COLEGIUL TEHNIC „VICTOR UNGUREANU”
CÂMPIA TURZII

PROIECT

PENTRU OBŢINEREA CERTIFICATULUI DE CALIFICARE
PROFESIONALĂ NIVEL 4

TEHNICIAN OPERATOR TEHNICĂ DE CALCUL

ABSOLVENT:
BUCUR M.M. RAUL-DENIS

COORDONATOR:
prof. ARION LOREDANA

2019 – 2020

Mijloace de fraudă prin intermediul Internetului

CONŢINUT

ARGUMENT 4
I. FRAUDA INFORMATICA 5
I.1. Conţinutul legal 5
II.2. Condiţii preexistente 5
II. FORME DE FRAUDĂ INFORMATICĂ 7
II.1. „Momeşte şi schimbă” (Bait and Switch) 7
II.2. „Trucuri bazate pe încredere – abuzul de încredere” (Confidence Tricks) 8
II.3. „Fraude cu avans” (Advance Fee Fraud) 8
II.4. „Depozitele false” (Fake Escrow) 10
II.5. „Frauda salam” 10
II.6. „Prizonierul Spaniol” 10
III. EXEMPLE DE FRAUDE INFORMATICE 11
IV. FRAUDE INFORMATICE AUTOHTONE 13
BIBLIOGRAFIE 17

ARGUMENT

Calculatorul şi Internetul au revoluţionat accesul la informaţie în ultimii ani. Astăzi, printr-o simplă tastare a unei adrese de net şi un Enter ridicăm rapid vălul asupra informaţiei. În acelaşi timp, internetul a deschis calea către aşa-numitele infracţiuni on-line, semn că în orice spaţiu ne-am afla – real sau virtual – nu există siguranţă absolută.

Calculatoarele au pătruns în activităţile tuturor ţărilor, devenind instrumente indispensabile pentru desfăşurarea diferitelor activităţi. Acestea au avut un impact global asupra vieţii de zi cu zi, asupra modului de desfăşurare a afacerilor, de comunicare şi de gestiune a informaţiei. Noua tehnologie a adus mari şi numeroase avantaje administraţiei, afacerilor şi chiar particularilor însuşi.

Această evoluţie rapidă şi radicală ridică o serie de probleme juridice în privinţa protecţiei programelor pentru calculator.

Apariţia calculatorului a deschis posibilitatea apariţiei unei game largi de acţiuni ilegale cu un caracter extrem de sofisticat, el putând fi folosit şi la comiterea sau la facilitarea comiterii unor infracţiuni clasice, cum ar fi furtul sau frauda.

Consiliul Europei a adoptat o recomandare asupra criminalităţii în relaţia cu calculatorul şi a publicat un raport ce cuprinde o listă minimală şi o listă facultativă de infracţiuni informatice. Astfel, lista minimală cuprinde fapte cum ar fi frauda informatică, falsul informatic, prejudiciile aduse datelor sau programelor pentru reproducerea neautorizată de programe pentru calculator protejate, iar lista facultativă cuprinde fapte cum ar fi alterarea datelor sau programelor pentru calculator sau utilizarea neautorizată a unui program pentru calculator protejat.

O infracţiune cu ajutorul calculatorului a fost catalogată ca fiind orice situaţie în care calculatorul a fost ţinta infracţiunii, un instrument de comitere a infracţiunii sau atunci când acesta este incidental, dar semnificativ legat de comiterea infracţiunii.

Cu mulţi ani în urmă au existat unele comentarii care avertizau că, într-o bună zi, computerul va fi implicat în toate formele de delincvenţă. Se pare că a existat o mare doză de adevăr în aceste previziuni şi, mai mult, acestea au rămas valabile şi în ziua de azi. Dacă luăm în considerare statisticile din ultimii cincisprezece ani, se poate susţine cu tărie că infracţiunea asistată de calculator nu poate fi socotită deloc inofensivă şi că fenomenul este într-o continuă creştere.

