UDK 005.334:336.71 ; 004.738.5:339

UPRAVLJANJE OPERATIVNIM RIZIKOM I SPREČAVANJE PREVARA U INTERNET BANKARSTVU

dr Bojan Đorđević
Fakultet za menadžment Zaječar
bojan.djordjevic@fmz.edu.rs

Mira Đorđević
Fakultet za menadžment Zaječar
mira.djordjevic@fmz.edu.rs

Rezime

Razvoj informacionih tehnologija i elektronskog novca uslovio je razvoj elektronskih plaćanja i to posebno u domenu Internet bankarstva. Sve je veći broj klijenata koji koriste elektronske usluge banaka putem Interneta. Kako se povećava broj elektronskih proizvoda i usluga banaka, broj klijenata i njihovih transakcija, raste i izloženost banke rizicima u svakodnevnom poslovanju, a time i broj prevarnih radnji i njihovih učinilaca tzv. sajber kriminalaca. Od identifikovanih rizika Internet bankarstva i oblika prevara i sajber kriminala kao najznačajniji izdvajaju se eksterni napadi na bankarske sisteme i s tim u vezi krađe identiteta korisnika i pljačke. U ovom radu razmatramo upravljanje operativnim rizikom u Internet bankarstvu sa akcentom na detekciju eksternih prevara i drugih oblika sajber kriminala kao i metode zaštite u cilju jačanja bezbednosti elektronskih bankarskih sistema i klijenata banaka.

Ključne reči: operativni rizik, Internet bankarstvo, sajber kriminal, fišing, pljačka

UDK 005.334:336.71 ; 004.738.5:339

OPERATIONAL RISK MANAGEMENT AND FRAUD PREVENTION IN INTERNET BANKING

Mira Đorđević
Fakultet za menadžment Zaječar
mira.djordjevic@fmz.edu.rs

Bojan Đorđević PhD
Fakultet za menadžment Zaječar
bojan.djordjevic@fmz.edu.rs

Summary

Development of information technology and electronic money determined the expansion of electronic payments, especially in the Internet banking domain. Number of clients using electronic banking services by Internet is growing. With the expansion of electronic products and banking services, bank exposure to risk in daily operations is growing, as well as the number of frauds and their perpetrators, the so-called cyber criminals. Among the identified Internet banking risks, and different forms of fraud and cyber crime, the most significant are the external attacks on the banking systems, regarding user identity theft and robbery. This paper deals with the operational risk management in Internet banking, with the focus on the detection of external frauds and other forms of cyber crime, together with protection methods for empowering safety of both the bank clients and of the electronic banking systems.

Key words: operational risk, internet banking, cyber crime, phishing, robbery.

Brzi razvoj informacionih tehnologija i širenje komunikacionih mreža, posebno primena novih mobilnih tehnologija, pružili su mogućnost korisnicima da sa bilo kog mesta i u bilo koje vreme pristupe velikoj količini informacija. Koristeći nove tehnologije, banke sve više koriste mogućnosti elektronskog bankarstva (e-banking). To je danas imperativ, ne samo da bi banke smanjile troškove poslovanja, već pre svega zadržale konkurentsku prednost i proširile bazu svojih klijenata. Banke se prilikom pružanja usluga elektronskog bankarstva suočavaju s određenim rizicima, među kojima se izdvajaju strateški, operativni, reputacioni, pravni i rizik međunarodnog (prekograničnog) poslovanja. Savremeno bankarsko poslovanje je svakodnevno izloženo napred pomenutim postojećim (evidentiranim), ali i novim rizicima tj. prisutan je rizik nastanka nepredviđenih događaja. Rizici kao mogućnost apsolutnog ili relativnog gubitka u odnosu na očekivanja u poslovanju banaka su karakteristika svakog bankarskog posla, a osvajanjem novih instrumenata, tehnika i strategija, novih bankarskih proizvoda i usluga, a naročito izlaskom i osvajanjem Internet tržišta, lista rizika se neprestano širi. Neizvesnost raste sa promenama u društvu i ekonomiji, promenama kamatnih stopa, promenama kreditne politike i sa nesposobnošću dužnika da vrati kredit, ali i pod dejstvom takvih faktora kao što su deregulacija, moralni hazard, porast finansijskog kriminala kao i ulaskom banaka u poslove koji ranije nisu bili tradicionalno bankarski (npr. poslovi lizinga i brokersko-dilerski poslovi).

U današnje vreme Internet pruža korisnicima usluge digitalne ekonomije koja nudi novu fleksibilnost u izboru opcija kao što su Internet bankarstvo i Internet trgovina, kao i razne druge finansijske usluge. Digitalna ekonomija je ekonomija koja se zasniva na razmeni elektronskih dobara i usluga. U digitalnoj ekonomiji kompanije posluju sa svojim partnerima i klijentima i sprovode transakcije putem Internet (web) tehnologija, odnosno Interneta. Dobro je poznato da se na digitalnom tržištu prenose veliki novčani iznosi i da digitalni „posao" ubrzano raste svake godine. Uz rastuću digitalnu ekonomiju, pojavljuje se i sve više kriminalnih aktivnosti vezanih za nju. Očigledno je da se sve više novca prenosi putem Internet bankarstva te da je broj sajber (*cyber)* kriminalaca u porastu. *Sajber* kriminalci su kriminalci koji koriste slabosti Interneta i računarskih aplikacija kako bi učinili kriminalno delo, kao što je npr. pljačka banke. Banke više ne drže velike svote novca u svojim sefovima i fizičke pljačke banaka su vrlo riskantne. Kako bi izbegli taj rizik, kriminalci pribegavaju sajber pljačkama.

Napadači koriste nekoliko metoda prikupljanja informacija potrebnih za izvođenje pljački. Jedna od njih je npr. pecanje podataka ili fišing (*phishing)* tehnika napada. Fišhing se zasniva na slanju lažiranih poruka elektronske pošte u kojima se navode korisnici da otkriju osetljive podatke (npr. PIN-ove sa kreditnih kartica). Osim primene fišing napada, pljačkaši mogu koristiti posebne zlоćudne programe, kao što su *trojanski konji.* Takvi programi se instaliraju na korisnikov računar, prate njegove navike i prikupljaju podatke potrebne za pristup korisnikovom sistemu Internet bankarstva i obavljanju novčanih, platnih transakcija. Pri tom se služe alatima za praćenje unosa znakova sa tastature (*keylogger*). Ukoliko je pljačka uspešna, napadači dobijaju veliku količinu novca uz vrlo mali rizik jer se veoma retko otkrivaju. Mnoge velike kompanije, a posebno banke često skrivaju činjenicu da ih je neko opljačkao elektronskim putem zbog toga što bi to značilo da njihovi sistemi nisu dovoljno sigurni i time višestruko uvećali reputacioni rizik. Uz to, takav zaključak mogao bi da izazove paniku kod klijenata banke gde bi mnogi od njih povukli svoja sredstva iz banke (tzv. juriš na banke) što bi ako dovoljno klijenata to učini moglo dovesti i do propasti banke.

U kontekstu prethodno navedenog ovaj rad razmatra specifične vrste operativnog rizika u Internet bankarstvu vezane za mogućnost nastanka eksternih prevara. Razmatraju se rizici napada na bankarske Internet sisteme i zloupotrebe bankarskih proizvoda i usluga. Opisane su vrste zlоćudnih programa koje napadači koriste za sajber pljačke, dati su primeri fišing napada. Takođe, razmatraju se posledice napada i preporučuju se mere zaštite na nivou banke i na nivou zaštite korisnika usluga Internet bankarstva.

Fast development of information technologies and the expansion of the communication networks, but especially the application of new mobile technologies, offered the options to users to access, from any given place and at any given time, a large quantity of information. With the application of new technologies banks are increasingly using the options offered by the electronic banking (e-banking). Today, this has become an imperative, not only for the cost reduction purposes of the banking operations, but primarily with the objective of maintaining the competitive advantages and expanding their consumer base. The banks, when offering electronic banking services, are faced with certain risks, among them outstanding being the strategic, operational, reputation, legal and cross-border risks. Modern banking is daily exposed to the above mentioned existing (identified and recorded) risks, but also to new risks, i.e. the risks of unforeseen events. The risks, as an inherent possibility of absolute or relative loss in respect to expectations in any banking operation, are the characteristic feature of every banking transaction, nowadays the very mastering of new instruments, techniques and strategies, together with the introduction of new banking products and services, but especially the venture into and the conquest of the Internet market, prompted that list of risks to acquire a constant upwards trend. The uncertainty is growing due to the changes in the society and the economy, the changes in interest rates, and changes in crediting policies, and the incapacity of obligor to service debt liability, but also due to the impact of such factors as the deregulation, moral hazards, growth of financial crime and the venture of banks into dealings that have not been in the past component parts of traditional banking (for example, leasing operation, and brokering-dealing jobs).

At present, Internet is making available to users various services of the digital economy, which in turn offers new flexibility in the choice of options, such as the Internet banking and the Internet trading, but also a variety of other financial services. Digital economy is the economy based on the electronic exchange of goods and services. In the digital economy, companies are dealing with their counterparts and clients and are conducting transactions via the internet (web) technology, i.e. through the Internet. It is well known that on the digital market there are transfers of large amounts of money and that the digital "trade" is increasingly growing every year. Together with the growth of digital economy, what also appears are the fast progressing criminal activities connected with it. It is evident that there are enormous sums of money transferred through the Internet banking and that the number of cyber criminals is also on the rise. Cyber criminals are those criminals that are using vulnerability of the Internet and computer applications for committing criminal offences, for example, bank robberies. Banks are no longer holding vast sums of money in their strongholds and the physical bank robberies are very risky. Therefore, in order to avoid such risks, criminals are resorting to the cyber theft.

