urmați pașii.

Semnale de alarmă

- Atașament arhivă (zip/exe) – vector comun de malware.
- Limbaj generic ("Stimate client"), erori gramaticale fine, lipsa personalizării.
- Amenințare cu suspendarea serviciului.

Cum verificați?

- Băncile comunică în aplicație sau prin documente PDF semnate digital;
- Băncile nu trimit executabile și nu cer instalarea de „actualizări" prin e-mail.

3. Pretins apel telefonic „departament antifraudă” – inginerie socială

Script: “Sunt de la banca X. Observăm o plată de 2.350 lei către Y. Pentru a o anula, am nevoie să-mi dictați codul OTP primit acum pe telefon.”

Semnale de alarmă

- Solicitare de OTP/PIN/parolă la telefon – interzis în bunele practici.
- Presiune temporală (“acum, altfel plata se finalizează”).
- Caller ID poate fi falsificat (spoofing).

Cum procedați?

- Închideți și apelați banca la numărul oficial;
- Verificați în aplicația de mobile banking dacă există o tranzacție în curs;
- Nu divulgați coduri.

4. Oferte false de pe marketplace – „curierul” și plata în afara platformei

Mesaj: “Sunt interesat, plătesc acum. Pentru siguranță, folosiți linkul oficial de curier: *https://livrare-verificata-pay.co* și introduceți datele cardului ca să primiți banii.”

Semnale de alarmă

- Solicitare de date de card „pentru a primi bani”.
- Link care imită pagini ale curierilor, fără conexiune cu platforma reală.

Cum procedați?

- Folosiți doar fluxurile de plată ale platformei;
- Pentru vânzări, nu se cere niciodată datele cardului pentru încasare.

5. Pretins „investitor/analist” – randamente garantate

Mesaj (WhatsApp/Telegram): “Suntem parteneri autorizați ai unei platforme europene. Profit garantat 12% pe lună, retrageri zilnice. Deschideți cont aici: https://eu-invest- secure.net. Pentru bonus, depuneți azi minim 500 EUR.”

Semnale de alarmă

- „Garantat” + randamente nerealiste;
- Presiune de timp, bonus de înscriere.
- Domeniu obscur;
- Lipsa licenței și a detaliilor privind entitatea juridică. Ulterior, pot solicita „taxe de retragere” – un semn clasic de scam.

Cum verificați?

- Consultați registrul autorității de supraveghere (de ex., ASF/EBA/ESMA pentru entități licențiate);
- Nu investiți prin linkuri primite pe chat.

6. Pretins „BNR” – solicitare de actualizare a datelor

SMS/e-mail: BNR: În contextul noilor reglementări, actualizați urgent datele de identitate pentru a evita blocarea conturilor: https://bnr-verificare-id.eu

Semnale de alarmă

- BNR nu contactează clienți bancari și nu colectează date personale pentru conturile acestora.
- Domeniu neoficial, formulare care solicită CNP, CI, selfie cu document/ card.

Cum procedați?

- Ignorați, raportați mesajul băncii și autorităților;
- Orice actualizare KYC (know your customer - procedura de cunoaștere a clientelei) se face prin banca unde aveți contul, pe canale oficiale.

7. Aplicație periculoasă – „actualizare bancă” prin APK

Mesaj (SMS/WhatsApp): „Actualizați aplicația bancară la versiunea de securitate 5.4.
Descărcare: http://banca-app-update.apk”

Semnale de alarmă

- Distribuție în afara magazinului oficial (Google Play/App Store).
- Fișier APK și solicitări ulterioare de permisiuni la SMS/Accesibilitate.

Cum procedați?

- Actualizați exclusiv din magazinele oficiale;
- Dezinstalați aplicațiile necunoscute;
- Rulați un scan și schimbați parolele dacă ați instalat astfel de fișiere.

8. „Informare” falsă despre securitatea depozitelor – abuz de autoritate publică

E-mail: „BNR anunță: din cauza instabilității, transferați economiile în contul de siguranță al programului național până la ora 18:00. IBAN: ROxx...”

Semnale de alarmă

- Autoritățile nu solicită transferuri către „conturi de siguranță”.
- Limbaj incitant la panică, termen-limită artificial.

Cum procedați?

- Ignorați, raportați către banca dvs;
- Consultați doar comunicatele de pe site-ul oficial al BNR și al băncii.

Recomandări operaționale de verificare

- **Verificarea sursei:** nu folosiți linkurile din mesaj; accesați manual site-ul oficial sau aplicația instalată din surse legitime. Confirmați telefonic la numărul oficial (din aplicație/site).
- **Analiza domeniului:** atenție la substituții vizuale (rn vs m), subdomenii lungi, TLD-uri neobișnuite; căutați certificat valid și identitatea organizației în certificat (EV/OV când este disponibil).
- **Conținutul:** căutați greșeli gramaticale, formule generice, promisiuni nerealiste, solicitări de date sensibile sau plăți neobișnuite (vouchere, cripto, carduri cadou).
- **Tehnic:** nu deschideți atașamente .zip/.exe; nu instalați APK-uri; limitați permisiunile aplicațiilor; mențineți sistemul actualizat.
- **Proceduri post-incident:** deconectați dispozitivul de la internet, blocați cardul, schimbați parolele, activați scanarea antimalware, contactați banca și depuneți sesizare la Poliție/DNSC; păstrați dovezile (capturi, header-e, linkuri).