Primele legi împotriva infracţiunilor săvârşite cu ajutorul computerului conţineau, în esenţă, prevederi împotriva actelor de pătrundere în baza de date, de înşelătorie şi copyright-ului. Dar aceste delicte ce caracterizează criminalitatea prin computer constituie doar o mică parte din cele posibile. La scurt timp s-a dovedit că şi traficul de stupefiante, comerţul ilegal cu arme, pornografia infantilă, diverse forme de delicte economice şi chiar privind protecţia mediului înconjurător pot fi făcute prin intermediul calculatorului.

I. FRAUDA INFORMATICA

I.1. Conţinutul legal

Infracțiunea de fraudă informatică este prevăzută de art. 49 din Legea criminalității informatice. Textul de lege definește frauda informatică după cum urmează:

Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la aceste date ori prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, constituie infracţiune şi se pedepseşte cu închisoare de la 3 la 12 ani.

Numărul fraudelor financiare din mediul online este în continuă creștere. Conform unui studiu Kaspersky Lab și B2B International, 43% dintre utilizatori s-au confruntat cu un atac cibernetic, care viza datele financiare. În plus, 44% dintre utilizatorii care au pierdut bani în urma fraudelor bancare online nu i-au mai recuperat.

Utilizatorii pot subestima riscurile la care se expun atunci când efectuează tranzacții online. Poate fi dificil pentru ei să urmărească toate etapele proceselor de plăți online și amenințările la care se expun pe parcurs. Procesul este similar indiferent de suma tranzacționată, iar utilizatorii trebuie să fie conștienți de riscuri în momentul în care transferă bani prin intermediul PC-ului, laptopului, a tabletei sau a smartphone-ului.

II.2. Condiţii preexistente

A. Obiectul infracţiunii

a) **Obiectul juridic special** îl constituie relaţiile sociale care protejează patrimoniul unei persoane, atunci când prezenţa respectivei persoane în spaţiul cibernetic se cuantifică într-un anumit volum de date stocate într-un sistem informatic sau vehiculate într-o reţea.

b) **Obiectul material** este reprezentat atât de datele informatice (stocate în sistemele informatice vizate), cât şi de entităţile materiale care compun un sistem informatic, individual sau aflat în comunicare cu alte sisteme prin intermediul unei reţele.

B. Subiecţii infracţiunii

a) **Subiectul activ** (autorul) poate fi orice persoană responsabilă penal. Manipulările frauduloase de acest gen sunt realizate adesea de iniţiaţi în domeniul calculatoarelor ori de persoane care, prin natura serviciului, au acces la date şi sisteme informatice. Participaţia este posibilă în toate formele sale: coautorat, instigare ori complicitate.

b) **Subiectul pasiv** va fi persoana al cărei interes patrimonial a fost prejudiciat prin acţiunea făptuitorului. Şi de această dată, subiect pasiv adiacent va fi proprietarul, deţinătorul de drept sau utilizatorul legal al unui sistem informatic.

II. 3. Conţinutul constitutiv

A. Latura obiectivă

a) Elementul material al infracţiunii se realizează printr-o acţiune alternativă de introducere, modificare sau ştergere de date informatice ori de restricţionare a accesului la respectivele date sau de împiedicare în orice mod a funcţionării unui sistem informatic. „Împiedicarea funcţionării sistemului informatic" vizat presupune înfăptuirea oricărui act de natură a duce la imposibilitatea utilizării, parţial sau total, temporar sau permanent, a respectivului sistem. Spre exemplu, făptuitorul acţionează la o anumită dată şi la o anumită oră asupra sistemului informatic al Bursei, reuşind să paralizeze tranzacţiile electronice de acţiuni, ceea ce are repercusiuni serioase asupra afacerilor şi câştigurilor entităţilor aflate în plin proces de vânzare-cumpărare.

În mediul informatic, frauda poate avea mai multe forme şi adesea se poate confunda cu înşelăciunea tradiţională, mijlocul de realizare fiind computerul.

b) Urmarea imediată constă în crearea unui prejudiciu patrimonial unei persoane.

c) Legătura de cauzalitate între activitatea făptuitorului şi urmarea produsă trebuie dovedită.