Attackers employ several methods in collecting information necessary for committing larceny. One of them, for example, is data phishing as an attack technique. Phishing is based on sending scam electronic mail messages where the users are induced to reveal their sensitive data (for example, PIN codes of their credit cards). In addition to phishing attacks, burglars may also use some special malignant programmes, such as *Trojan horses*. These programmes are installed in the user's computer, keeping a follow up on the user's lifestyle and routine, and gathering data needed for the access to the user's Internet banking system and the way user conducts his payment transactions. In doing this, assailant is using tools for monitoring user's keyboard input (*key logger).* If the theft is successful, attackers obtain a large amount of money with a very low risk as they are very seldom discovered. Many major companies, and especially the banks, are often concealing the fact that they have been robbed electronically, because that would designate that their systems are not sufficiently safe and thus they would have a manifold increase of damage caused to their reputation risk. In addition, such a conclusion could cause panic amongst the bank clients leading them to withdraw their funds from the bank (the so-called rush on banks) which could, in turn, cause the bank to collapse if sufficiently large

Operativni rizik u bankarstvu

Banke su se oduvek štitile od ključnih pretnji za njihove operacije kao što su pljačke i interne prevare. Do nedavno, upravljanje ovakvim pretnjama je bilo fokusirano na praktične tehnike za minimiziranje šanse gubitaka, bilo da je to podrazumevalo službu fizičkog obezbeđenja banke, osiguranje nezavisnosti tima za internu reviziju ili izgradnju robusnog IT sistema. Samo su neke banke nastojale ili da utvrde nivo operativnog rizika kojima su izložene ili da tim rizicima upravljaju sistemski kao posebnom kategorijom rizika. Međutim, pod uticajem *Bazela II*, situacija u pogledu tretmana operativnog rizika banaka se drastično promenila. Danas banke ulažu ogromnu energiju u upravljanje širokim spektrom operativnih rizika na agregatnom (portfolio) nivou i nastoje da rizik direktno povežu sa ekonomskim kapitalom korigovanim za rizik (*risk-based capital*), koga formiraju za pokriće neočekivanih gubitaka (Đukić, 2007).

Sveobuhvatno upravljanje operativnim rizikom banke podrazumeva identifikaciju, evaluaciju, kontrolu (redukciju), monitoring i formiranje adekvatnog kapitala za pokriće izloženosti operativnom riziku na nivou banke kao celine. Proces upravljanja operativnim rizicima započinje njihovom identifikacijom. Identifikacija je ključna faza u procesu upravljanja operativnim rizikom zbog toga što treba da dovede do proaktivnog umesto reaktivnog delovanja na rizike. Cilj identifikacije jeste da se utvrdi izloženost operativnim rizicima i da se ista dokumentuje. Svaka banka mora identifikovati postojeće i potencijalno najveće ili najznačajnije izvore operativnih rizika i mora ih pratiti po poslovima u skladu sa sopstvenom organizacijom (npr. za poslove sa privredom, poslove sa stanovništvom, brokerske poslove i sl.), u cilju formiranja baze istorijski relevantnih podataka o operativnim rizicima. Proces formiranja baze podataka za uspešnu evaluaciju operativnih rizika je relativno dug iz razloga što treba da prođe barem 3 - 5 godina da se prikupe svi relevantni podaci. Prema tome, identifikacija rizika je najvažnija pretpostavka za razvoj efikasnog i održivog sistema za kontrolu i monitoring operativnog rizika. Specifikaciju poslova i/ili događaja u kojima postoji izloženost operativnim rizicima (poslova i/ili događaja koji mogu prouzrokovati operativne rizike i gubitke) treba detaljno utvrditi i dopunjavati kao i šifrirati radi lakšeg praćenja. Identifikaciju treba vršiti kontinuirano i prilagođavati je promenama u banci i okruženju. U skladu sa preporukama Bazelskog komiteta za superviziju banaka (BCBS), moguća su 4 pristupa u identifikaciji operativnih rizika i to (BCBS, 2003):

- razvrstavanje rizika - risk mapping,
- indikatori rizika,
- merenje i
- samoprocenjivanje s obzirom na katalog potencijalnih izloženosti operativnim rizicima

Risk mapping je proces koji se provodi kroz sve organizacione jedinice banke da bi se dobile informacije o izloženosti riziku tih jedinica, tipu rizika i njegovom nivou. Rezultat kvantitativnog mapiranja rizika je tzv. verovatnoća-uticaj dijagram (*probability-impact diagram*), tj. tipični dijagram frekvencije očekivanog gubitka u odnosu na uticaj za svaki tip rizičnog događaja ili liniju poslovanja.

Indikatori rizika su statistički i/ili metrički podaci, neretko finansijski, koji ukazuju na rizični profil svake organizacione jedinice (aktivnosti) i banke u celini. Takvi indikatori su: broj neautorizovanih transakcija kreditnim karticama, broj žalbi klijenata, stopa prometa po zaposlenom, frekvencija i/ili uticaj grešaka i propusta u procesuiranju transakcija, premije osiguranja, broj propalih trgovačkih transakcija, itd.

Neke banke mere svoju izloženost operativnim rizicima koristeći, npr., podatke koji se odnose na istorijske gubitke ili kombinuju te podatke sa eksternim podacima o gubicima, analizama scenarija i faktorima za evaluaciju rizika. Efikasan način da se ti podaci (informacije) dobro iskoriste jeste uspostavljanje sistema za monitoring i evidentiranje frekvencije i uticaja pojedinih slučajeva operativnih gubitaka i ostalih relevantnih podataka (informacija) o njima.

Najčešće korišćen pristup identifikaciji operativnih rizika jeste njihova identifikacija zasnovana na taksonomiji koju vrši sama banka. Polazna tačka je podela banke kao organizacije

number of clients is to close their accounts.

In the context of the above stated, this paper is examining specific forms of operational risks in the internet banking connected with the possibility of occurrence of external fraud. Risks of attacks on the Internet banking systems and the misuses of banking products and services are investigated. Types of malignant programmes are described that the attackers use for cyber theft and cases of phishing attacks are given. In addition, the consequences of attacks are examined and protection measures recommended at the level of the bank and at the level of the Internet banking services user protection.

Operational risk in banking

Banks have always protected themselves from crucial menace to their operations such as robberies and internal fraud. Until recently, managing such threats was focused on practical techniques for minimisation of loss incurring chances, either through the services of physical security in banks, or by insuring independence of the internal auditing team, but also by building up of robust IT systems. There were but a few banks that were striving to either determine the level of their exposure to operational risk, or to manage such risk in a systemic manner and as a separate risk category. However, under the influence of Basel II Accord, situation regarding the treatment of operational risks in banks has drastically changed. Banks today are investing enormous efforts in managing a broad spectrum of operational risks on an aggregate (portfolio) level and are trying to link the risk directly to the economic risk-based capital, formed for purpose of covering unexpected losses (Djukic, 2007).

Comprehensive operational risk management in banks covers identification, assessment, control (reduction), monitoring and setting up of capital adequacy for covering operational risk exposure at the level of the bank as a whole. Operational risk management process starts with risk identification. Identification is the key phase in the process of operational risk management as it is directed towards a proactive instead of a reactive action focused on risks. The objective of the risk identification is to determine operational risk exposure and to document the same. Every bank must identify both the existing and the potential greatest or most significant sources of operational risks and must conduct monitoring per business lines in accordance with its own organisational set up (for example, for corporate, for retail, for brokerage, etc.) for purpose of establishing a database of history of the relevant data on operational risks. The process of establishing database for a successful evaluation of operational risks is rather a lengthy one as it takes at least 3 to 5 year history in order to gather all the relevant data. Therefore, risk identification is the most important assumption for the development of an efficient and sustainable system for control and monitoring of the operational risks. Specification of jobs and/or events susceptible to operational risk exposure (jobs and/or events that may cause operational risks and losses) should be determined in detail and updated and coded for purpose of an easier follow up. Identification should be done on continuous basis and should be adjusted to the changes in the bank and in its environment. According to the Basel Committee for Banking Supervision (BCBS) recommendations, there are four possible approaches to the identification of the operational risks, as follows (BCBS, 2003):

- risk mapping
- risk indicators
- measurement, and
- self-assessment based on the catalogue of potential operational risk exposure

Risk mapping is a process that is implemented throughout all of the organisational units of the bank for purpose of obtaining risk exposure information of these units, type of risk and its level. The result of quantitative risk mapping is the so-called *probability-impact diagram*, i.e. a typical diagram of expected loss frequency in respect to the impact for each type of risk event or business line.

Risk indicators are statistical and/or metric data, not seldom financial ones, that are indicating the risk profile of every organisational unit (activity) and of the bank as a whole. These indicators are the following: number of unauthorised credit cards transactions, number of clients' complaints, turnover rate

na jedinice da bi se dobila bolja procena i bolji pogled na sve aspekte rizika. Identifikacija se može vršiti po (BCBS, 1998):

1. linijama poslovanja:
   - poslovanje sa privredom (*corporate finance*)
   - trgovina i prodaja (*trading and sales*)
   - poslovanje sa stanovništvom (*retail banking*)
   - komercijalno bankarstvo (*commercial banking*)
   - plaćanja i obračuni (*payment and settlement*)
   - agentski poslovi (*agency services*)
   - poslovi upravljanja imovinom (*asset management*)
   - brokerski poslovi sa stanovništvom (*retail brokerage*)
2. događajima u kojima postoji izloženost operativnom riziku:
   - interne prevare (*internal fraud*) - namerne aktivnosti, odnosno propusti, najmanje jedne osobe koja radi za banku ili u banci u svrhu sticanja sopstvene (ekonomske) koristi
   - eksterne prevare (*external fraud*) - (zlo)namerne aktivnosti trećih lica prema banci, u smislu podvala, zloupotrebe i/ili izbegavanja zakona, regulative, propisa i politike banke
   - odnos prema zaposlenim i bezbednost radnog okruženja (*employment practices and workplace safety*) - mogući gubici zbog neprimenjivanja (kršenja) zakona o radu i drugih regulativa vezanih za rad, zapošljavanje, zdravstvenu i socijalnu zaštitu i bezbednost na radnom mestu
   - klijenti, proizvodi i poslovna praksa (*clients, products and business practice*) - mogući gubici zbog nenamernih (nemarnih) propusta u ispunjavanju profesionalnih obaveza prema klijentima i/ili zbog prirode (konstrukcije) proizvoda/usluge
   - štete na fiksnoj imovini (*damage to physical assets*) - moguća oštećenja fiksne imovine (poslovne zgrade, infrastrukture i sl.) i ljudski gubici zbog prirodnih katastrofa/nepogoda i drugih događaja
   - prekid u poslovanju i pad informacionih i drugih sistema (*business disruption and system failures*) - mogući gubici zbog neadekvatnosti, neefikasnosti, lošeg funkcionisanja ili pada IT sistema banke i/ili sistema javnih/spoljašnjih usluga/informacija (provajdera)
   - izvršenje, isporuka i upravljanje procesima (*execution, delivery and process management*) - mogući gubici zbog nenamernih grešaka u procesima i/ili podršci upravljanju (uključeni su i odnosi sa poslovnim partnerima, klijentima i provajderima)

   i/ili
3. vrstama uzroka
   a) ljudski faktor (*people*)
   b) procesi (*processing*)
   c) sistemi (*systems*)
   d) eksterni faktori (*external causes*)

Operativni rizik u elektronskom bankarstvu

Operativni rizik u elektronskom bankarstvu proizilazi iz potencijalnog gubitka zbog manjkavosti u sistemu bankarske bezbednosti i integriteta. On se sve do implementacije *Bazel II* regulative, nije izdvajao kao posebna kategorija, što je otežavalo njegovo merenje, kontrolu i upravljanje. Pitanje bezbednosti sistema je od najvećeg značaja, jer uvek postoje mogućnosti raznih internih i eksternih napada na banku, tj. njen sistem i proizvode, a time se dovodi u pitanje i integritet klijenata banke.

