

Marian GHERMAN, doctor în drept, conferențiar universitar,
șef al Catedrei „Investigații operative” a Academiei „Ștefan cel Mare” a MAI
Cristina LESNIC, inspector principal al Direcției relații internaționale
și integrare europeană a MAI, master în drept, doctorandă

MODALITĂȚI DE SUSTRAGERE A BANILOR CU FOLOSIREA FRAUDULOASĂ A CARDURILOR BANCARE

Fraudele bancare, în special cele legate de confecționarea și folosirea frauduloasă a cardurilor, au devenit o provocare în epoca actuală odată cu evoluția tendințelor criminalității și datorită noilor tehnici moderne de sustragere a banilor. Acest fenomen a căpătat o amploare mondială, fapt care a determinat o preocupare stringentă a organelor de drept.

În ultimii ani, industria bancară a depus eforturi considerabile pentru ameliorarea securității utilizării cărților de credit sau a mijloacelor de plată prin sofisticarea sistemelor criptografice, însă în ciuda acestor măsuri, acest fenomen rămîne a fi tentant pentru unii infractori.

Pentru moment, prin acțiunile de ofensivă, întreprinse de organele de drept internaționale pentru contracararea criminalității financiar-bancare în special, lumea interlopă este nevoită să recurgă la noi forme și metode de comitere a infracțiunilor, inclusiv cu folosirea tehnologiilor informaționale performante.

În același timp, evoluția tehnologiilor informaționale și a modului electronic de plată a impulsionat dezvoltarea comportamentelor criminale legate de aceste noi metode de tranzacții, în special a sustragerilor de bani cu folosirea frauduloasă a cardurilor bancare. Odată cu extinderea sistemului bancar în țara noastră, apar și unele efecte secundare nedorite. Numărul atentatelor criminale de acest gen se înmulțește de la o lună la alta. Mai mult ca atât, statisticile arată că metodele sustragerilor din bancomate sunt în permanentă dezvoltare. Pe măsură ce se extinde rețeaua de bancomate, crește și riscul apariției fraudelor.

Cele mai frecvente metode de furt cu ajutorul automatelor bancare se bazează pe necunoașterea de către posesorul cardului a condițiilor generale de folosire a lui.

O primă metodă, și probail cea mai simplă, prin care pot fi sustrate mijloacele bănești este furtul propriu-zis al cardului prin blocarea acestuia în interiorul bancomatului. Hoții folosesc o bucată de film ascunsă în fanta prin care introducem cardul, cu care îl rețin ulterior, după ce află PIN-ul utilizatorului, recuperează cardul și fură banii. În fotografiile de mai jos este descris întreg procedeu:

Furturile din Bancomate



♦ In primul slide vedeti o persoana care, aparent, realizeaza o tranzactie la bancomat.

Amplasarea capcanei



♦ De fapt, amplaseaza o capcana in bancomatul, dupa ce "captura" cardul urmatorului utilizator.

Cineva sta de paza



♦ Fraudarea bancomatelor este o afacere riscanta, de aceea se lucreaza in echipe. Cel care sta de paza avertizeaza asupra eventualelor martori oculari sau a unei potentiale victime.

Victima



♦ Aici vedeti urmatorul client care utilizeaza bancomatul, dupa ce "capcana" a fost montata. Introduce cardul si incepe tranzactia.

Declansarea "capcanei"



♦ Cardul este retinut in bancomat, iar clientul este confuz, intrebandu-se de ce a fost retinut cardul? In orice caz vedem cavaleria venind sa "ajute".

Onestul "Samaritean" oferindu-si "ajutorul"



♦ Aici veti vedea hotul prefacandu-se ca ajuta. De fapt, incearca sa afle PIN-ul, acum ca a capturat deja cardul.

Calea spre aflarea codului PTN



♦ Bunul Samaritean isi convinge victima ca poate recupera cardul, daca tasteaza PIN-ul in acelasi timp ce el apasa tastele "cancel" si "enter" sau alta combinatie.

Situatie fara iesire asa ca amandoi pleaca



♦ Dupa mai multe incercari victima este convinsa ca i-a fost retinut cardul. Victima si "Bunul Samaritean" pleaca.

Recuperarea cardului



- ◆ După ce zona este liberă, hoțul se întoarce să recupereze cardul reținut de capcană. Acum nu numai că are cardul, dar și aflat PIN-ul.

Succes



- ◆ În posesia cardului și a PIN-ului, parasește bancomatul cu 4000\$ din contul victimei.

Capcana



- ◆ Capcana este făcută dintr-un film pentru radiografii, care este preferat de hoți deoarece are aceeași culoare, negru, cu cititorul de card.

Montarea capcanei



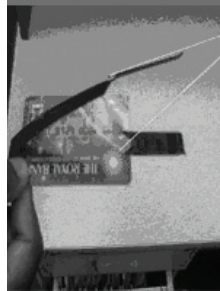
- ◆ Capcana este introdusă în cititorul de card al bancomatului. Cu grijă, pentru a nu introduce întregul film - capetele sunt îndoite și pe ele este pus adeziv pentru o bună lipire de partea interioară și exterioră a ramei cititorului de card.