B. Latura subiectivă

Frauda informatică se săvârşeşte numai cu **intenţie directă**, aceasta fiind calificată prin scop. Fapta se săvârşeşte în scopul obţinerii un beneficiu material pentru sine sau pentru altul.

Pentru existenţa laturii subiective a infracţiunii nu este nevoie ca prejudiciul material să fi fost efectiv realizat, ci numai să fi existat ca o posibilitate urmărită de făptuitor.

II. FORME DE FRAUDĂ INFORMATICĂ

În mediul informatic, frauda poate avea mai multe forme şi adesea se poate confunda cu înşelăciunea tradiţională, mijlocul de realizare fiind computerul.

Dat fiind mediul informatic în care acestea sunt iniţiate şi derulate, cele mai întâlnite mijloace de fraudă informatică sunt:

- „Momeşte şi schimbă" (Bait and Switch)
- „Trucuri bazate pe încredere – abuzul de încredere" (Confidence
- Tricks)
- „Fraude cu avans" (Advance Fee Fraud)
- „Depozitele false" (Fake Escrow)
- „Frauda salam"
- „Prizonierul Spaniol"

II.1. „Momeşte şi schimbă" (Bait and Switch)

Este o formă de fraudă informatică în care făptuitorul ademeneşte potenţiali clienţi făcând publicitate (preţ foarte mic, profitabilitatea afacerii etc.) unor produse, care fie nu există în realitate, fie sunt ulterior schimbate cu produse aparent similare, dar cu calităţi net inferioare.

În esenţă, clientului i se prezintă posibilitatea de a achiziţiona un anumit produs la un preţ foarte mic, însă în momentul onorării comenzii, acestuia i se comunică faptul că produsul „nu mai există în stoc" şi i se oferă o altă posibilitate, un alt produs (contrafăcut) ca o „consolare" pentru „inexistenţa" celui original prezentat în anunţ.

Caracteristic pentru această fraudă este faptul că în nici un moment autorul nu are de gând (nu intenţionează) să vândă produsul-momeală.

Fapta se realizează cel mai adesea prin intermediul sistemelor informatice şi al reţelei Internet. Ademenirea clienţilor se poate face şi prin mesaje de poştă electronică (email) sau prin intermediul unei (bine alcătuite) pagini Web.

II.2. „Trucuri bazate pe încredere – abuzul de încredere" (Confidence Tricks)

Se bazează pe intenţia de a induce în eroare o persoană sau un grup de persoane (denumite „ţinte") cu privire la posibilitatea de a câştiga importante sume de bani sau de a realiza ceva însemnat.

De obicei, făptuitorul se bazează pe ajutorul unui complice, care, pe parcursul înşelăciunii, va acţiona psihologic asupra ţintei inducându-i artificial senzaţia că „jocul", „acţiunea" etc. sunt cât se poate de reale şi profitabile, ele însuşi „având încredere în autor".

La origine, acest truc se baza pe exploatarea anumitor laturi ale personalităţii umane, cum ar fi lăcomia sau necinstea. Adesea, victimelor le sunt exploatate dorinţele de „înavuţire rapidă", de „câştiguri de bani fără efort" sau de investiţii „prea bune ca să fie adevărate".

Astfel, spre exemplu, ţinta va fi convinsă de către făptuitor că va câştiga o importantă sumă de bani participând la înşelarea unei a treia persoane, care, de fapt, este în legătură cu infractorul şi participă în complicitate la realizarea acestei acţiuni. Bineînţeles, victima este cea care pierde „jocul".

Şi în acest caz, abordarea victimei de către infractor şi chiar desfăşurarea acţiunii se fac prin intermediul mijloacelor electronice (email, pagină Web etc.).

II.3. „Fraude cu avans" (Advance Fee Fraud)

Sunt adesea cunoscute sub denumirea de „transferuri nigeriene" sau „scrisori nigeriene" ori, pur şi simplu, „înşelătorii 419" (după numărul articolului din Codul Penal al Nigeriei care incriminează astfel de fapte).

