



SECURITATEA PLATIILOR PE INTERNET



Realizat de: Margarint Nicoleta;
Chitaica Loredana.

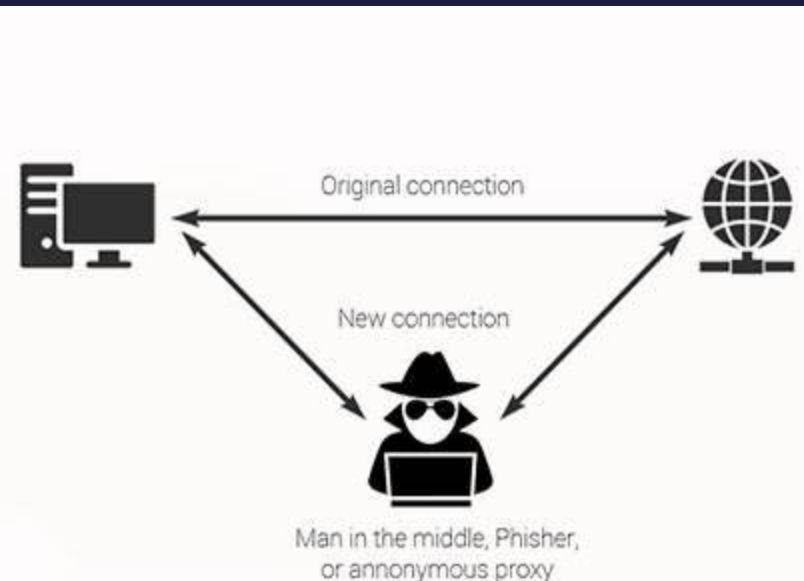
Amenințările ce pot apărea în timpul unei plăți

- **Malware** (prescurtarea de la "malicious software" în limba engleză) este un termen generic și se referă la orice software rău-intenționat (malicios) care a fost creat cu scopul de a rula în mod neautorizat și ascuns față de utilizatorul computerului.
- Înregistratoarele de taste, **keyloggers** în limba engleză, sunt programe destinate înregistrării tastelor apăsate de către utilizator și folosite pentru a obține informații sensibile ca parole, coduri PIN, numere de carduri. Aceste programe rulează în background și sunt invizibile.

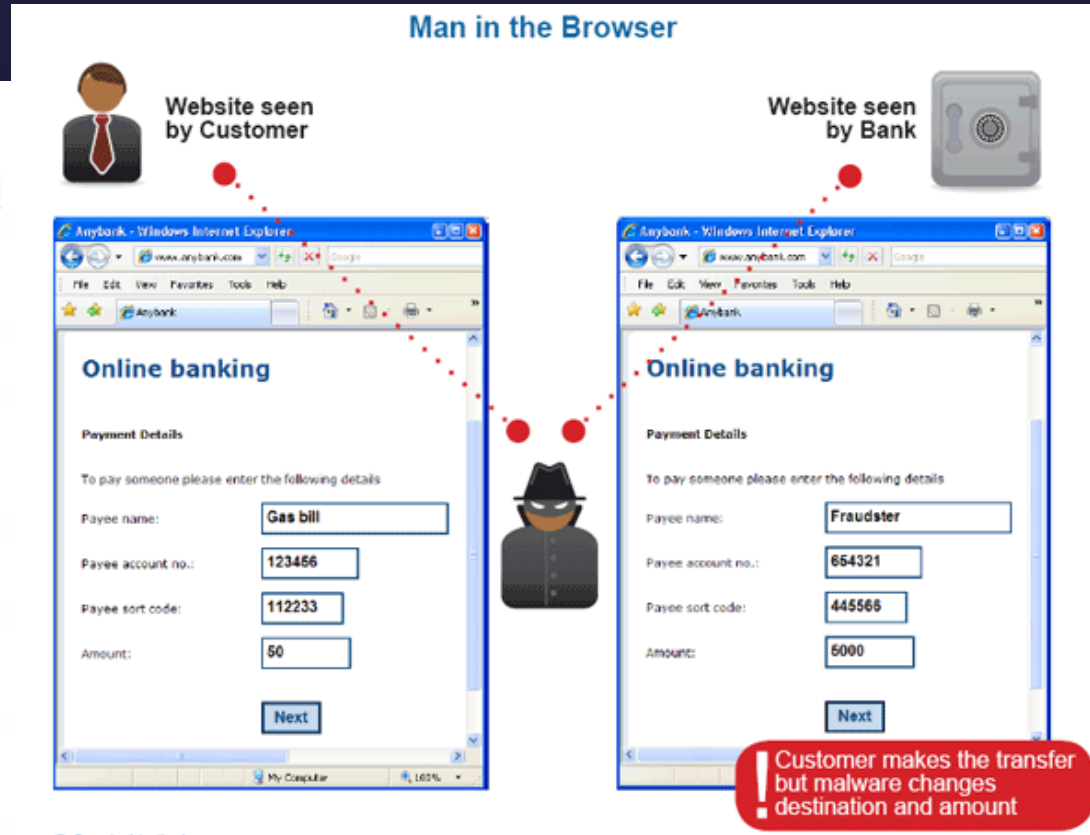


Tipuri de atacuri

- Un atac de tip **"drive-by-download"** se referă la descărcarea ne-intentionată (fără știința utilizatorului) și fără ca acesta să observe, pe un computer sau terminalul mobil, a unor programe malițioase.
- Un atac de tip **"man-in-the-middle"** (omul de la mijloc), este un atac sofisticat în care atacatorul se interpune ca "stație de transit" în comunicația dintre două sisteme. Atacatorul controlează toată conversația, fiind capabil să intercepteze și modifice mesajele schimbate de cele două părți. Folosind un astfel de atac atacatorul ar putea modifica date ale unor tranzacții financiare.