INVIZIBIL



- ◆ De îndată ce capetele au fost lipite și fixate de rama, sunt aproape imposibil de detectat de către clienții neșuspicioși.

„Cum este cardul confiscat?”



- ◆ Pe ambele părți sunt făcute tăieturi. Aceasta previne returnarea cardului înainte de încheierea tranzacției.

Tragerea cardului confiscat



- ◆ De îndată ce victima pleacă, și are PIN-ul, hoțul dezlipște părțile lipite și retrage filmul în care este reținut cardul.

RECOMANDĂRI.



1. - În cazul în care ți-a fost reținut cardul, verifică dacă cititorul de card prezintă urme de falsificare. Dacă observi capetele lipite ale unei capcane, dezlipeste-le, trage capcana și recuperează cardul.
2. - Raportează IMEDIAT la Banca.

Altă metodă, puțin mai performantă, prin care hoții pot încerca să fure banii de pe card, este utilizarea unui bancomat fals. În atare cazuri, infractorul se folosește de o carcasă de bancomat de un tip mai vechi, care este mutată dintr-un loc în altul, strategic amplasat în zone în care nu există bănci. Din momentul în care ai introdus cardul și încerci să scoți bani, îți scanează cardul și memorizează PIN-ul, iar ulterior îți golește contul de card.

Imitația este perfectă, hoții de obicei fiind niște electroniști foarte buni, care folosesc dispozitive de citire asemănătoare bancomatelor originale.

Una din cele mai performante metode de sustragere a informațiilor de pe banda magnetică a cardului (în scopul ca să fie folosită ulterior pentru sustragerea banilor) este „skimmingul”.

Avantajul acestei metode constă în folosirea pe larg a noilor tehnologii informaționale, în special a aparatului electronic „card-reader”, care are capacitatea de a citi și de a înscrie informația electronică furată.

„Skimming” vom numi tipul de fraudă în care se sustrag informațiile conținute în cardurile bancare prin instalarea deasupra automatelor bancare a diferitor dispozitive electronice care permit fixarea și transmiterea la distanță a informației obținute fraudulos în momentul efectuării operațiunilor electronice. Dispozitivele electronice utilizate de către infractori se maschează sub diferite părți componente ale automatelor bancare publice. Adeseori se folosesc minicamere de luat vederi mascate în carcasa bancomatului și care permit înregistrarea parolelor de identificare culese de clienți (PIN-cod). În practica judiciară, mai întâlnim o varietate specifică, foarte asemănătoare cu metoda „skimming”, dar puțin mai complicată și mai mascată. Cu ajutorul dispozitivului „card-reader” se citește și se memorizează informația de pe banda magnetică a cardului în procesul achitării diferitor servicii, spre exemplu: la restaurante, markete, baruri etc., iar prin intermediul minicamerelor se fură PIN-codul. Ulterior hoții amplasează pe paginile Internetului informații, precum că se vinde informația electronică și parola unui sau altui card, uneori chiar indicându-se suma de bani ce poate fi extrasă de la bancomat.

Utilizatorii Internetului, accesând site-urile respective, contra unei sume negociabile pot obține informațiile respective și, confecționând un nou card alb bancar, golesc ușor conturile bancare străine.

Cea mai nouă metodă de fraudare a cardurilor bancare la noi în țară a apărut recent, mai precis din momentul în care instituțiile bancare au acordat un nou serviciu – efectuarea operațiunilor financiare prin intermediul Internetului.

Tehnologia obținerii frauduloase a PIN-codului e foarte simplă. Pe adresa electronică a Dvs. primiți o scrisoare de la banca unde depozitați banii, prin care sunteți rugați a indica parola cardului în scop de comparare, de reînnoire a datelor, ori din altă pricină. Acest gen de fraudare se numește „phishing”.

În final, v-aș propune cele mai simple reguli a căror respectare vă va proteja mijloacele financiare:

– străduiți-vă să folosiți bancomatele instalate în centrele comerciale mari sau nemijlocit în bănci, nu se recomandă folosirea celor aflate pe stradele, în locuri

mai puțin;

– nu efectuați operațiuni electronice cu cardul bancar alături de persoane suspecte;

– în nici un caz nu divulgați nimănui PIN-codul cartei (nici funcționarului băncii, nici celor din jur care doresc „să vă ajute” etc.);

– până la introducerea cardului în fantă, cercetați bancomatul minuțios dacă la el nu sunt conectate instalații adiacente;

– la folosirea bancomatului nu permiteți nimănui să vă sustragă atenția, nu acceptați ajutorul cuiva la efectuarea operațiunilor electronice;

– folosiți-vă de alt bancomat în cazul în care observați că acesta nu funcționează ca de obicei;

– anunțați imediat banca emitentă despre blocajul cartei Dvs. în fanta bancomatului;

– regulat, străduiți-vă să controlați contul Dvs., iar în cazul apariției unor neconcordanțe, anunțați imediat banca.