În acest caz, victimele sunt oameni bogaţi sau investitori din Europa, Asia Australă sau America de Nord. Mijloacele de comitere variază de la scrisorile expediate prin poştă sau faxuri la email sau pagini web, în special după 1990.

Schema de operare este relativ simplă. O persoană (investitor, om de afaceri etc.) este contactată după următorul şablon: „...oficial cu rang înalt din Nigeria, intenţionez să expatriez importante fonduri şi vă solicit ajutorul de a folosi conturile dvs. pentru transferul bancar, în schimbul unui comision de 10-20% din suma transferată...". Presupusa afacere este în mod atent prezentată şi ca un "delict nesemnificativ" (gen white collar crime – infracţionalitatea gulerelor albe), care, însă, oferă posibilitatea unor „importante câştiguri". Inducerea, aproape subliminal, a ideii de „mică ilegalitate" în legătură cu „operaţiunea" are rolul de a descuraja victima să raporteze cazul autorităţilor în momentul în care realizează că, dându-şi detaliile de cont unor necunoscuţi, a fost în realitate deposedată de toate lichidităţile sau economiile.

Astfel de înşelăciuni îşi au originea în Nigeria şi, de regulă, sunt pregătite astfel încât adresele de email, site-urile Web, numerele de telefon sau fax etc. să pară a fi cele ale unor centre de afaceri, firme sau chiar instituţii guvernamentale locale.

Există şi cazuri în care, în corespondenţa prin email, autorii au solicitat în mod direct victimelor sume de bani în lichidităţi pentru aşa-zise „mituiri ale altor oficiali ori ale personalului bancar care urma să asigure transferul cel mare" etc.

În alte abordări, se preciza că „pentru a putea facilita transferul, trebuie ca dumneavoastră (ex. Investitorul) să aveţi deschis un cont la o bancă nigeriană, în valoare de cel puţin 100.000 USD".

În câteva situaţii, chiar, victimele au fost invitate în Nigeria să se întâlnească cu respectivii „oficiali guvernamentali" sau cu „alte persoane importante" – în fapt complici ai autorilor care susţineau scenariul „autenticităţii şi iminenţei expatrierii de fonduri".

În 1995, un cetăţean american care a întreprins o astfel de vizită în Nigeria a fost ucis, moment în care anchetele au fost preluate spre soluţionare de către US Secret Service.

Astfel de fapte se produc încă frecvent în Nigeria, dar fenomenul s-a şi internaţionalizat. Cel mai răsunător succes al organelor de securitate a fost arestarea, în 2004, la Amsterdam, a 52 de persoane implicate în acţiuni similare.

Într-o altă variantă a fraudei, victima primeşte un mesaj de email de la un presupus avocat ori reprezentant al unei societăţi de administrare valori mobiliare sau imobiliare prin intermediul căruia este anunţată cu privire la decesul unei „rude foarte îndepărtate", de care, bineînţeles, victima nu avea cunoştinţă, şi care i-ar fi lăsat o moştenire însemnată. Autorul solicită într-un mesaj ulterior victimei detaliile conturilor bancare în vederea „transferului bancar al lichidităţilor moştenite" (sume exorbitante care au menirea să inhibe instinctul de apărare).

În cea mai nouă versiune a acestui tip de fraudă, autorul se oferă să cumpere unul dintre produsele scumpe postate spre vânzare de victimă pe o pagină de Web specializată în vânzări şi cumpărări online (ex. **eBay**), printr-un ordin de plată, filă cec sau alt instrument oficial emis de a

autoritate bancară. În mod „accidental” cec-ul va avea înscrisă o sumă mai mare decât valoarea produsului „cumpărat”, motiv pentru infractor să-i solicite (prin email) victimei să-i returneze diferenţa de bani, telegrafic, la o terţă adresă, la confirmarea primirii coletului. De regulă, cec-ul intră ca bun de plată după o zi sau două, însă contrafacerea lui iese la iveală abia după aproape o săptămână, timp în care victima a apucat să trimită şi produsul şi „restul de bani” infractorului.