Operativni rizik takođe može nastati i zbog zloupotrebe od strane klijenata ili loše dizajniranog sistema elektronskog bankarstva. U tom smislu, mogući su sledeći operativni rizici u elektronskom bankarstvu (Crouhy, Galai, 2006):

- Rizik bezbednosti sistema,
- Rizik dizajniranja, implementacije i održavanja sistema i
- Rizik zloupotrebe proizvoda ili usluga od strane klijenata

Rizici bezbednosti ili sigurnosti sistema se pojavljuju u vezi s kontrolom informacija pomoću kojih banka komunicira sa okruženjem, transfera elektronskog novca, kao i sprečavanja falsifikata. Primer mogućeg rizika bezbednosti jeste npr. neautorizovani pristup sistemu. Banke mogu da primene određene mere za

per one employee, frequency and/or impact of errors and faults in transaction processing, insurance premiums, number of failed trading transactions, etc.

Some banks are measuring their operational risk exposure by using, for example, data on historical losses or combining this data with data on external losses, scenarios analyses and factors for risk evaluation. The efficient way for these data (information) to be used properly is the establishment of a system for monitoring and recording frequency and impact of individual cases of operational losses and other relevant data (information) about them.

The approach most frequently used in the identification of operational risks is their identification based on the taxonomy made by the bank itself. Starting point is the division of the bank, as an organisation, into units in order to obtain better assessment and insight into all the risk aspects. Identification may be made according to the following (BCBS, 1998):

1. Business lines:
   - Corporate finance
   - Trading and sales
   - Retail banking
   - Commercial banking
   - Payments and settlement
   - Agency services
   - Assets management
   - Retail brokerage
2. Events with operational risk exposure:
   - Internal fraud - intentional activities, i.e. mistakes, by not less than one person employed at the bank, or present at the bank for purpose of acquiring personal (economic) gain;
   - External fraud - activities with malicious intent of third persons against the bank for purpose of fraud, misuse and/or evasion of laws, regulations, rules and bank policies;
   - Employment practices and workplace safety - possible losses from absence of application of laws (violation), labour law and other regulations governing labour matters, employment practices, healthcare and social protection and workplace safety;
   - Clients, products and business practices - possible losses due to unintentional (slack) errors in fulfilling professional obligations towards clients and/or the nature (structure) of product/service;
   - Damage to physical assets - possible damages caused to fixed assets (office buildings, infrastructure and similar), and human losses due to natural catastrophes/disasters and other events;
   - Business disruption and system failures - possible losses due to inadequate, inefficient, poor functioning or fall of the IT bank systems and/or fall of public systems and those of exterior services/ information providers;
   - Execution, delivery and process management - possible losses due to unintentional errors in processes and/ or management support (including relations with business counterparts, clients and providers);

   and/or
3. Types of causes
   a) Human factor - people
   b) Processing
   c) Systems
   d) External causes

Operational risks in electronic banking

Operational risks in electronic banking derive from potential losses caused by shortcomings in the banking security and integrity systems. Operational risk, until the Basel II Accord implementation started, was not singled out as a separate category of risks, which made its measurement difficult, as well as its control and management. The issue of system security is of the utmost importance as there are always possibilities for various internal and external attacks on the bank, i.e. on its system and products, thus also raising the question of integrity of the bank's clients.

Operational risk may also occur due to misuses by clients or because of poorly designed system of electronic banking. In this sense, it is possible to identify the following operational risks in electronic banking (Crouhy, Galai, 2006):

- Security system risk,
- System design, implementation and

upravljanje rizikom bezbednosti. Moguće je primeniti sigurnosne komunikativne mere, kao što su „*firewall*", lozinke, tehnologiju enkripcije i autorizaciju korisnika. Potrebno je da banka vrši testiranje na „ranjivost" sistema, kao i stalno proveravanje sistema na viruse.

Rizici dizajniranja, implementacije i održavanja sistema bitno utiču na razvoj sistema elektronskog bankarstva. Radi se o prekidima i/ili usporavanju sistema, što izaziva negativne posledice na klijente.

Zloupotreba proizvoda i usluga od strane klijenata ili trećih lica nije retka pojava. Zbog toga lične informacije klijenata banke koji učestvuju u elektronskom bankarstvu (broj kreditne kartice, broj računa u banci, i sl.) moraju biti posebno zaštićene prilikom transakcija elektronskog novca.

U nastavku teksta akcenat stavljamo na eksterne rizike Internet bankarstva i mere zaštite od delovanja istih.

Internet bankarstvo i motivi napadača

Poslednjih nekoliko godina beleži se porast sajber napada na banke. Sajber napad jeste napad na računarske resurse ili sisteme upotrebom neke od tehnika zloupotrebe ranjivosti tog sistema ili korišćenje korisnika računara kao posrednika za uspešno izvođenje napada. Napadači koriste različite vrste napada, inovativna sredstva i tehnike kako bi prevarili legitimne korisnike i opljačkali banke. Neke od metoda koje napadači koriste su krađa identiteta i/ili brojeva kreditnih kartica, korišćenje specijalnog programa tzv. kilogera, trojanskih konja, crva, virusa i drugih malicioznih programa. Napadači koriste jednostavnost, brzinu i fleksibilnost Internet bankarstva namenjenog klijentima banke za poboljšanje iskustva korišćenja bankarskih usluga. Američki FBI (Federal Bureau of Investigation) izneo je krajem 2009. godine podatke o značajnom porastu Internet prevara usmerenih na banke čiji su klijenti mala i srednja preduzeća (SMEs) i lokalne samouprave. Mnoge kompanije nisu svesne pretnje napada putem Internet bankarstva sve dok se ne desi slučaj pljačke.

S obzirom da napadači koriste ukradene identitete, brojeve kreditnih kartica i bankarskih računa za pljačku banaka, korisnici često nisu svesni da im je ukraden identitet i/ili broj računa u banci. U mnogo slučajeva kompanije ne uspevaju da vrate ukradeni novac. Napadači stalno usavršavaju tehnologiju za izvođenje sajber pljački, što otežava efikasnu primenu zaštita od takvih napada. Često se napadi pokreću zloupotrebom sigurnosnih propusta u računarskim programima instaliranim na personalnim računarima korisnika. Osim toga, napadači mogu iskoristiti i lakovernost korisnika i nagovoriti ih na odavanje osetljivih podataka koje mogu kasnije upotrebiti u pljački. Uočeno je da tipičan napad na banke sve češće uključuje direktan pristup aplikaciji Internet bankarstva, posle čega sledi trenutno prebacivanje dostupnih sredstava na račun pljačkaša. Osim toga, čest je slučaj krađe identiteta. U SAD-u je najčešći način prevare stvaranje lažnih bankarskih računa i kreditnih kartica kao i njihova upotreba u pljački bankomata. Razlike u infrastrukturi, tipična pitanja sigurnosti računarskih mreža i psihologija korisnika uvek će usmeriti napadače prema najslabijoj tački sistema u smislu sigurnosti prilikom planiranja i pokretanja sajber pljačke.

Prevare putem zloćudnih bankarskih programa

Programi za praćenje unosa znakova sa tastature - Kilogeri (Keyloggers)

Kilogeri (Keyloggers) predstavljaju špijunske programe koji prate i beleže svaki znak sa tastera koji korisnik pritisne. Dele se u dve grupe:

- alati u obliku softverskih paketa i
- uređaji koji se ugrađuju u sklopove računara

Programi za praćenje unosa znakova sa tastature se uključuju u lanac događaja između pritiska tastera na tastaturi i prikaza znaka na monitoru računara. Ovo se postiže na više načina:

- postavljanjem video nadzora,
- podmetanjem prislušnog uređaja u tastaturu,
- presretanjem znakova upotrebom samog računara,
- promenom upravljačkih programa tastature,
- promenom programa za obavljanje posebnih funkcija tastature (eng. *filter driver*),

maintenance risk, and
- Clients' misuse of products or services risk.

Security risk or the security system risk appears in connection with the information control by which the bank communicates with its environment, in the electronic money transfer operations, and in prevention of forgery. An example of the possible security risk is an unauthorised access to the system. Banks may apply certain measures for managing security risk. It is possible to apply safety communication measures, such as the *"firewalls"*, passwords, encryption technologies and user authorisation. It is necessary for the bank to conduct testing to the "vulnerability" of the system, and also to perform continuous system virus check-ups.

System design, implementation and maintenance risks have a significant impact on the development of the electronic banking systems. They are the risks of interruptions and/or of the slowing down of the system which causes negative repercussions for the clients.

Clients' misuse of products and services risk or by third persons is not an uncommon occurrence. Therefore personal information of the bank clients participating in the electronic banking (credit card number, bank account number, etc.) must be especially protected in the electronic money transactions.

Further in this paper we shall focus on the external risks of the Internet banking and the protective measures in this respect.

Internet banking and motivation of attackers

During the last few years, growth was recorded in the number of cyber attacks on banks. Cyber attack is an attack on the computer resources or systems by applying an abuse technique against a vulnerability of the given system, or the exploit of the computer user as an intermediary for the successful execution of the attack. Attackers are using various kinds of attacks, innovative tools and techniques in order to scam legitimate users and rob the banks. Some of the methods used by attackers are identity theft and/or theft of the credit cards numbers, application of special programmes the so-called key loggers, Trojan horses, worms, viruses and other malicious programmes. Attackers are using simplicity, speed and flexibility of the Internet banking provided to the bank clients for upgrading of experience in the use of banking services. The US FBI (Federal Bureau of Investigation) disclosed in late 2009 data on a significant growth of the Internet fraud against banks with clients small and medium enterprises (SMEs) and the local self-governments. Many companies are not even aware of the threat of attacks through the Internet banking until such a case of robbery occurs.

Mindful of the fact that the attackers are using stolen identities, credit cards numbers and bank accounts for the bank robbery, the users themselves are often unaware of their stolen identity and/or of their bank account number. In many cases companies are unsuccessful in retrieving the stolen money. Attackers are constantly upgrading and perfecting their technology for execution of cyber crimes, which is undermining an efficient application of protection against such attacks. The attacks are often triggered by the abuse of safety errors in the computer programmes installed on personal computers of the users. In addition, the attackers may also exploit the naivety of the users inducing them to disclose the most sensitive data that may be used later on in the burglary attack. It was observed that the typical attack on banks is increasingly acquiring direct approach to the Internet banking application, where the immediate aftermath is an instant transfer of accessible funds to the account of the robbers. In addition, there are frequent cases of identity thefts. In the USA the most familiar manner of fraud is the creation of false banking accounts and credit cards and their use in the theft at ATMs. Differences in the infrastructure, typical questions of the computer network security and the user psychology shall always direct the attackers towards the weakest points in the system, in the sense of security, during planning and setting in motion of a cyber robbery.