Încorporarea acestor semnale de alarmă în rutina utilizatorului – coroborată cu verificarea prin canale oficiale și cu prudență sporită față de mesaje care invocă autoritatea (banca, "investitori", BNR) – reduce semnificativ expunerea la fraude și întărește reziliența individuală în mediul financiar digital.

4. Utilizarea metodelor sigure de plată și autentificare

Adoptarea consecventă a metodelor moderne de plată (tokenizare, carduri virtuale, 3DS2) și a autentificării rezistente la Phishing (Fast Identity Online / passkeys, semnare tranzacțională cu dynamic linking), dublată de controale operaționale (limite, alerte, geolocație) și disciplină digitală (dispozitive curate, parole unice), reduce semnificativ probabilitatea și impactul fraudelor.

Acest mix tehnologic și comportamental, aliniat cadrului normativ european, constituie fundamentul unei experiențe de plată online sigure și robuste. Selecția instrumentelor de plată și a mecanismelor de autentificare trebuie să echilibreze uzabilitatea cu cerințele de securitate (autentificare puternică a clientului, criptare, control tranzacțional).

Definiții esențiale

Autentificare multifactor (MFA)

Mecanism prin care identitatea utilizatorului este verificată folosind cel puțin doi factori din categorii diferite: cunoaștere (ce știe – parolă, PIN), posesie (ce are – telefon, token, cheie hardware) și inerent (ce este – biometrie).

Exemplu: *confirmarea unei plăți în aplicația bancară prin amprentă (inerent) pe un telefon înregistrat (posesie).*

Autentificare puternică a clientului (SCA, conform PSD2/PSR)

Tip particular de MFA aplicat plăților electronice în UE, care impune combinarea a cel puțin doi factori independenți și „dynamic linking" – legarea criptografică a autentificării de suma și beneficiarul tranzacției.

Exemplu: *aprobarea unei plăți către IBAN specific, valoare 250 lei, vizibile pe ecranul de autorizare.*

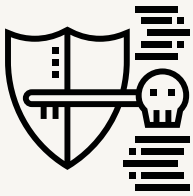
3D Secure (versiunea 2.x)

Protocol de autentificare pentru plăți cu cardul pe internet, care permite „step-up" (autentificare suplimentară) la risc crescut și fluxuri mai ergonomice (ex. notificare push în aplicație). Înlocuiește parole statice cu autentificare contextuală.

Tokenizare

Înlocuirea datelor sensibile (de ex. PAN – numărul cardului) cu un token (ex. DPAN pentru plăți mobile), inutilizabil în afara contextului propriu.

Exemplu: *la Apple Pay/Google Wallet, comerciantul primește un token, nu numărul real de card.*



Chei FIDO2 /WebAuthn (passkeys)

Metode de autentificare criptografică fără parolă, rezistente la phishing, bazate pe perechi cheie publică/privată stocate în dispozitiv sau chei hardware; confirmarea se face local (PIN/biometrie).

OTP (One-Time Password)

Coduri unice, cu valabilitate limitată, trimise prin SMS, generate în aplicații sau tokenuri. Sunt utile, dar mai vulnerabile la nterceptare/ingenierie socială decât notificările push sau FID02.

Semnare tranzacțională

Confirmarea unei tranzacții prin generarea unei semnături criptografice care include atributele esențiale (sumă, beneficiar). Implementări: TAN-uri dinamice, QR-TAN, challenge-response în aplicația băncii.

4.1. Metode de plată recomandate și controlul riscului

- **Carduri cu 3D Secure 2 și SCA:** standardul minim pentru plăți online cu cardul în UE.
  Exemplu: la checkout, sunteți redirecționat către o pagină de autorizare a băncii sau primiți o notificare push în aplicație pentru aprobare.

- **Portofele digitale cu tokenizare (Apple Pay, Google Wallet):** reduc expunerea datelor de card; tranzacțiile sunt autorizate local (biometrie) și protejate de un „secure element".
  Exemplu: plata pe un site acceptat prin butonul „Pay with Apple Pay".

- **Carduri virtuale și de unică folosință:** generate din aplicația băncii/fintech-ului pentru abonamente sau comercianți noi; pot avea limite scăzute sau valabilitate limitată.
  Exemplu: card virtual cu plafon de 100 lei pentru o singură achiziție.

- **Mecanisme escrow/protecție cumpărător:** pe marketplace-uri consacrate, plata rămâne reținută până la confirmarea livrării; reduce riscul de neconformitate.
  Exemplu: „Payments" ale platformei care permite deschiderea disputei și recuperarea sumelor.