II.4. „Depozitele false” (Fake Escrow)

O altă metodă de fraudare în sisteme informatice este aceea prin care, autorul, după ce câştigă o licitaţie de produse pe un site Internet specializat (gen eBay sau AltaVista), solicită victimei utilizarea unui site (sau serviciu) de escrow „sigur”, „neutru” care să „depoziteze” bunurile (produsele – în general echipamente electronice) până la perfectarea aranjamentelor financiare.

Bineînţeles, site-ul de escrow este creat şi controlat de infractor, iar la primirea bunurilor „în gaj”, respectiva pagină Web este închisă (dezactivată) iar contul şters.

II.5. „Frauda salam”

Este o operaţiune destul de simplu de realizat, dar necesită accesul în sistemul informatic al unei instituţii bancare.

Autorul accesează aplicaţia informatică de gestionare conturi clienţi sau pe cea de facturare şi modifică anumite linii din program în aşa fel încât produce o rotunjire în minus a sumelor rezultate din calculele bancare specifice, diferenţele fiind direcţionate către un anumit cont. Numele fraudei este sugestiv pentru operaţiunea de obţinere, sumare şi transfer a tuturor procentelor rezultate din rotunjirile aritmetice impuse prin soft.

II.6. „Prizonierul Spaniol”

Metoda, pe cât de simplă, pe atât de jenantă pentru victime, îşi are originea într-o înşelăciune la modă în secolul 17.

În esenţă, autorul contactează ţinta (om de afaceri, familia acestuia, persoane cu tendinţe caritabile etc.) printr-un mijloc electronic (email, mesagerie instant – IM etc.) şi îi „dezvăluie” faptul că este în legătură (telefonică, email etc.) cu un „foarte important” ori „binecunoscut” personaj din lumea politică, economică - socială ori artistică, ce se află încarcerat sub un alt nume în Spania, fiind victima unei înscenări. Întrucât personajul ar dori să evite publicitatea de scandal, autorul înşelăciunii solicită „sprijinul financiar” al ţintei pentru a „plăti cauţiunea personalităţii arestate”, urmând ca aceasta, la revenirea în ţară, să se „revanşeze considerabil”.

Adesea, frauda nu se opreşte după primul transfer bancar de acest gen, victima realizând mult mai târziu, în cursul corespondenţei electronice cu autorul, că sunt necesare şi alte „operaţiuni

costisitoare” cărora a trebuit (trebuie) să le facă faţă „pentru eliberarea personajului”, totul fiind, evident, construit artificial.

Succesul fraudei rezidă de cele mai multe ori în măiestria jocului psihologic al autorului care îmbracă povestea „incredibilă” într-o aură de mister şi confidenţialitate, reuşind să-i creeze victimei impresia că participă la o „acţiune de mare însemnătate” în plan politic – economic - social ori artistic.

III. EXEMPLE DE FRAUDE INFORMATICE

În legătură cu delictele comise prin intermediul calculatorului există la această oră un adevăr incontestabil: doar o mică parte a acestora sunt descoperite de politie iar organele de anchetă dispun de un volum mic de informații. În același timp, aceștia nici nu sunt pregătiți suficient de bine pentru un domeniu aproape nou.

În acest context, analizând cifrele relativ scăzute din statisticile acestor infracţiuni, s-ar putea trage concluzia falsă că pericolul este supraestimat. Societăţile, în general, nu sunt pregătite suficient de bine la această oră pentru a preîntâmpina aceste infracţiuni.

În continuare sunt enumerate câteva exemple concrete de infracţiuni săvârşite prin intermediul calculatorului, atât pe plan mondial, cât si pe plan autohton.

- Primele cazuri importante de acces neautorizat au fost depistate în 1985 când a fost atacată cunoscuta rețea ArpaNet. În același an revista on-line "Phrack" a publicat o listă destul de bogată de numere de apel dial-up. În continuare această activitate s-a desfășurat din plin. Pentru tinerii americani inteligenți care dispuneau de serviciile unui calculator electronic începea să se deschidă o lume nouă, în general lipsită atunci de legi.