Malicious banking programme fraud

Keyloggers programmes

Keyloggers are the spying programmes keeping a follow-up and recording every sign pressed on the keyboard by the user. They can be divided into two groups:

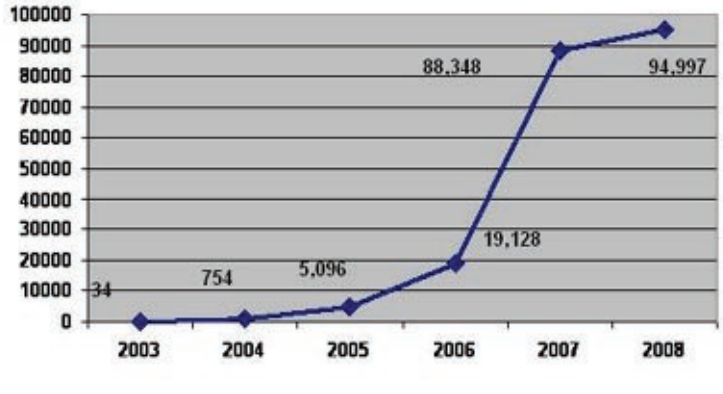
- presretanjem funkcija jezgre operativnog sistema ili
- presretanjem .dll datoteka (eng. *Dynamic-link library*) funkcija (.dll je dinamička biblioteka koja se koristi u operativnom sistemu Windows).

Sklopni uređaji za praćenje unosa znakova sa tastature su obično male veličine i postavljaju se u tastaturu na komunikacijski kabl koji povezuje tastaturu i računar ili u sam računar, dok se programski paketi sastoje od alata koji prate i beleže pritiske tastera na tastaturi.

Napadači koriste opisane programe kako bi preuzeli osetljive informacije kao što su brojevi kreditnih kartica, PIN-ovi, korisnički podaci i sl. Programi za praćenje unosa znakova sa tastature prikupljaju podatke i dostavljaju ih na posebne računare za odlaganje takvih podataka (*dropzones*) sa kojih ih napadač lako može preuzeti (Holtz, Elgenberth, Freiling, 2009). Moguće je otkriti računare na koja program šalje prikupljene podatke obavljanjem dinamičke analize upotrebom programa za analizu ponašanja zloćudnih programa (poput programskog paketa CW Sandbox i simulacijom zloćudnih programa u kontrolisanom okruženju) (CW Sandbox Program, 2010). Podaci dobijeni tim putem mogu se iskoristiti za automatsko otkrivanje računara za odlaganje podataka koje je prikupio program za praćenje unosa znakova sa tastature. Upotreba ove tehnike vrlo je uspešna. Jedan od problema programa koji prate isključivo unos znakova sa tastature je da se takvom metodom prikupe ogromne količine podataka koje treba poslati na računar kojim upravlja napadač, a zatim među njima treba naći korisne podatke (broj kartice, pin i sl.). Osim toga, potrebno je shvatiti u kojem kontekstu je pritisnut taster i odrediti da li je taster pritisnut kako bi korisnik uneo znak za lozinku ili kako bi, npr., napisao tekst u program Word. Napadači imaju izbor u korišćenju programa koji isključivo beleže pritiske tastera na tastaturi i/ili programe koji se aktiviraju na određenu ključnu reč, snimaju stanje monitora ili preuzimaju HTTPS tokove podataka. Zloćudni programi koji su napredniji od opisanih programa za praćenje unosa znakova sa tastature, a koriste iste u svom radu su trojanski konji o kojima će biti više reči u nastavku.

Trojanski konji (Trojan horses)

Trojanski konji su jedni od najjednostavnijih i vrlo raširenih oblika zloćudnih programa. Oni sadrže neku korisnu funkcionalnost i time privlače korisnika da ih preuzme na svoje računar i pokrene. Tom akcijom korisnik omogućuje napadaču pokretanje zlonamernog programskog koda, odnosno pristup određenim podacima na računaru ili čak preuzimanje kontrole nad celim računarom (zavisno od namene trojanskog konja). Trojanskog konja može izraditi sam napadač ili ga može preuzeti (kupiti) od nekog drugog napadača ili grupe. Posebno opasna vrsta trojanskih konja su bankarski trojanski konji koji su prvenstveno oblikovani za napad na bankarske sisteme, ali i berze akcija koje se oslanjaju na Internet za prenos podataka. Osnovna funkcija pomenutih trojanskih konja je krađa ličnih podataka žrtve, kao što su brojevi kreditnih kartica i PIN-ovi, kao i preuzimanje potpune ili delimične kontrole nad računarom korisnika. Napadači koriste različite tehnike, kao što je HTML injekcija, kako bi ukrali podatke potrebne za pljačku banke i ukrali PIN-ove, lozinke, korisničke račune, brojeve kreditnih kartica i druge osetljive podatke. HTML injekcija je ubacivanje HTML koda u odgovor web provajdera kako bi se izmenio sadržaj web stranice koju korisnik učitava. Trenutno ne postoji efikasna zaštita protiv njih pa se ni jedan korisnik Internet bankarstva ne može osećati potpuno sigurno. Naravno, postoje određene mere zaštite, ali ni jedna od njih ne pruža potpunu zaštitu (Search Financial Security, 2008).



Slika 1. Registrovani napadi bankarskim trojancima (2003-2008)

- Tools in the form of software packets, and
- Devises installed in the computer configuration

Keyloggers programmes are incorporated into the chain of events between the pressure made on any key of the keyboard and the presentation of that sign on the computer monitor screen. This can be achieved in several ways:

- by establishing a video monitoring,
- by planting a bugging device in the keyboard,
- by intercepting signs through the use of the computer itself,
- by the change of the keyboard driving programmes,
- by the change in the special keyboard function driving programmes (*filter driver),*
- by intercepting operative system core functions, or
- by intercepting Dynamic-Link Library function (dll is the dynamic library used in the Windows operative system).

Configuration devices for the follow-up on the input of signs from the keyboard are usually small in size and they are placed in the keyboard on the communication cable linking the keyboard with the computer or inserted into the computer itself, while the programme packages consist of the tools which are monitoring and recording pressures on the keys of the keyboard.

Attackers are using the above described programmes in order to seize sensitive information such as the credit cards numbers, PIN codes, user data, and similar. Programmes for the key logging are gathering data and sending them to special computers for depositing of such data (*dropzones)* where the attacker can easily take them over (Holtz, Elgenberth, Freiling, 2009). It is possible to uncover computers where the programme is sending the collected data by conducting a dynamic analysis through the application of the programme for analysis of malicious programme behaviour (programme packages like the CW Sandbox and simulation of malignant programmes in controlled environment) (CW Sandbox Programme, 2010). Data obtained in this manner may be used for automatic disclosure of the computer for data depositing - the dropzones, that it has collected from the key logger programme. Application of this technique has been very successful. One of the problems in the key logger programmes is that in such a method enormous quantities of data are being collected that are to be sent to the computer operated by the attacker, and thereupon amongst this multitude to find useful data (credit card numbers, Pin codes, etc.). In addition, it is also necessary to understand in which context the key was pressed on the given keyboard and to determine whether the key was pressed in order for the user to log-in the password or, for example, to write a text in the Word programme. Attackers are having a choice in the use of programmes which are exclusively recording key logging and/or programmes which are being activated at the use of a certain predetermined key word, which are recording the state of the monitor screen or are taking over the HTTPS data flows. Malignant programmes that are more progressive than the key logging programmes described here, but which are using the same in their particular work, are the Trojan Horses to be discussed in more detail further in this paper.

Trojan Horses

Trojan Horses are some of the simplest yet very widely dispersed forms of malignant programming. They contain a certain useful functionality thus attracting the user to take them into his computer and set them in motion. With this action, the user allows the attacker to start the function of the malignant programme code, i.e. access to certain computer data or even taking over the control of the entire computer (depending on the purpose for which the Trojan Horse is being used). Trojan horse may be designed by the attacker himself or may be taken over (purchased) by some other attacker or a group of attackers. Especially dangerous kind of Trojan horses are the banking Trojan horses which are primarily designed for the attacks on banking systems, but also on the stock exchanges which are relying on the Internet for data transfer. The basic function of the above mentioned Trojan horses is the theft of personal data of the victim, such as the credit card numbers and the PIN codes, but also taking over of either complete

Bankarske trojance obično izrađuju profesionalni sajber kriminalci, kao što je ruska grupa RBN (Russian Business Network) (RBN, 2010). Takvi trojanci koriste sve napredne tehnike za izbegavanje detekcije antivirusnim programima. Kako bi se suprotstavile, antivirusne kompanije razvijaju posebne algoritme kako bi se suprostavili ovim naprednim programima. Primeri ove vrste trojanskih konja su Sinowal, Bancos, Limbo, Zeus i dr. Primera radi, trojanski konj *Haxdoor.ki* je napao švedske i nemačke banke 2006. godine i prouzrokovao veliku finansijsku štetu bankama u tim zemljama (ZdNet, 2007). Trojanski konj je prikupio korisnička imena, lozinke i PIN-ove korisnika bankarskih usluga. Ovakav trojanski konj obično prilikom prikupljanja podataka prikazuje lažne informacije u dijaloškim prozorima korisnicima. Na primer, kada korisnik upisuje svoje korisničko ime i lozinku, trojanski konj se aktivira i prikazuje prozor u kome obaveštava korisnika da je pogrešno uneo podatke. U međuvremenu sprema korisničke podatke i šalje ih napadačima koji ih mogu iskoristiti. Mnogi bankarski trojanci kradu korisničke podatke, transakcijske brojeve (TAN) ili jednokratne lozinke (OTP - one-time passwords) i šalju ih poslužiocima kojima upravljaju napadači. Napadač se može prijaviti na sistem Internet bankarstva i prebaciti novac na račun koji mu pripada ili verovatnije prebaciti na račun koga nije moguće kontrolisati. Banke mogu da spreče ovakve napade upotrebom popisa lozinki, praćenjem nepravilnosti kod pristupa stranici i sl. Sve više banaka počinje da koristi poboljšane i sigurnije načine autentikacije, kao što je dvokoračna autentikacija, pa se napadači sve više usredsređuju na banke koje još uvek nisu poboljšale svoje sigurnosne mehanizme. Dvokoračna autentikacija može uključivati u prvom koraku upotrebu tekstualne i u drugom koraku grafičke lozinke. Ako je tekstualna lozinka ukradena, napadač ne može pristupiti računu jer ne zna grafičku lozinku. Mnoge banke u SAD-u još uvek ne koriste jednokratne lozinke ili neke druge bolje mehanizme prijave na sistem. To ih čini ranjivima na uobičajene programe za praćenje unosa znakova sa tastature i fišing (phishing) napade.

