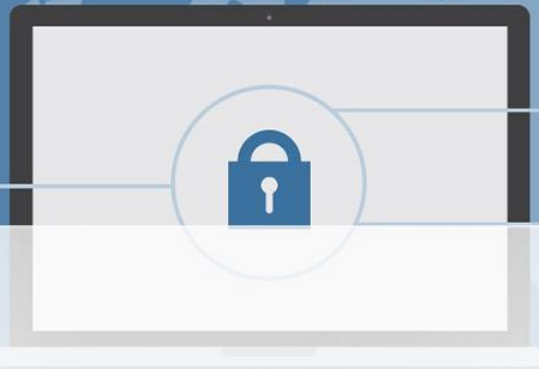
# Securitatea plăților pe internet

Proiect realizat de : Sajina Arina și Gopleac Olivia

# Cuprins



# Amenințările informatice

- Malware
- Troian
- Keyloggers
- Adware

# Atacurile pot fi de 3 tipuri:

- 1. Drive-by-download
- 2. Main-in-the-middle
- 3. Main-in-the-browser

# Ameninţări de tip inginerie socială

Ingineria socială este arta de a manipula, minţi, sau influenţa pe ceilalţi ca să realizeze/nu realizeze anumite acţiuni ori să divulge informaţii confidenţiale.


Tipurile de inginerie socială sunt:

1. PHISHING
2. SMSishing

# Ce înseamnă:

- PHISHING
- SMSishing

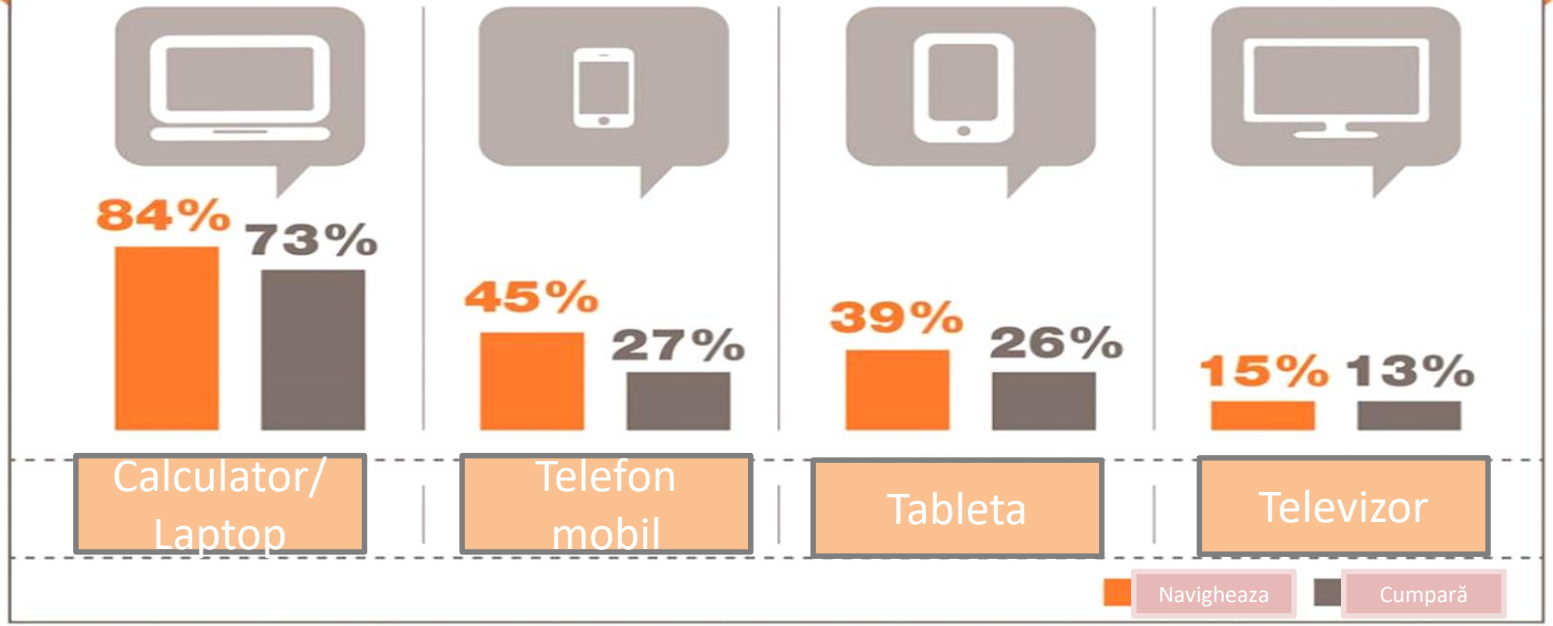
# Metodele de obținere a informației private prin mijloace ilegale sunt:

- Sms-shing
- Phishing
- Vishing(voice+phishing)
- Ceo fraud/BEC

# Sfaturi de prevenire a acestor situații neplăcute

- ✓ Evitați să folosiți corespondența electronică neprotejată pentru vehicularea informațiilor cu caracter confidențial (coduri IBAN, parole, detalii de plată, etc);
- ✓ Folosiți întotdeauna softuri antivirus pentru protecția calculatoarelor dvs;
- ✓ NU efectuați plăți către conturi noi pe care nu le-ați mai utilizat
- ✓ În situația în care ați efectuat o plată către un cont eronat, contactați urgent banca dvs. pentru a putea afla dacă mai sunt posibile demersuri de blocare/returnare a sumelor implicate;
- ✓ Înștiințați cât mai rapid organele de poliție locale

# Procentajul consumatorilor ce folosesc aparate electronice să navigheze pe internet sau sa facă cumparaturi online



# Fraude la vânzarea online a produselor

Pentru a preveni astfel de situații, vă recomandăm să:

- nu efectuaţi tranzacţii decât pe platformele cunoscute de intermedieri online
- verificaţi cu atenţie reputaţia cumpărătorului şi ce tranzacţii a efectuat în trecut
- comunicaţi cu partenerul de afaceri şi pe alte canale nu doar pe email (ex. telefon, video-call)
- verificaţi cu atenţie termenii şi condiţiile platformei care intermediază vânzarea
- vă informaţi cu privire la riscurile care pot apărea în urma unei astfel de tranzacţii.

# Ameninţări privind utilizarea serviciilor de plată pe internet

1. Întotdeauna navigaţi pe siteul oficial şi folosiţi linkurile de acolo.

2. Verificaţi cu atenţie dacă atunci când desfăşuraţi operaţiuni financiare (transferuri sau plăti cu cardul) conexiunea utilizată este una securizată (https://).

3. Activaţi opţiunea de blocare a ferestrelor pop-up. Nu daţi click pe “Agree” sau “OK” pentru a închide o fereastră.

4. Dezactivaţi salvarea parolelor.

!!! Banciile NU apelează (telefonic, email sau SMS) la clienţii săi pentru a cere informaţii precum: CNP, număr card, PIN, ID logare, parola, cod token sau orice alte informaţii personale.

# Ameninţări privind plăţile cu cardul

La efectuarea unei tranzacţii pe internet sunt necesare o multitudine de date.

Parola 3D-Secure sau codul unic OTP sunt elemente de siguranţă, de antifrauda, dezvoltate de VISA şi MasterCard. Folosirea acestui sistem permite creşterea securităţii tranzacţiilor online, deoarece ambele sunt solicitate la fiecare comandă online prin sistemul 3D Secure.

# Ameninţări privind utilizarea reţelelor wireless (WiFi)

Reţele Wi-Fi gratuite (restaurant, cafenele, aeroporturi) sunt cele mai vulnerabile dacă nu sunt securizate corespunzător. Atunci când vă conectaţi la o reţea nesecurizată orice persoană aflată în raza de acţiune a reţelei ar putea intercepta traficul dvs. şi “vedea” anumite informaţii ce au fost transmise nesecurizat.

# Cum verifici dacă un site este sigur?

Browserele web moderne, printre care Chrome, marchează site-urile care nu oferă conexiune securizată. Astfel, la fiecare accesare in browser, în partea stângă a linkului apare un semn specific.