- Unul din cazurile celebre de fraudă informatică este cel al unui grup de hackeri care a preluat controlul centralei telefonice de la Casa Albă, utilizând-o pentru convorbiri telefonice transatlantice.
- Pe data de 6 ianuarie 1993, câțiva hackeri din Marea Britanie au pătruns în banca de date a unei companii comerciale din Londra, operând un transfer de 10 milioane de lire sterline. Este un exemplu de infracțiune concretă, făcând parte din categoria "campaniilor active", adică a acelora care lasă prejudicii ce pot fi imediat cuantificate.
- Tot în aceeași perioadă câteva site-uri oficiale americane au fost "ocupate" de o acțiune spectaculoasă, de tip protestatar, a unor chinezi. Aceștia au introdus în locul mesajelor standard existente, propriile lor texte de protest, provocând un fel de mini-război psihologic. Este un exemplu de "campanie pasivă", cu implicații de natură psihologică în primul rând, dar si de natură politică, fiind mai degrabă o dovadă că războiul informațional a devenit o realitate care nu mai poate fi neglijată.
- În anul 1993 un chinez a fost condamnat la moarte prin împușcare pentru o fraudă de 193 milioane USD în mediul on-line. Abia după înregistrarea acestui caz unic, statul chinez a elaborat si prima lege în acest domeniu.
- Un cunoscut hacker american, a cărui poveste a stat si la baza realizării unui film de succes, a fost prins si pedepsit de justiție; la scurt timp a fost eliberat cu o interdicție de câțiva ani să se apropie de un telefon public.
- Iată un exemplu de infracțiune de omor: un individ, dorind să-si elimine rivalul aflat la tratament într-un spital din Florida, a pătruns în baza de date a spitalului modificând diagnosticul pacientului. Fiind tratat pentru altceva decât boala de care suferea, pacientul a decedat în scurt timp.
- Jim Jarrard din Simi Valley, California, a avut surpriza să constate că în timp ce si-a lăsat calculatorul într-o noapte să funcționeze pentru a finaliza un download de mari dimensiuni, un hacker i-a accesat PC-ul prin conexiunea DSL și a instalat un program care i-a permis să controleze calculatorul, să fure fișiere importante și să șteargă informațiile de pe hard disk-uri. Jarrard a scăpat de catastrofă datorită unei blocări neașteptate a sistemului.
- Allan Soifer, administrator de postă electronică în Ottawa, nu si-a dat seama că un hacker îi scana PC-ul de acasă de câteva ore. Hackerul găsise o poartă de intrare si avea nevoie numai de o parolă pentru a accesa fișierele. Acesta bombarda respectivul calculator cu parole generate aleator, sperând că va nimeri combinația corectă. Victima a fost norocoasă deoarece avea instalat ZoneAlarm, un program de protecție de tip firewall personal preluat de la firma ZoneLabs. Programul l-a alertat despre multitudinea de parole cu care era

bombardat PC-ul. În plus, el a putut identifica chiar ISP-ul hackerului pe care l-a localizat în Anchorage, Alaska.

- Câteva exemple de viruși reali, altele decât cele arhicunoscute, dar care au provocat pagube însemnate în diferite companii și organizații americane:
  - "Typo", virus orientat pe distrugerea datelor care creează erori de dactilografiere atunci când utilizatorul depășește 60 de cuvinte pe minut.
  - Un virus de distrugere a producției a fost lansat într-o întreprindere metalurgică, și avea rolul de a micșora cu câteva grade temperatura în cea de-a treia fază a procesului de răcire a otelului, conducând la o calitate inferioară a produsului.
  - Cel mai mic virus a fost scris prin rescrierea algoritmului comenzii Unix "sh". Acesta avea dimensiunea de 8 caractere și în afară de reproducere nu mai avea altă funcție.
  - La începutul anilor '90 dintr-un institut de cercetări din Bulgaria a fost lansat în circulație un set de 24 viruși care au fost cu greu detectați atât în Europa, cât și în SUA.

IV. FRAUDE INFORMATICE AUTOHTONE

Evoluţia crimei organizate în Romania în ultimii anii este strâns legată de evoluţia criminalităţii informatice şi de folosirea tot mai intensă a tehnologiei IT&C, în comiterea de infracţiuni.

