Finanțat de
Uniunea Europeană

BUNELE PRACTICI ÎN COMBATEREA FRAUDELOR BAZATE PE SCENARII DE INGINERIE SOCIALĂ

Raluca Micu
Serviciul Monitorizare a plăților și a instrumentelor de plată
Chișinău, 6 Decembrie 2023

PROIECTUL TWINNING:
MD 20 ENI FI 01 21R2 (MD/36) „CONSOLIDAREA SUPRAVEGHERII, GUVERNANȚEI CORPORATIVE ȘI GESTIONĂRII RISCURILOR ÎN SECTORUL FINANCIAR"
TWINNING

1. Rolul băncii centrale

Banca Națională a României *reglementează, autorizează, supraveghează și monitorizează sistemele de plăți și instrumentele de plată, în vederea promovării funcționării sigure și eficiente a acestora, cu scopul menținerii încrederii publicului în sistemul financiar.*

monitorizarea și evaluarea instrumentelor de plată, aranjamentelor de plată și schemelor de plată

formulează recomandări și măsuri de remediere, precum și termene de implementare

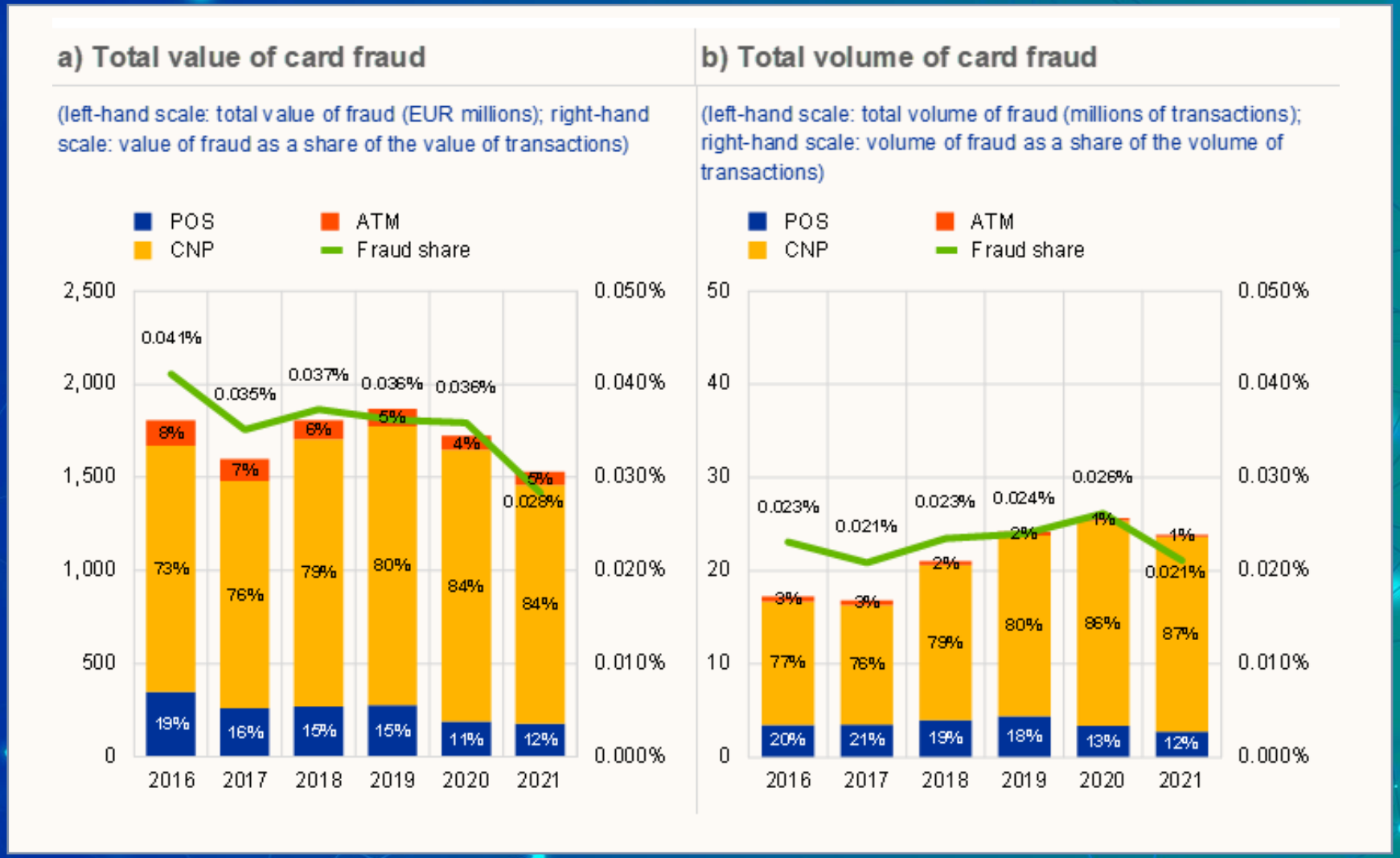
gestionează și soluționează plângerile utilizatorilor serviciilor de plată, referitoare la potențiale încălcări ale securității plăților