Preusmeravanje (Pharming)

Neki bankarski trojanci preusmeravaju korisnika prilikom prijave na Internet bankarstvo na lažnu web stranicu. Ova metoda napada naziva se preusmeravanje ili farming (*pharming).* Napadač oblikuje stranicu tako da ona oponaša web stranicu banke. Takva stranica takođe može služiti za napad s čovekom u sredini, menjajući sadržaj prometa koji se prenosi između bankarske stranice i korisnikovog web pretraživača. Postoji više različitih tehnika *farming* napada. Npr., trojanski konj može dodati nazive web stranica banke u datoteku sa IP adresama koje upućuju na zlonamernu stranicu. Dobar primer takvog trojanca je *Ohost.je*. Još jedna tipična metoda je presretanje funkcija iz biblioteke „wininwt.dll" u procesu web pretraživača Internet Explorer. Takođe, trojanac *Haxdoor* ima ovu opciju. Mnogi web pretraživači imaju opciju upozoravanja korisnika da web stranica koju posećuju nema valjani sertifikat. Bankarski trojanski konj koji izvodi *pharming* napade upotrebom funkcija „wininet.dll" u pretraživaču može zaobići dijaloške prozore o upozorenjima. Takođe, trojanski konj koji može menjati datoteke na korisničkom računaru, može i instalirati sopstveni sertifikat i na taj način sprečiti pojavu upozorenja.

Zloćudni programi sa više koraka

Postoje programi koji izvode napade na bankarske račune u više koraka. Prvi korak je početna infekcija računara. Zloćudni program se instalira na korisnikov računar ukoliko on poseti stranicu koja ga sadrži. Preuzeti program šalje svaki URL, odnosno adrese web stanica, koje korisnik poseti poslužiocu kojim upravlja napadač. U drugom koraku zloćudni program prati kriptovani promet web stranica, kao što je onaj koji se stvara prilikom posete web stranice za Internet bankarstvo. Takav promet se presreće i šalje prema napadačevom poslužiocu. U trećem koraku napadač analizira promet i zaključuje u kojoj banci žrtva ima račun. Zatim šalje žrtvinom računaru drugi program koji presreće pritiske tastera kada on pristupa stranicama za Internet bankarstvo. Sledeća slika prikazuje tok izvođenja napada u 3 koraka:

or partial control over the user's computer. The attackers are using different techniques, such as the HTML injection, in order to steal the data necessary for the bank robbery and stealing of PIN codes, user's bank account number, credit cards numbers and all other sensitive data. HTML injection is injecting the HTML code in the response of the web provider in order to change the contents of the web page loaded by the user. At present, there is no efficient protection against the Trojan horses, and thus not a single user of the Internet banking can feel completely safe. There are certain protection measures, of course, but none of them is offering complete protection (Search Financial Security, 2008).

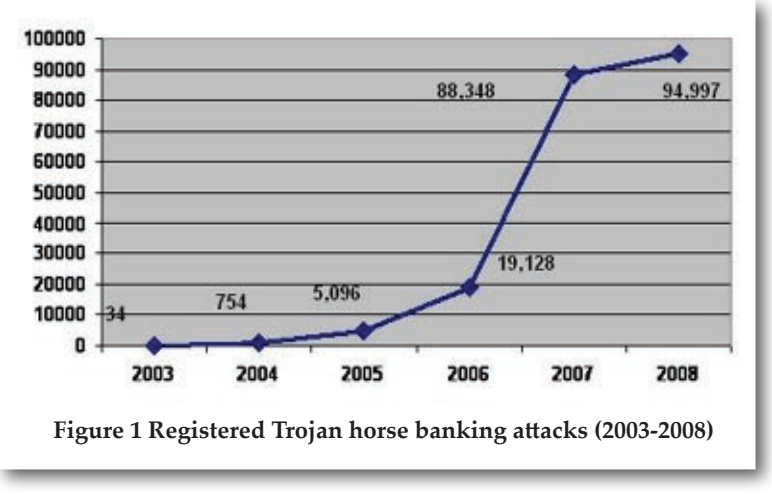
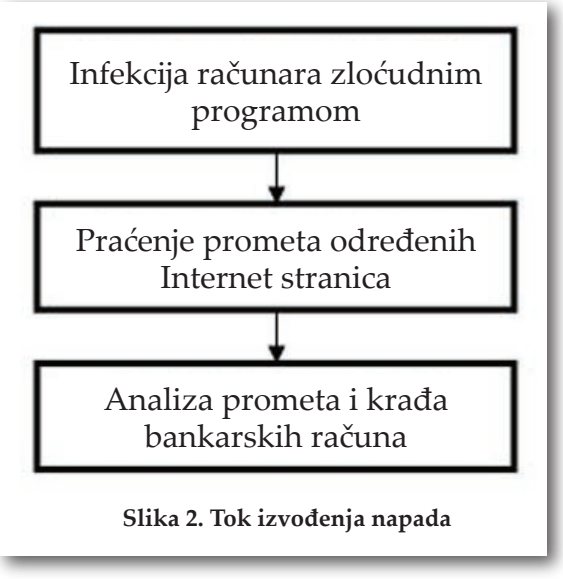


Figure 1 Registered Trojan horse banking attacks (2003-2008)

Trojan horses for banking attacks are usually designed by professional cyber criminals, such as the Russian group RBN (Russian Business Network) (RBN, 2010). Such Trojan horses are using all the state-of-the-art techniques for avoiding the detection by anti-virus programmes. In order to countermand such attacks, antivirus companies are developing special algorithms in order to challenge these advanced programmes. Examples of this kind of Trojan horses are Sinowal, Bancos, Limbo, Zeus, and others. To give an example, Trojan horse *Haxdoor.ki* made an attack on Swedish and German banks in 2006 and caused extensive financial damages to the banks in these countries. Trojan horse collected user names, passwords and PIN codes of the banking services users. Such a Trojan horse, when collecting data, usually would be presenting false information in the dialogue windows viewed by users. When the user would be logging his user name and password, for example, Trojan horse would activate and present the window informing the user that he made an error in entering data. In the meantime, he would be filing user data sending them to the attackers for their own use. Many banking Trojans are stealing user data, transaction numbers (TAN), or one-time passwords (OTP) and are sending them to the providers managed by the attackers. Attacker can apply to the Internet banking system and transfer money on the account that is his own or more probably on the account that is not possible to control. Banks can prevent such attacks by the use of lists of passwords, by monitoring irregularities in the access to the page, and similar. A growing number of banks are starting to use upgraded and more secure ways of authentication, such as a two-step authentication, so that the attackers are now increasingly focusing on those banks that have not as yet improved their safety mechanisms. Two-step authentication may include in the first step the use of textual, and in the second step the graphic password. If the textual password is stolen, the attacker can not access the computer without knowing the graphic password. Many banks in the USA still do not use the one-step passwords or some other better mechanisms for the access to the system. This is rendering them vulnerable to the usual programmes for the key logging and for the phishing attacks.

Pharming

Some of the banking Trojans are re-routing the user, when applying to the Internet banking, on to a false website. This method of attack is called re-routing or pharming. Attacker is designing the website page in such a way that it imitates the website page of the bank. Such a page can also serve for an attack with the man in the middle, changing the contents of the traffic which is transferred between the banking website page and the user's web browser. There are several different techniques for the *pharming* attack. Trojan horse, for example, may add names of the web pages of the bank to the



Slika 2. Tok izvođenja napada

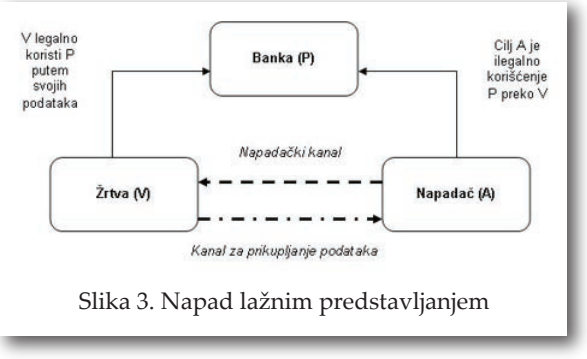
Na gore opisani način napadač saznaje informacije o korisničkom bankarskom računu, broj računa, lozinku i sl. Napadač ima sve potrebne elemente za pljačku i krađu identiteta. Korisnici se ne mogu potpuno zaštititi, ali mogu sprečiti prvi korak upotrebom antivirusnih programa koji sprečavaju preuzimanje zloćudnih programa sa sumnjivih stranica.

Prevare putem lažnog predstavljanja

U napadima lažnim predstavljanjem postoje tri glavna aktera i to su:

1) Pružalac usluga - P (npr. banka),
2) Žrtva - V (korisnik usluga banke)
3) Napadač - A.

Kako bi pružalac usluga, odnosno banka, osigurala isključivo autorizovani pristup svojim uslugama, ona obavlja autentikaciju pre dozvole pristupa svojim uslugama. Zbog toga ona dodeljuje korisnicima korisničke račune. Napadač želi da koristiti usluge banke pretvarajući se da je njen korisnik. Kako bi to učinio mora ukrasti lične podatke i korisnički račun. Prema tome, napadač uspostavlja komunikacioni kanal prema žrtvi za preuzimanje podataka. Osim pomenutog kanala, postoji još jedan komunikacioni kanal između napadača i žrtve. Taj kanal se koristi za pokretanje napada lažnim predstavljanjem i naziva se napadački kanal.



Slika 3. Napad lažnim predstavljanjem

Postoji više metoda za izvođenje napada lažnim predstavljanjem. Tipičan primer su fišing (*phishing)* napadi. Ukoliko se uzme primer fišing napada na korisnike banke (Slika 3.) pružalac usluge je banka i napadač želi podatke korisnika za prijavu na Internet bankarstvo. Napadački kanal je obično lažna poruka elektronske pošte koja upućuje korisnika na lažnu web stranicu. Web stranica je deo komunikacionog kanala za preuzimanje korisnikovih podataka.