Analizele realizate la nivelul organismelor europene privind trendul criminalităţii organizate, definesc criminalitatea informatica ca o ramură importantă a crimei organizate la nivelul ţărilor UE.

Din evaluările grupărilor infracţionale care acţionează în domeniu s-au desprins următoarele caracteristici, privind criminalitatea informatica produsa din România:

- caracter predominant financiar, se urmăreşte obţinerea unui produs financiar substanţial si sunt vizate sisteme de plata si produse de credit şi plăti oferite de instituţii financiare;
- organizarea grupărilor care acţionează, structurarea si specializarea membrilor acestora;
- folosirea de tineri cu abilităţi în a utiliza computerele si noile tehnologii, care sunt organizaţi şi coordonaţi de către leaderi ai grupărilor infracţionale;
- trecerea de la fraudele informatice, in care încrederea era elementul primordial in realizarea tranzacţiilor, la fraude in care predomina folosirea de programe informatice in fraudare;
- caracterul transnaţional al acestor fapte, in sensul ca sunt vizate victime din alte tari, anumite activităţi sunt derulate de pe teritoriul altor state sau sunt folosite sisteme informatice din alte state;

- permanenta preocupare pentru identificarea de noi moduri de operare, de identificarea de produse ce pot fi fraudate, precum si sisteme informatice ce pot fi compromise;
- reorientarea grupărilor infracţionale către fraudarea mijloacelor de plata electronica oferite de instituţiile financiare din România;
- reorientarea grupărilor infracţionale care comit fraude informatice de la fraudele mărunte (prejudicii mici) îndreptate împotriva persoanelor, către fraudele mari (prejudicii marii - sute de mii/milioane de euro) împotriva companiilor;
- specializarea infractorilor pe tipuri de infracţiuni si tari de destinaţie, datorată specificului zonei (zone turistice, zone cu număr ridicat de grupări infracţionale bine organizate, etc).

În continuare sunt enumerate câteva exemple concrete de infracţiuni săvârşite prin intermediul calculatorului în România.

- Un hacker din România, supărat pe preturile mereu în creștere practicate de RomTelecom, a pătruns în rețeaua societății si a modificat tarifele din site, făcându-le 1 leu pentru 5 ore de convorbire.
- Niște hackeri români au pătruns în urmă cu câțiva ani într-un server extern al Pentagonului. Deși nu sau ales cu nimic, site-ul fiind de mică importantă, ei au fost descoperiți la timp înainte de a provoca anumite stricăciuni.
- Ministerele de Interne, Justiție și Finanțe din tara noastră au fost atacate de mai multe ori de viruși ce au adus modificări majore ale informațiilor din site-urile respective.
- În anul 2001, pe când guvernul a anunțat mărirea accizelor la băuturile alcoolice, pe pagina de Web a Ministerului de Finanțe a pătruns un hacker care a introdus în site mesajul de protest: "Acest site a fost spart de Regele Berii".
- Câțiva hackeri români și-au bătut o vreme joc de pagina de Web a guvernului, amestecând pozele acesteia.
- Un alt hacker din România a reușit să intre pe site-ul FBI, "prinzând" pe acesta poza lui Ion Iliescu.
- În ceea ce privește comerțul electronic, românii s-au specializat în realizarea de cumpărături de pe magazinele virtuale aflate în afara tării (marea majoritate fiind în SUA), folosind cărți de credit furate sau false. În acest scop au fost folosite site-uri specializate în comerț electronic si baze de date cu numere de cărți de credit. Atacurile de acest gen sunt favorizate și de faptul că timpul dintre momentul plătii nelegitime și momentul în care proprietarul cărții de credit sesizează evenimentul și refuză plata este suficient de mare.
- Un hacker român a descoperit niște bug-uri (erori) în rețeaua de calculatoarele a unui cetățean american care tocmai deschisese un Internet - Cafe în București. L-a avertizat pe

acesta în câteva rânduri cu privire la faptul că administratorul acelei rețele nu-și face corect datoria sau nu se pricepe să-și protejeze sistemul. Americanul l-a invitat pe hacker să vină să lucreze la firma sa. Și de atunci, acesta este angajat acolo, are un salariu decent, taxiul decontat, telefonul plătit de firmă etc.