Un atac de tip **“man-in-the-browser”** este un tip de atac “man-in-the-middle” prin care un troian (program malitios prezentat ca un program legitim) infectează un browser web folosindu-se de vulnerabilitățile de securitate ale browser-ului. Atacatorul modifică pagini web, elemente ale unei tranzactii sau chiar întreaga tranzactie, toate aceste actiuni având loc “în background”, fără ca utilizatorul să observe.



Procese prin care se realizeaza activitati criminale in sistmele informatice

- În domeniul informatic, **phishing** (eng) reprezintă o formă de activitate criminală care constă în obținerea datelor confidentiale, cum ar fi credentialele de acces (username, parola, PIN, OTP) pentru aplicatii financiare sau informatii referitoare la cardul de credit, folosind tehnici de manipulare a identității unei persoane sau a unei institutii.
- Un atac de tip phishing constă în trimiterea de către atacator a unui mesaj electronic, folosind programe de mesagerie instantă (e-mail) – **PHISHING**, sau telefon (SMS) - **SMSishing**, în care utilizatorul este sfătuit să introducă credentialele de access (nume utilizator, parola), numere de card, coduri PIN.



- Un exemplu de *phishing*: primiți un email în care ați fost informat că ați câștigat o excursie în străinătate iar tot ce trebuie să faceți pentru a primi voucherul de călătorie este să introduceți (pe un site asemănător cu cel al băncii) următoarele informații pentru a confirma identitatea: numele, adresa și datele cardului dvs.
- Exemplu de *smsihing*: primiți un mesaj SMS de la un număr necunoscut care pretinde a fi banca dvs. și care va invită să descărcați o nouă versiune a aplicației de mobile banking.
- **Vishing** este un termen care provine din termenii voice și phishing și reprezintă o formă de înșălătorie prin care utilizatorul este păcălit să furnizeze informații sensibile, credențialele de acces, numere de card, sau coduri de acces.



Pentru efectuarea unei tranzacții online sau unei plăți, vă recomandăm să:

- nu efectuați tranzacții decât pe platformele cunoscute de intermediari online;
- verificați cu atenție reputația cumpărătorului și ce tranzacții a efectuat în trecut (atunci când este posibil);
- comunicați cu partenerul de afaceri și pe alte canale nu doar pe email (ex. telefon, video-call);
- verificați cu atenție termenii și condițiile platformei care intermediază vânzarea;
- vă informați cu privire la riscurile care pot apărea în urma unei astfel de tranzacții;

De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de înșelătorie să înștiințați cât mai rapid organele de poliție locale.

Dispozitivile folosite de dvs. pentru efectuarea tranzactiilor electronice reprezintă elemente importante ce trebuie securizate. Adesea prin compromiterea lor, atacatorii reusesc să desfășoare tranzactii frauduloase si să obțină câștiguri materiale (în defavoarea dumneavoastră). Va recomandam următoarele masuri:

Calculator

- Instalați pe calculatorul dumneavoastră numai aplicații cu licență validă și care provin din surse sigure;
- Instalați o soluție de securitate ce oferă cel puțin protecție anti-virus;
- Nu conectați dispozitive necunoscute la calculatorul dumneavoastră (de ex. stick-uri USB găsite în locuri publice);
- Dezactivați conexiunile de rețea pe care nu le utilizați, opțiunile wireless – WiFi, Bluetooth;
- Nu uitați să efectuați copii de siguranță pentru datele dvs. pe un suport extern (backups) în mod periodic;
- Nu folosiți alte computere care nu vă aparțin (la Internet Café, hotel, aeroport sau la “prieteni”) atunci când faceți tranzacții bancare.

Tableta/smartphone

- Protejați accesul la smartphone-ul sau tableta dumneavoastră folosind una din opțiunile de securitate disponibile (PIN, parola, sau “semn grafic”);
- Actualizați sistemul de operare de pe smartphone-ul sau tableta dumneavoastră (Android, iOS, Windows);
- Instalați aplicații (Apps) doar din magazinele de aplicații oficiale (Google Play, Apple App Store, Microsoft Store);
- Dezactivați opțiunile de conectivitate (Wi-Fi, Bluetooth, NFC, etc) pe care nu le utilizați în mod curent.

Amenințări privind utilizarea serviciilor de plată pe internet

- Nu este recomandat să accesați site-ul de Internet Banking al băncii dintr-un link primit pe email sau SMS. Linkurile primite pe email vă pot redirecționa către un site fals controlat de atacator. Acesta vă poate păcăli să introduceți credențialele de acces pe acest site fals controlat de atacatori.
- Verificați cu atenție dacă atunci când desfășurați operațiuni financiare conexiunea utilizată este una securizată (https://).
- Dezactivați salvarea parolelor (în special salvarea automată a acestora) în browser;
- Credențialele de acces (utilizator, parola, cod acces, etc) sunt informații personale și nu trebuie comunicate altor persoane. NU notați pe foi hârtie sau în fișiere text nesecurizate aceste informații .
- este recomandat că parola să fie schimbată periodic. De asemenea este foarte important să nu folosiți aceeași parola pentru mai multe servicii (ex. cont email, cont internet banking, cont rețea socializare, etc).
- Bancile NU apelează (telefonic, email sau SMS) la clienții săi pentru a cere informații precum: CNP, număr card, PIN, ID logare, parola sau orice alte informații personale.