Fišing (Phishing)

Fišing (Phishing) napadi podrazumevaju aktivnosti kojima napadači upotrebom lažnih poruka elektronske pošte i lažnih web stranica finansijskih organizacija (najčešće banaka) pokušavaju da korisnika navedu na otkrivanje osetljivih ličnih podataka. Pri tom se misli na podatke kao što su brojevi kreditnih kartica, korisnička imena, lozinke, PIN-ovi i sl. Termin fišing dolazi od engleske reči "phishing" kojom se metaforički opisuje postupak kojim neovlašćeni korisnici - napadači, sajber kriminalci mame korisnike Interneta kako bi dobrovoljno otkrili svoje podatke. Napadač može koristiti XSS (*Cross-site scripting*) napad i iskoristiti propuste u dizajnu web stranica za preusmeravanje žrtvi na lažne web stranice gde one (žrtve) otkrivaju osetljive podatke potrebne pljačkašu da dođe do novca ili nekih drugih ličnih podataka korisnika. Još uopšteniji oblik napada jeste oblik socijalnog inženjeringa gde napadač nagovara korisnika da kaže svoje podatke napadaču preko telefona.

database with IP addresses which are directing to the malignant web page. Good example of such a Trojan is the *Ohost.je*. Another typical method is the interception of the function from the library "wininwt.dll" in the process of the Internet Explorer web browser. In addition, Trojan *Haxdoor* also has this option. Many web browsers have the option which is warning the user that the web page to be visited does not have a valid certificate. Banking Trojan horse, executing *pharming* attacks through the use of the "wininer.dll" function in the browser, can circumvent the dialogue warning windows. In addition, Trojan horse that can change database in the user's computer can also install its own certificate and in this way prevent the warning from appearing.

Malignant programmes with several steps

There are programmes which are executing attacks on banking accounts in several steps. Step one is the initial infection of the computer. Malicious programme is being installed in the user's computer if he is to visit the web page which contains it. Programme which is taken over, in turn, is sending every URL, i.e. the addresses of the web pages which the user is visiting, to the provider controlled and managed by the attacker. Step two is when the malignant programme is monitoring encrypted traffic on the web pages, like the one which is created during the visit to the web page for Internet banking. Such traffic is intercepted and sent to the attacker's provider. Step three is when the attacker is analysing the traffic and finds in which bank the victim is having its account. Thereupon, the attacker sends to the victim's computer the second programme which is intercepting key logging when the victim is accessing web pages for the Internet banking. The figure that follows presents the course on an attack executed in 3 steps:

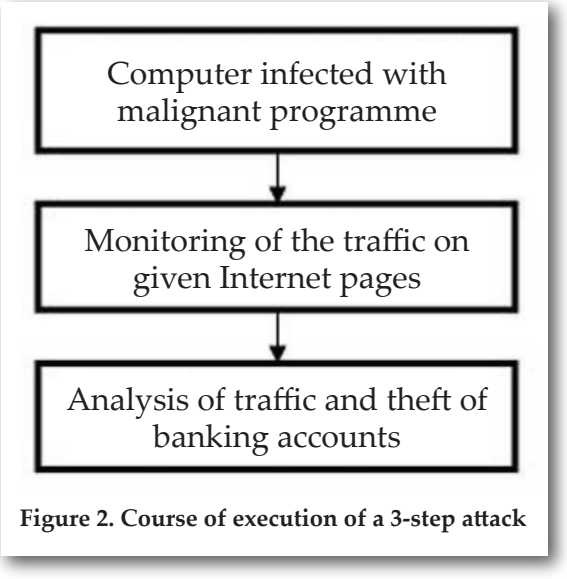


Figure 2. Course of execution of a 3-step attack

The attacker, in the above described way, obtains information about the user's bank account, the number of the bank account, the password, etc. Attacker now has all the necessary elements for plunder and theft of identity. Although the users can not fully protect themselves, they can prevent step one from taking place, by the use of anti-virus programmes which are preventing taking over of malignant programmes from suspicious pages.

Scams under false pretences

In the attacks under false pretences there are three main actors, as follows:

1) Services provider - P (for example, the bank)
2) Victim - V (user of bank services)
3) Attacker - A

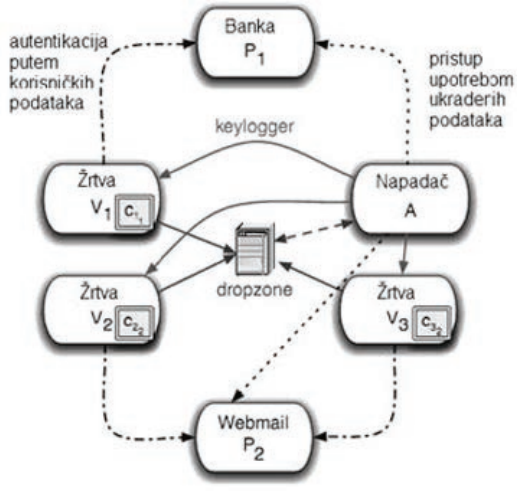
In order for the services provider, i.e. the bank, to secure an exclusive and authorised access to its services, it must conduct an authentication prior to granting access to its services. For this purpose the bank is allocating users their user accounts. Attacker, wishing to use bank services, pretends to be its user. In

Napadači mogu podmetnuti zloćudni program koga korisnik može preuzeti bez znanja posećivanjem zloćudne stranice ili svesnim kopiranjem sadržaja poruke e-pošte. Zloćudni program može sadržati program za praćenje unosa znakova sa tastature koji dostavlja podatke napadaču na poseban računar. Slika 5. daje primer *fišing* prevare ciljane na korisnike američkih banaka Citibank i Washington Mutual. U poruci e-pošte napadač tvrdi da pomenuta banka postavlja nove sigurnosne mere zbog kojih je potrebno potvrditi podatke o kreditnoj kartici. Kao što je to uobičajeno kod fišing prevara, žrtva se usmerava na lažnu web stranicu na koju unosi podatke o svojoj kreditnoj kartici bez znanja da ih upravo predaje sajber pljačkašu.

Slika 4. Tok fišing napada
(Izvor: Bank Safe Online, 2010)

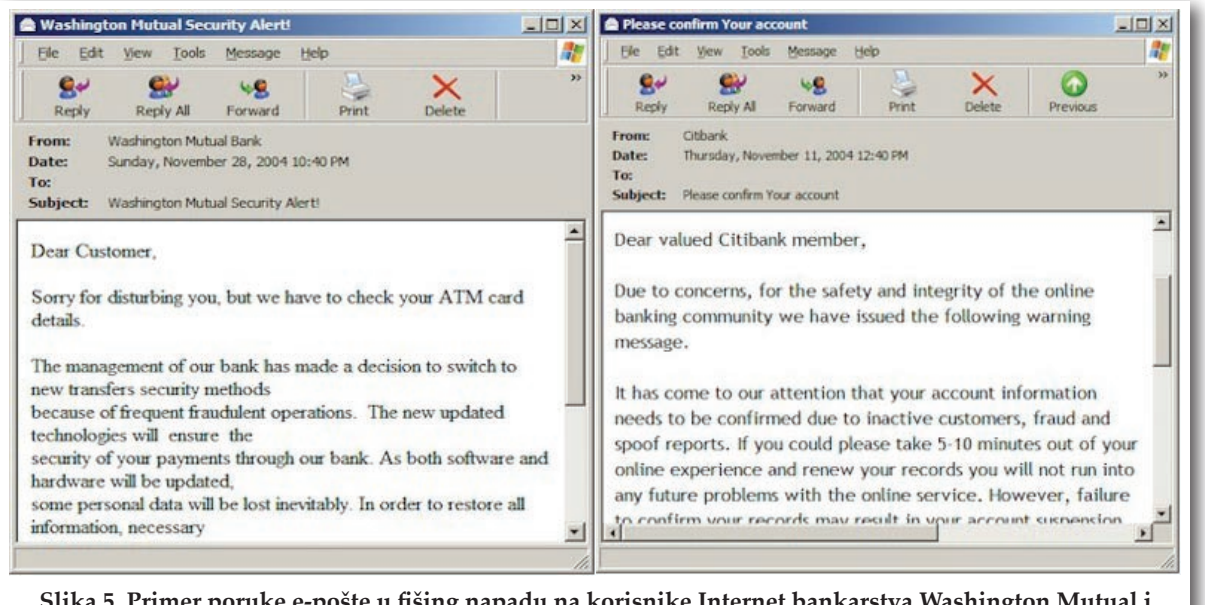
Lažno predstavljanje upotrebom kilogers (Keyloggers) programa

Na Slici 6. prikazan je pregled toka napada lažnim predstavljanjem upotrebom programa za praćenje unosa znakova sa tastature.



Slika 6. Shematski prikaz prikupljanja i transfera podataka
(Izvor: Holtz, Elgenberth, Freiling, 2009)

Svaka žrtva ima svoje korisničke podatke koje koristi za autentifikaciju kod pružaoca usluga (banke). Npr., na Slici 6. je $\mathbf{P}_1$ web stranica Internet banke i žrtva $\mathbf{V}_1$ koristi svoj broj računa i lozinku za prijavu na stranicu. Napadač A koristi različite tehnike kako bi zarazio svaku žrtvu **Vi** programom za



Slika 5. Primer poruke e-pošte u fišing napadu na korisnike Internet bankarstva Washington Mutual i Citibank
(Izvor: Phishing Scams, 2010)

order to accomplish this, he must steal personal data and the user bank account. Therefore, attacker establishes a communication channel towards the victim for taking over of the data. In addition to the said channel, there is yet another communication channel between the attacker and the victim. This channel is being used for setting in motion of the attack under false pretences and is called the *attack channel.*

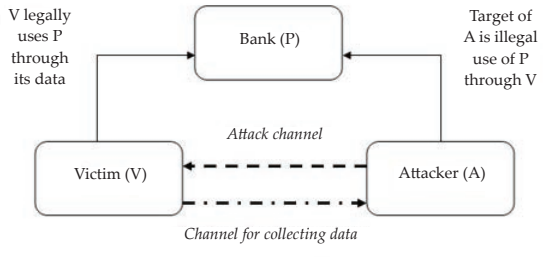


Figure 3. Attack under false pretences

There are several methods for executing an attack under false pretences. Typical example is the *phishing* attack. In the case of a phishing attack on the bank users (Figure 3), services provider is the bank and the attacker wishes to acquire user data for making his application for the Internet banking. Attack channel is usually a false message sent by electronic mail which is directing user to the false web page. Web page is a part of the communication channel for taking over of the user data.

Phishing

Phishing attacks are the activities where attackers, by using false electronic mail messages and false web pages of financial organisations (mostly banks), are trying to induce the user to disclose sensitive personal data. In this case, the information targeted are credit card numbers, user names, passwords, PIN codes, and similar. The term phishing derives from the English word "phishing" which metaphorically describes the acts of an unauthorised user - attacker, cyber criminal trying to induce and attract Internet users to voluntarily take the bait and disclose their data. Attacker may use XSS (*Cross-site scripting)* attack and use errors in the web site pages design for re-routing victims to false website pages, where they (victims) disclose sensitive data necessary to the robber in order to take the money or of some other personal data of the users. An even more general form of attack is the form of social engineering where the attacker is inducing the user to recount his data to the attacker over the telephone. Attackers may plant the malignant programme which the user may take over without knowing, when visiting the malignant web page, or by conscientious copying of the e-mail message content. Malignant programme may contain a programme for the key logging which is in turn sending data to the attacker on to his special computer. Figure 5 gives examples of the *phishing* scams aimed at the users of the American banks Citibank and Washington Mutual. In an e-mail message, the attacker is claiming that the said bank is putting in place new safety measures and therefore needs confirmation of data contained in the credit card. This being the usual case in phishing scams, victim is directed to the false web page for providing data on its credit card without having any knowledge that the data so disclosed is actually given to the cyber criminal.