autorizează punerea în circulație a instrumentelor de plată, funcționarea aranjamentelor/schemelor de plată

evaluarea măsurilor de securitate implementate pentru gestionarea riscurilor TIC și de securitate

cooperează cu Autoritatea Bancară Europeană și alte autorități naționale relevante din statele membre cu privire la incidentele operaționale și de securitate majore

2. Date statistice privind fraudele



Sursa: https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230526~f09bc3c664.en.html

3. Securitatea plăților

Autentificarea strictă cu doi factori - SCA

Prestatorii de servicii de plată aplică autentificarea strictă a clienților atunci când plătitorul:

a) își accesează online contul de plăți;

b) inițiază o operațiune de plată electronică;

c) întreprinde orice acțiune, printr-un canal la distanță, care poate implica un risc de fraudare a plății sau alte abuzuri.

- art. 220 din Legea 209/2019 privind serviciile de plată

Ceva ce doar utilizatorul cunoaște	Ceva ce doar utilizatorul posedă	Ceva ce reprezintă utilizatorul
		
- Parola statică - Codul PIN	- OTP SMS - Dispozitivul mobil asimilat	- Recunoaștere facială - Scanarea amprentei

Prin urmare, se aplică SCA atunci când:

a) înrolăm un card într-un portofel digital;

b) instalăm o aplicație de mobile banking pe un dispozitiv inteligent;

c) ne autentificăm în aplicațiile de internet & mobile banking;

d) autorizăm operațiunile de plată inițiate cu cardul;

e) autorizăm operațiunile de transfer credit inițiate electronic (prin internet & mobile banking);

f) autorizăm operațiunile de debitare directă inițiate electronic (din browser sau aplicații mobile).

4. Scenarii de fraudă

Exemple de tehnici de fraudare

Atacatorul fură elementele de securitate ale victimei:
- phishing/smishing/vishing
- spearphishing (phishing țintit)
- spoofing
- pagina de Internet Banking sau de inițiere plăți clonată

Victima este păcălită și autorizează plata:
- inginerie socială
- manipularea plătitorului
- atac ‘omul din mijloc’

Orice mijloace de comunicare

Tentativă de fraudă pe OLX, sesizată de CERT-RO / Capcana întinsă de atacatori prin care vor să obțină datele cardului / Avertismentele specialiștilor: Tot mai multe incidente de phishing și pe WhatsApp

ENERGIE Joi, 02 Noiembrie 2023, 14:16

Știri false și atacuri de tip phishing care promit câștiguri mari cu acțiuni Transgaz. Compania avertizează că este o fraudă

Florentina Cernat • HotNews.ro

3

Transgaz atrage atenția cu privire la existența în mediul online a unor știri false și atacuri de tip phishing care se bazează pe promisiuni false de câștiguri rezultate din tranzacționarea acțiunilor companiei pe diverse platforme nelegitime. Pe rețelele sociale circulă tentative similare de fraudă care implică imaginea Hidroelectrica și Solar City, una dintre companiile cumpărate de Elon Musk.

Cum funcționează cea mai recentă fraudă prin SMS. Anunțurile false despre angajare prin care sunt furate date bancare

Autor: Irina Chirtoc Miercuri, 23 Februarie 2022, ora 20:18 4254 citiri

Atacatorii pot extrage date personale și financiar-bancare de la utilizatori FOTO Pixabay

Directoratul Național de Securitate Cibernetică a atenționat miercuri, 23 februarie, asupra unor propuneri primite de utilizatori pe aplicațiile de mesagerie sau prin SMS care prezintă oportunități de angajare sau de investiții cu câștiguri rapide.

"Atenție la propunerile primite prin intermediul aplicațiilor de mesagerie sau sms, care vă prezintă oportunități de angajare sau de investiții ce promit câștiguri rapide! Unii utilizatori din România au început să primească astfel de mesaje:"Buna, ati fost selectat pentru un job part-time/full time, mai mult de 900 de zile. accepta acest post vacant -LINK-." Mesajul primit are și un link care, odată accesat, redirecționează utilizatorul către aplicația de mesagerie WhatsApp și deschide o conversație cu infractorii cibernetici din spatele acelui contact. În urma

Cum a rămas o femeie fără 2.000 de lei pentru un colet prin „Poșta Română”. Hackerii au clonat site-ul oficial