- **Transferuri bancare cu verificare beneficiar (SANB):** confirmați identitatea beneficiarului prin canal secundar; utilizați liste de „beneficiari de încredere" și verificări suplimentare (name check, acolo unde banca oferă).

- **Plăți instant (SEPA Instant) cu notificări:** oferiți-vă alerte în timp real pentru a detecta imediat tranzacții neautorizate; pentru plăți P2P, confirmați verbal detaliile cu destinatarul.

- **Plăți prin coduri QR verificate:** scanați doar coduri generate în aplicații oficiale (banca, comercianți certificați); vizualizați datele tranzacției (beneficiar, sumă) înainte de confirmare.

4.2 Practici de autentificare sigure și exemple concrete

Preferința pentru autentificare rezistentă la phishing

Alegeți passkeys/FIDO2 sau aprobări prin aplicația băncii cu afișarea clară a sumei și destinatarului. Exemplu:

- Cheie hardware (YubiKey) pentru login la fintech și semnare tranzacții;
- Evitați OTP prin SMS când aveți opțiune de push/biometrie; OTP poate fi sustras prin SIM swapping sau malware care citește SMS-uri.

Izolarea dispozitivului de autorizare

- Nu folosiți dispozitive „rootate/jailbreak”; activați blocarea biometrică și criptarea.
- Separați profilul de utilizare pentru plăți de cel de test/aplicații neesențiale.

Dynamic linking și atenție la ecranul de autorizare

- Nu folosiți dispozitive „rootate/jailbreak”; activați blocarea biometrică și criptarea.
- Separați profilul de utilizare pentru plăți de cel de test/aplicații neesențiale.

Exemplu: *dacă autorizați 2.500 lei către „SC EXEMPLE SRL” dar intenționați 250 lei către alt beneficiar, anulați imediat – e un semnal de redirecționare frauduloasă.*

Politici de parole și manager dedicat

- Parole unice, lungi, generate în manager de parole;
- MFA activ pentru conturile de e-commerce și e-mail (piesa centrală a recuperării).
- Evitați reutilizarea parolelor între bancă și alte site-uri.

4.3 Configurări de control tranzacțional

Limite și geolocalizare

- Setați plafoane zilnice/săptămânale, dezactivați plățile online sau contactless când nu le folosiți;
- Blocați geografic tranzacții din regiuni unde nu operați.

Alerte și aprobări explicite

- Activați notificările push/SMS pentru fiecare plată;
- Cereți aprobare în aplicație pentru tranzacții peste un prag.

Liste albe/negre

- Uilizați liste de comercianți de încredere;
- Blocați comercianți recurenți nedoriți sau MCC-uri specifice atunci când banca oferă această granularitate.

Monitorizare comportamentală și step-up

- Acceptați „challenge”-uri suplimentare atunci când banca detectează risc crescut (dispozitiv nou, locație neobișnuită); aceste mecanisme de control vă protejează contul.

4.4. Scenarii uzuale și soluții

Cumpărături la comercianți noi

- Folosiți card virtual cu plafon mic + 3DS2;
- Verificați domeniul și certificatul site-ului. Dacă se solicită salvarea obligatorie a cardului, renunțați.

Abonamente și „free trial"

- Utilizați carduri dedicate sau tokenizate;
- Setați mementouri înainte de termenul de facturare;
- Verificați opțiunile de anulare în cont.

P2P și marketplace

- Folosiți protecția cumpărătorului;
- Refuzați linkuri de plată trimise prin mesagerie;
- Nu introduceți datele cardului „ca să primiți banii".

Plăți către entități „de investiții"

- Confirmați licențierea pe registrele autorităților (ASF/ESMA/EBA);
- Evitați transferuri în cripto la presiunea „consilierilor".

4.5 Greșeli frecvente de evitat

Divulgarea codurilor OTP la telefon: „agentul antifraudă” cere OTP pentru anulare – este fraudă. Banca nu solicită OTP/PIN/parole prin telefon sau chat.

Instalarea de APK din linkuri: „actualizați aplicația băncii” prin WhatsApp – poate instala viruși de tip trojan bancar care interceptează SMS și suprapun ecrane.

Autorizarea în orb: aprobarea notificărilor push fără a citi detaliile tranzacției („push fatigue”). Verificați întotdeauna suma/beneficiarul.

Reutilizarea parolelor: compromiterea unui magazin online duce la credential stuffing” pe e-mail și apoi pe contul bancar.

4.6.Proceduri de răspuns în caz de suspiciune

Blocați imediat instrumentul (card, portofel) din aplicația băncii; activați „freeze” temporar dacă nu sunteți sigur.

Contactați banca pe canalul oficial și raportați incidentul; solicitați contestarea plății (chargeback acolo unde se aplică).

Schimbați parolele, revocați sesiunile active, dezactivați dispozitive necunoscute din setările contului.

Notificați autoritățile competente (Poliție, DNSC) și păstrați probele (capturi de ecran, e-mailuri, URL-uri, loguri).

FUNDAȚIA ACADEMIEI DE STUDII ECONOMICE
București, România
Fondată în 2013

Tranzacții online

Raiffeisen Bank