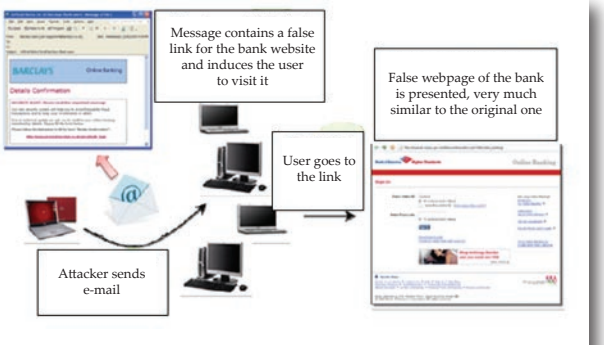


Figure 4. Course of execution of a phishing attack
(Source: Bank Safe Online, 2010)

praćenje unosa znakova sa tastature. On to može učiniti, na primer, slanjem poruka neželjene e-pošte (eng. *spam*) koje sadrže zloćudni program, ubacivanjem zloćudnog programa kada korisnik poseti zlonamernu web stranicu ili na neki drugi sličan način. Jednom kada je računar žrtve Vi zaražen, program počinje snimanje unosa znakova. Kako bi to ostvario, napadač mora prethodno da odredi koji će se pritisci tastera snimati, a koji ne. Npr., napadač definiše da se snima unos znakova samo kada se korisnik prijavljuje na web stranicu za Internet bankarstvo. Nakon što je program prikupio određenu količinu podataka šalje ih na posebne računare (dropzones) sa kojih ih napadač prikuplja i dalje koristi za lažno predstavljanje kao korisnik banke.

Bezbednost i zaštita Internet bankarskih sistema

Bezbednost predstavlja najveću brigu banaka koje nude usluge Internet bankarstva i najčešće je definisana kao kombinacija tehnologija, mera i postupaka zaštite informacija od neovlašćenog eksploatisanja i upada u sisteme. Savremene banke koriste četiri (4) osnovna sigurnosna servisa (Turner, Wunnicke, 2003):

- **Tajnost podataka** se ostvaruje šifriranjem, odnosno upotrebom kriptografskih algoritama.
- **Autentifikacija**, tj. proveravanje identiteta kojim se korisnik predstavlja. Ovo se može vršiti na razne načine: PIN-om (*Personel Identification Number*), pasword-om, biometrijskim metodama (otisak prsta i dr.), smart karticom.
- **Integritet podataka** predstavlja bezbeđivanje razmene finansijskih i drugih podataka između banke i korisnika tako da niko neovlašćen ne može iskoristiti ili izmeniti podatke. Integritet podataka se može obezbediti tehnologijama zaštite (SSL - *Secure Socket Layer*, S-HTTP - *Secure HyperText Transfer Protocol* i dr.).
- **Neporicanje (neodricanje) poruka**, servis koji sprečava pošiljaoca da porekne slanje i sadržaj poruke, odnosno primaoca da porekne prijem i sadržaj poruke. Veoma je bitna i zaštita mreže banke (*firewall*) i kontrola pristupa.

Od osnovnih i sveprisutnih sigurnosnih mehanizama koji se najčešće koriste u svim vidovima elektronskog bankarstva izdvajamo (4): šifrovanje (kriptografija), digitalni potpis, digitalni sertifikat i inteligentne (smart) kartice.

1. Šifrovanje (Kriptografija)
   Šifrovanje je transformacija originalne poruke pomoću odgovarajućeg postupka u nečitljivu formu za sve, sem za korisnika snabdevenog mehanizmom za dešifriranje. U postupku šifrovanja, u mehanizam šifrovanja ulazi originalna poruka i specifičan sadržaj koji se zove ključ. Dešifrovanje je inverzna transformacija kojom se od šifrovane poruke uz pomoć ključa i mehanizma za šifrovanje dobija ponovo originalni ili izvorni oblik poruke. Šifrovanje može imati dva oblika (Vuksanović, 2006):
   1. *Simetrično šifrovanje* (Metod jedinstvenog ključa) - Podrazumeva da su ključ za šifrovanje i ključ za dešifrovanje isti. Tajnost se zasniva na tajnosti ključa. Ključni problem je distribucija ključeva. Za više korisnika mora postojati više ključeva. Ovo nije pogodno za Internet kanale banke.
   2. *Asimetrično šifrovanje* (Metod javnih ključeva) - Podrazumeva dva ključa: javni i tajni. Postoji relacija između njih. Javni ključ se šalje kroz mrežu. Tajni se unosi samo kod dešifrovanja. Postupak rada je sledeći: javni ključ se pošalje drugome i on sa njim kriptuje poruku koju šalje. Sa njim se ne može dekriptovati poruka. Poruku može dekriptovati samo vlasnik tajnog ključa.
2. Digitalni potpis i *Hash* funkcija
   Poruka se može digitalno overiti tako što pošiljalac koristi svoj tajni ključ za overu - kako svog identiteta, tako i sadržaja poruke, čime se sprečava bilo kakva izmena poruke tokom prenosa. Ako bi neko neovlašćeno dopisao ili izmenio sadržaj poruke, primalac bi uz pomoć javnog ključa pošiljaoca otkrio neregularnost u poruci, što znači da je došlo do neautorizovane izmene poruke. Digitalni potpis kao nova metoda zaštite dobija se kombinovanjem dve tehnike - privatnog ključa i hash funkcije, kriptografske tehnike koja pomoću sažimanja poruke (digest) u hash rezultat pokazuje da li je poruka

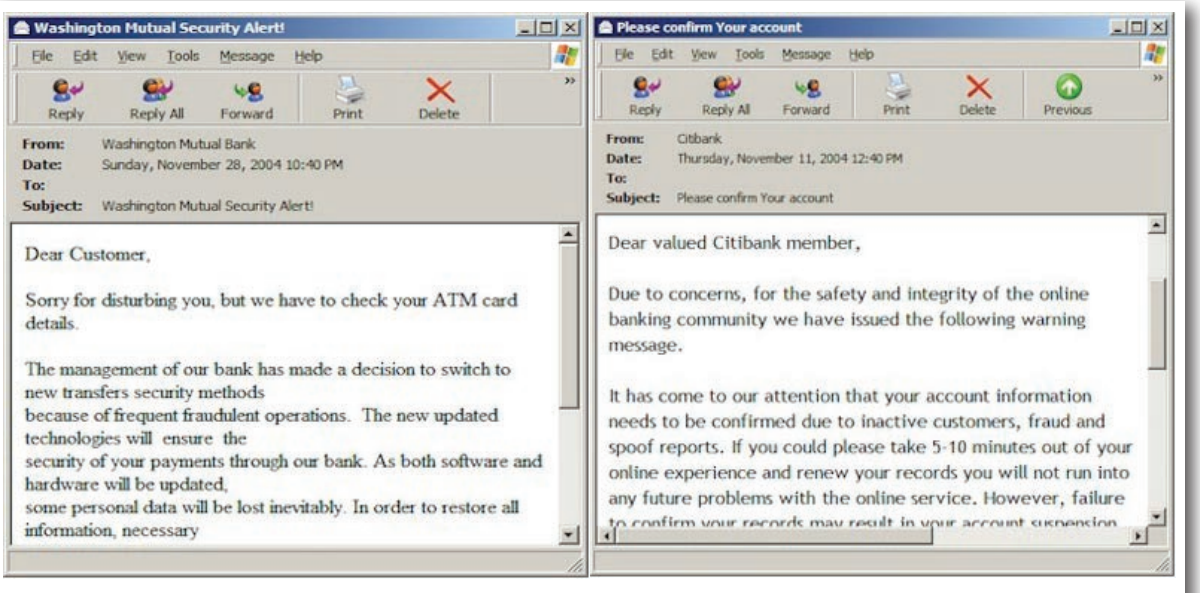


Figure 5 Example of an e-mail message in the phishing attack on the users of the Internet banking services of banks Washington Mutual and the Citibank
(Source: Phishing Scams, 2010)

False pretences with the use of the key logger programme

Figure 6 presents the course of an attack under false pretences with the use of the key logger programme.

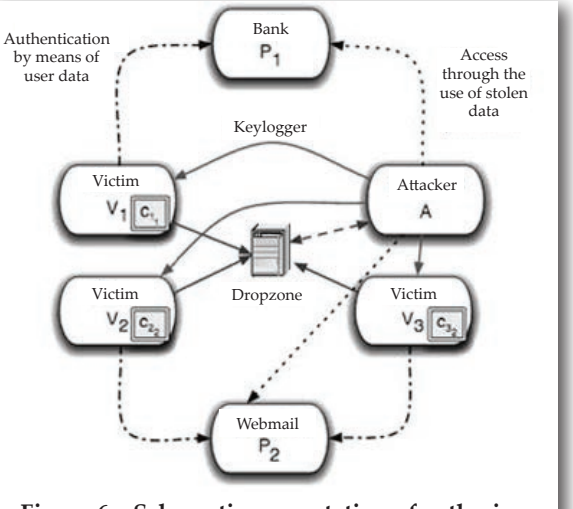


Figure 6 Schematic presentation of gathering and transfer of data
(Source: Holtz, Elgenberth, Freiling, 2009)

Every victim had its own user data used for authentication with the services provider (bank). For example, in Figure 6, P1 is the webpage of the Internet bank and V1 is using its account number and the password to visit the page. Attacker A is using different techniques in order to contaminate every victim Vi with the programme for key logging. He can do that, for example, by sending spam e-mail messages containing malignant programme, by injecting malignant programme when the user is visiting malignant webpage, or in some other manner. Once the computer of the victim Vi is contaminated, programme starts with recording key logging. In order to achieve that, the attacker firstly must determine which key logs will be recorded, and which ones will be disregarded. For example, the attacker defines recording to be done for key logging only when the user is applying for access to the webpage for Internet banking. Once the programme has collected a certain quantity of data, it is sending the data to the special computers (dropzones) from which the attacker is collecting them and using them further on for false pretences in the role of the bank user.