STIRI ACTUALE 04-05-2023 | 20:06

Numele Poștei Române, dar și al altor companii de curierat este tot mai folosit de hackeri în campanii înșelătoare. Diverși oameni au primit pe telefoanele mobile mesaje care îi îndeamnă să acceseze o pagină de internet care seamănă cu cea a Poștei Române

Analiză Binance: Fraudele de tip „Pig Butchering” s-au dublat în ultimul an

NUMĂRUL 36, 13-19 SEP. 2023 » CONECTAREA LA ERA DIGITALĂ

Tweet

Tentativele de fraudă tip „Pig Butchering”, care vizează utilizatori neexperimentați atrași de hackeri cu promisiuni de randamente mari, s-au dublat în ultimul an (+100,5%), avertizează platforma globală de schimb de criptomonede Binance, într-o analiză citată de Agerpres. "Manipulatorii intră în grațiile victimelor construind în timp un sentiment de încredere, studiindu-le îndeaproape și arătându-le profiturile inițiale ale investiției lor. Odată ce încrederea victimelor este câștigată și investesc sume mai mari de bani pe platforma frauduloasă, escrocii dispar brusc cu fondurile victimelor. Frauda poartă numele de «Pig Butchering», deoarece escrocii «îngrașă victimele» cu câștiguri false înainte de a le «sacrifica» pentru restul banilor lor. Este important de reținut că tehnici similare au fost folosite de ani de zile în diverse tipuri de fraudă, iar consumatorii trebuie să fie conștienți că aceste escrocherii nu se limitează la spațiul cripto", explică specialiștii.

Tweet

Polițiștii au blocat o fraudă bancară de 11.700 de euro, realizată prin accesarea ilegală a unui sistem informatic

Autor: Andreea Năstase
Publicat: 02/06/2020 15:40
Sursa foto: facebook.com

Polițiștii clujeni au reușit să blocheze transferul ilegal al sumei 11.700 de euro din conturile unei asociații, realizat prin accesarea ilegală a unui sistem informatic.

5. Tipuri de fraudă

Phishing, Spoofing

Vânzarea de produse/ servicii fictive

Fraude de investiții/ 'Pig butchering'