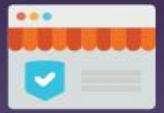
Aceste semne sunt diferite și semnifică:

- Securizat
- Informații
- Nesecurizat
- Periculos

CE SĂ FACI

## Cumpără din surse sigure.

Cumpără de la firme sau magazine pe care le cunoști sau pe care le-ai folosit și verifică rating-ul vânzătorilor pe site-urile de comerț online.



## Fii atent la plățile recurente (automate).

Înainte de a furniza datele cardului pentru a plăti un serviciu cu reînnoire, informează-te cum poți să încetezi serviciul plăților recurente.

Mulți comercianți online îți vor cere să stocheze informațiile tale de plată.


**Gândește-te de două ori înainte să iei o decizie și fii sigur că ai înțeles riscurile pe care le implică.**

## Folosește carduri de credit atunci când cumperi online.


Majoritatea cardurilor de credit au politici stricte în ceea ce privește siguranța clienților. Dacă nu primești ce ai comandat, emitentul cardului îți va returna banii.

## Asigură-te că transferul informațiilor se face în mod securizat.

Verifică existența simbolului de tip lacăt în bara URL și folosește un protocol HTTPS sau SSL atunci când navighezi pe internet.

https

## Păstrează întotdeauna documentele referitoare la plățile pe care le-ai efectuat online.

Acestea pot fi folosite pentru stabilirea termenilor și condițiilor vânzării sau pentru a face dovada că ai plătit pentru bunuri.

# REGULI DE AUR

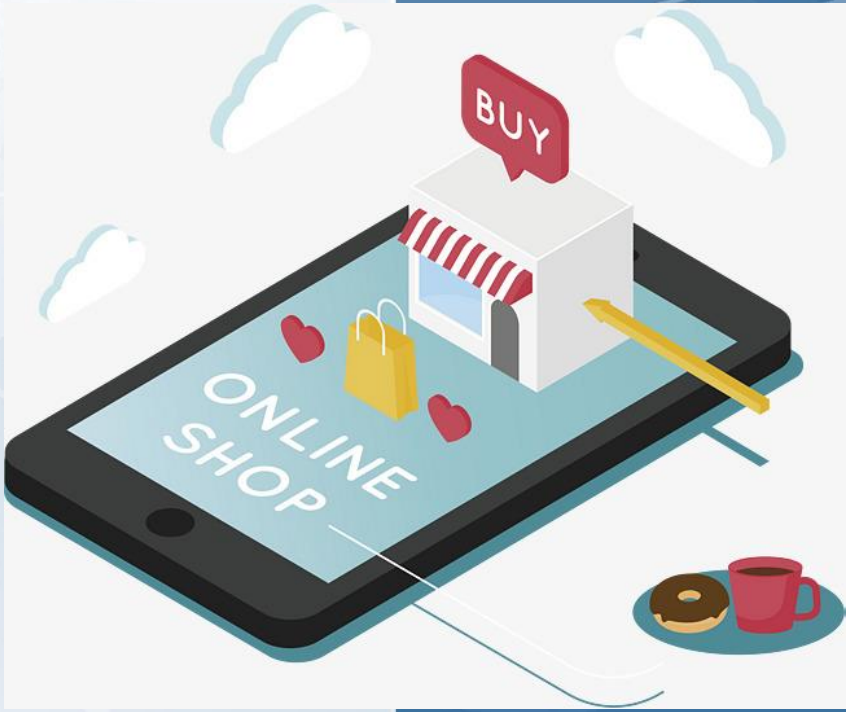
## CUMPĂRĂTURI ONLINE SIGURE

EUROPOL EC3 European Cybercrime Centre

POLIȚIA ROMÂNĂ

# Concluzie

- Plățile efectuate pe internet au o multitudine de riscuri ce trebuie luate in considerație. Cu dezvoltarea tehnologiilor evolueaza si metodele de fraude online a informațiilor private. Asfel cunoașterea riscurilor si protejarea contribuie la securizarea informației.



# Bibliografie


1) http://www.arb.ro/wp-content/uploads/ARB-Ghid-Securitate-Plati-Internet-noiembrie-2016.pdf
2) https://www.mxhost.ro/chrome-cum-verifici-daca-un-site-este-sigur/


# Vă mulțumim pentru atenția acordată!