- Alt hacker român a blocat calculatorul unui individ pe care nu-l simpatiza deloc, în așa fel încât atunci când îl deschidea intra pe Word, scria un text și se reseta. Desigur, calculatorul a devenit practic inutilizabil. Revenind la sentimente mai bune, hackerul a îndreptat el însuși situația doar după câteva zile.
- Un foarte bun hacker român, de data aceasta în sensul inițial al termenului de hacker, a găsit niște bug - uri în rețeaua firmei Ericsson și a trimis acesteia constatările lui și felul în care se poate rezolva problema. A primit în schimb de la patronii firmei un telefon de ultimul tip, placat cu aur.
- La începutul lunii octombrie, 1999 Judecătoria Ploiești a pronunțat prima sentință de condamnare a administratorului firmei ANDANTINO la șase luni de închisoare cu suspendare condiționată a executării pedepsei. Pe data de 18 septembrie 1998 inculpatul a fost surprins de polițiști și inspectori ai Oficiului Român pentru Drepturi de Autor în timp ce vindea CD-uri cu programe de calculator la punctul de lucru al societății sale. "Aceasta este prima sentință penală în materie de piraterie software de la adoptarea în anul 1996 a Legii nr. 8 a Drepturilor de Autor si Drepturilor Conexe si reprezintă o primă dovadă concludentă că proprietatea intelectuală începe să fie respectată si în România" a declarat un avocat reprezentant pentru România al Business Software Alliance.
- În primăvara anului 1999, pe unul din calculatoarele din rețeaua dezvoltatorilor de software din Sidex a fost descoperit un virus spion. Intrusul nu a apucat însă să-si atingă scopul, fiind detectat și anihilat la timp. Tot atunci a fost descoperit și autorul, o firmă de soft din București care urmărea anumite interese comerciale cu Sidex. La vremea respectivă primul autor acestui manual a publicat un articol într-un cotidian local despre acest eveniment, fără însă a oferi detalii suficiente, ci doar cu intenția de avertizare asupra acestei categorii de pericole.
- În toamna anului 2000, un hacker a pătruns în sistemul informatic al CS SIDEX SA. Sistemul, bazat pe o rețea de câteva calculatoare Hewlett-Packard 9000, a fost "deranjat" de un intrus care a început prin a lansa câteva mesaje injurioase, apoi și-a vărsat amarul pe directorul IT. Neluându-se măsurile cuvenite, intrusul a apărut și a doua zi, reușind să lanseze în execuție două comenzi Unix de ștergere a fișierelor care începeau cu o anumită literă. Intruziunea a fost posibilă din cauză că hackerul a cunoscut datele de identificare (UserName și Password) ale unui programator. Din fericire, lucrurile sau oprit aici, găsindu-

se imediat metode de a repara stricăciunile provocate si de a se înlătura pe viitor pericolul unor astfel de atacuri.

- Și alte instituții și societăți din Galați au trecut prin astfel de evenimente, multe din ele nefăcându-se publice, în ideea de a-l tenta pe infractor să revină și altădată când, se presupunea că, vor fi pregătiți să-l prindă în flagrant. Unii infractori au fost prinși, dar au scăpat cu o simplă admonestare, fără vâlvă prea mare, alții însă nu au fost prinși și identificați nici în ziua de azi.

BIBLIOGRAFIE

1. Maxim Dobrinoiu, **INFRACŢIUNI ÎN DOMENIUL INFORMATIC**, Bucureşti, 2006
2. Petre Rău, **INFRACŢIONALITATEA PE CALCULATOR**, Bucureşti, 2001
3. Pagini WEB:

   http://www.criminalitatea-informatica.ro/

   http://www.criminalitate.info/

   http://www.capital.ro/cum-iti-protejezi-banii-de-fraudele-online.html