Furtul identității/ Uzurparea contului

Compromiterea adresei de e-mail de muncă

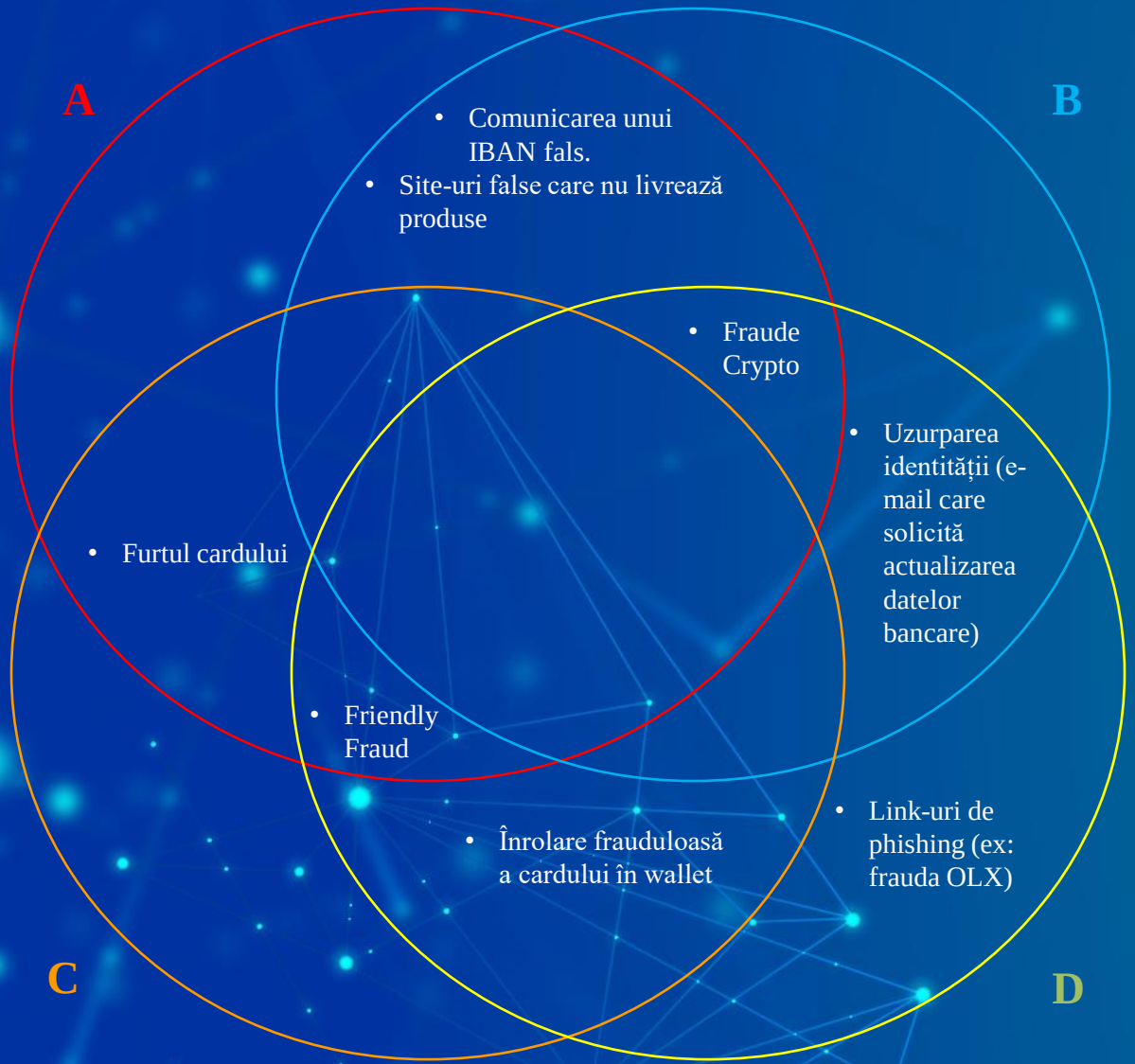
Atacuri prin acces la distanță

Facturi fictive

Fraude cu plată (comision/taxă) anticipată

Romance scams

6. Bune practici pentru prevenirea fraudelor



A – Monitorizare în timp real

Trendul crescător al plăților efectuate în timp real impune necesitatea unei monitorizări a tranzacțiilor în timp real.

Stabilirea criteriilor cu scopul identificării operațiunilor de plată potențial frauduloase, cum ar fi dar fără a se limita la:

- numărul operațiunilor de plată inițiate consecutiv într-un anumit interval de timp;
- categoria de comercianți;
- conturi IBAN și comercianți în black-list;
- istoricul tranzacțional al clientului;
- valoare anormală a tranzacției;
- zona geografică.

B – SANB

Serviciul **A**fișare **N**ume **B**eneficiar este un serviciu pus la dispoziție participanților Transfond. Obligatoriu prin recomandarea BNR și în viitor prin PSD3 și Regulamentul privind plățile instant în euro.

C – SCA

Autentificare strictă cu doi factori: cunoaștere, posesie, inerență.

D – Educarea utilizatorilor

Campanii de educare inițiate de bănci;

Comunicate BNR;

Informarea utilizatorului cu privire la utilitatea codului OTP (exemplu SMS: “NU comunica NIMANUI acest cod! Introdu-l doar in APLICATIA WALLET din iPhone pentru a face plati POS sau online prin Apple Pay. Codul pt card **** este *****.”)

6. Cum evităm fraudele?

securizează-ți dispozitivele

stai informat

păstrează în siguranță elementele de securitate personalizate

schimbă-ți parolele la orice suspiciune

verifică autenticitatea adresei de e-mail înainte de a da curs solicitărilor primite

monitorizează frecvent activitatea contului tău

verifică autenticitatea website-ului înainte de a accesa sau a oferi date

ferește-te de promisiuni nerealiste

citește notificările băncii privind noile metode de fraudare

verifică cu atenție informațiile de pe facturile primite

7. Trenduri și tipare noi de fraudă

Tehnologia AI

Beneficii

- Instituțiile financiare încep să utilizeze tehnologia AI cognitivă din ce în ce mai mult (ex: biometrie comportamentală, detecția de phishing, securitate adaptivă)

Reversul medaliei

- Vulnerabilitățile specifice (ex: vulnerabilități cunoscute ale librăriilor open-source, 'otrăvirea' datelor de antrenament, alterarea predicțiilor)
- Utilizarea tehnologiei AI în scopuri alternative a escaladat. Tehnologia AI a ajuns la îndemâna oricui iar atacatorii utilizează AI generativ pentru atacuri de fraudă pe scară largă și din ce în ce mai complexe.

Exemple de atacuri bazate pe tehnologia AI:

- *deepfake*-uri care pot manipula clienții
- keystroke monitoring malware
- e-mail-uri de phishing sofisticate
- scrierea de programe malițioase (ex: ransomware) accesibilă oricui

Alte trenduri de fraudă în creștere

- Uzurparea contului
- Furtul identității sintetice din ce în ce mai greu de detectat
- Înșelătorii cu investiții în criptomonede
- *Fraud as a service*, datorită dezvoltării rețelelor de crimă cibernetică
- Inginerii sociale, inclusiv în contextul muncii de la distanță

Mulțumesc!

Q&A