Security and protection of the internet banking systems

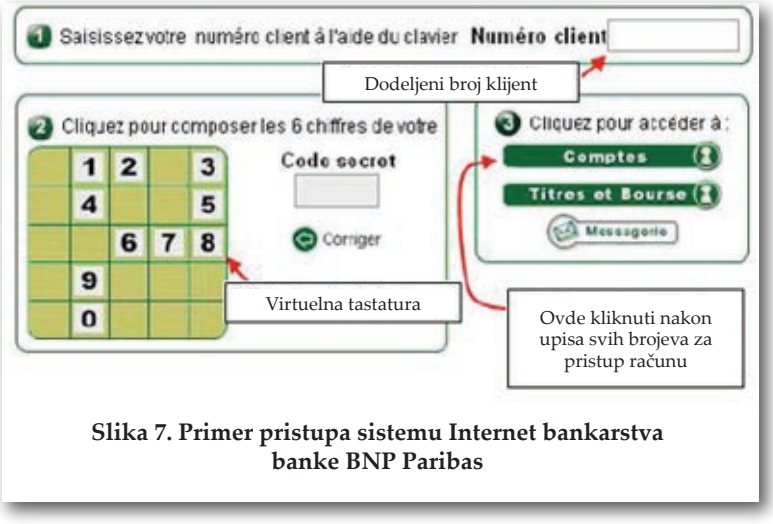
Security is the major concern of banks offering services of internet banking and is most often described as a combination of technology, measures and procedures for information protection from unauthorised exploitation and raids on the systems. Modern banks using four (4) basic security services (Turner, Wunnicke, 2003):

- **Data confidentiality** achieved by coding, i.e. the application of encrypting algorithms;

izmenjena u toku transfera. Pošiljalac uz pomoć javnog ključa primaoca vrši enkripciju originalne poruke i hash rezultata i još jednom vrši enkripciju ali sada pomoću svog privatnog ključa da bi obezbedio autentičnost i neopozivost (kriptovani tekst koji je spreman za slanje putem Interneta). Kada primalac primi poruku primenjuje hash funkciju (ako je bilo izmena u poruci, primalac će dobiti drugu hash vrednost od one koja mu je poslata). Dakle, samo pravi pošiljalac može da upotrebi svoj privatni ključ i potpiše poruku i samo pravi primalac može privatnim ključem da dešifruje kriptovanu poruku.

3. Digitalni sertifikat
   Infrastruktura javnih ključeva i kreiranje digitalnog sertifikata usmereni su na pitanje rešavanja identiteta u digitalnom prostoru. Suština rešenja bazira se na javnim ključevima i digitalnom potpisu. Ključni elementi ove infrastrukture su: digitalni sertifikat, sertifikaciona tela i registraciona tela. Digitalni sertifikat je lična karta u elektronskom prostoru. Sertifikat autoriteti (sertifikaciona tela - Certification Authority, CA) dokazuju identitet klijenta. Sertifikat mora da sadrži:
   - Naziv organizacije
   - Dodatne podatke za identifikaciju
   - Klijentov javni ključ
   - Datum do kog važi javni ključ
   - Ime CA koji je izdao sertifikat
   - Jedinstveni serijski broj.

   Ovi podaci se na kraju šifruju tajnim ključem CA.
4. Inteligentne (smart) kartice
   Autentifikacija podrazumeva dokazivanje identiteta korisnika. Identitet u okviru Interneta najčešće se dokazuje korisničkim imenom i lozinkom, odnosno tajnim ključem, a u poslednje vreme i inteligentnim karticama (smart cards), kao savremenijim i efikasnijim mehanizmom zaštite podataka. Ugradnja elektronskih čipova u plastične kartice je tehnologija stara dvadesetak godina, ali je masovna proizvodnja i primena inteligentnih kartica relativno novija. Jezgro inteligentne kartice čine mikroprocesor i memorija, na kojoj, osim opštih podataka, može biti zapisan i tajni ključ i može biti aktiviran samo uz pomoć vlasnika kartice, kako bi se izvršio odgovarajući kriptografski algoritam.
5. Ostali mehanizmi zaštite
   Pored prethodno navedenih bezbednosnih mehanizama, banke sa svoje strane primenjuju nove mehanizme zaštite od napada, kao što je upotreba virtuelnih tastatura, mada se i trojanski konji prilagođavaju novim sigurnosnim merama. Prilikom pristupa bankarskom računu preko sistema Internet bankarstva neke banke, kao što je BNP Paribas, koriste unos posebnog broja za pristup virtuelnoj tastaturi. Na takvim virtuelnim tastaturama raspored brojeva se svaki put menja kada korisnik pristupa stranici. Primer takve tastature dat je na Slici 7.



Slika 7. Primer pristupa sistemu Internet bankarstva banke BNP Paribas

Kako bitka između banaka i sajber kriminalaca traje a moglo bi se reći da će uvek trajati, jedino što preostaje krajnjim korisnicima Internet bankarstva jeste da zaštite svoje računare preko kojih pristupaju bankarskim sistemima na mreži. Kako bi se to postiglo korisnici moraju steći određena znanja o računarima i primeniti preporučene mere zaštite. Neke od njih su:

- zaobilaženje otvaranja linkovanih sajtova (eng. *link*) u sumnjivim porukama e-pošte (to su obično one poruke u kojima se traži odavanje ličnih podataka, PIN-ova i sl.),

- **Authentication,** i.e. verification of identity presented by the user. This may be done in several ways: PIN codes (Personal Identification Number), passwords, biometric methods (fingerprints, etc.), smart cards.
- **Data integrity** is a method securing exchange of financial and other information between banks and users in such a way that no unauthorised person may either use or change the data. Data integrity may be secured through protection technologies (SSL - Secure Socket Layer, S-HTTP - Secure HyperText Transfer Protocol, and others).
- **Undeniable message quality,** service preventing the sender from denying sending or the contents of the message, i.e. the recipient from denying the receipt and contents of the message. Very significant also is the protection of the bank network (*firewall)* and the access control.

Among the basic and omnipresent safety mechanisms which are most often used in all forms of electronic banking, we are singling out the following four (4): coding (encrypting), digital signature, digital certificate, and intelligent (smart) cards.

1. Coding (Encrypting)
   Encrypting is the transformation of the original message by means of an appropriate procedure, into an unreadable for all, except for the user supplied with the deciphering mechanism. In the deciphering procedure, the original message enters the deciphering mechanism and the specific contents that are called the key. Deciphering is an inverse transformation which renders from the encrypted message with the aid of the key and mechanism for deciphering again the original or initial form of the message. Encrypting may have two forms (Vuksanovic, 2006):
   1. *Symmetric coding* (Single key method) - Method where the key for coding and the key for deciphering are the same. Confidentiality is based on the secrecy of the key. The crucial problem is the key distribution. For several users there must be several keys. This is not suitable for the Internet bank channels.
   2. *Asymmetric coding* (Public keys method) - Method where two keys are involved: the public and the secret ones. There is a correlation between them. The public key is being sent through the net. The secret one is inserted only for the deciphering. Work procedure is the following: Public key is being sent to the other key, and together with it, the message it is sending is being encrypted. It can not be used for deciphering the message. The message may be deciphered only by the owner of the secret key.
2. Digital signature and *Hash* function
   The message may be digitally verified in such a way that the sender is using his secret key for verification - both of his identity and of the message contents, thus preventing any changes in the message during transmission. If any person should in an unauthorised way add or amend something to the message contents, the recipient by the aid of the public key of the sender would discover the irregularity in the message, which means that there had been an unauthorised amendment to the original message. Digital signature, as the new method of protection is obtained by combining the two techniques - of the private and of the hash function, encrypting technique which by the aid of digesting the message in the hash result is showing whether the message has been amended during the transfer. Sender, with the aid of the public key of the recipient, is doing the encryption of the original message and the hash result, and is once again doing the encryption but this time with the aid of his private key in order to secure the authenticity and undeniability of the encrypted text which is ready for sending by the Internet. When the recipient receives the message, he applies the hash function (if there were changes in the message, the recipient will receive the hash value that difers from the one that was sent to him). Therefore, only the true sender can use his own private key and sign the message, and only the true recipient can decipher the encrypted message with his private key.
3. Digital certificate
   Infrastructure of the public keys and the creation of the digital certificate are aimed

- upotreba filtera za neželjenu e-poštu (eng. *spam filter*),
- upotreba antivirusnih programa,
- upotreba zaštitnog zida (eng. *firewall*),
- primena najnovijih zakrpa i instalacija programa u kojima su ispravljeni sigurnosni propusti (eng. *update*),
- korišćenje *antispyware* programa,
- česte provere stanja bankarskih računa, kao i
- edukacija o bezbednosti na Internetu.

Edukacija o bezbednosti možda je i najvažniji savet korisnicima jer broj Internet prevara svakodnevno raste i korisnici moraju da budu svesni opasnosti koje vrebaju, kao i načina kojima se mogu zaštititi.

Internet bankarske prevare u svetu

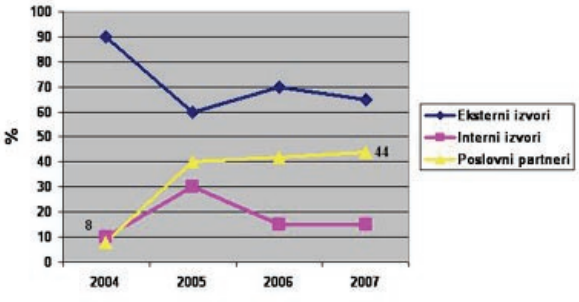
Po izveštajima organizacija koje se bave statističkim praćenjem Internet prevara i napada na računarske sisteme kao što su **Verzion** i **APWG Commited to Wiping Out Internet Scams and Fraud**, najveći broj napada i prevara dolazi od eksternih izvora tj. eksternih napadača i to 73% u 2008. godini. Po njihovim podacima najveći broj gubitaka podataka je posledica grešaka (62%) i eksternih napada i proboja u sisteme od strane sajber kriminalaca ili hakera (59%). Ostali podaci prikazani u **Tabeli 1.** ukazuju na značaj pretnji različitih vidova napada kao što su fišing, farming itd.

Tabela 1. Izvori i vrste uzroka gubitaka podataka

Izvori gubitaka podataka	Vrste uzroka gubitaka podataka
Eksterni izvori 73%	Greške 62%
Interni izvori 18%	Napad hakera i proboj 59%
Poslovni partneri (klijenti) 39%	Zlonamerni programi 31%
Više izvora 30%	Iskorišćenje ranjivosti 22%
	Fizičke pretnje 15%

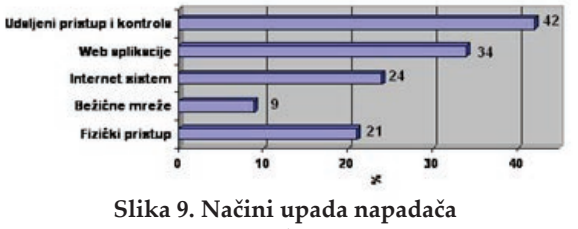
Izvor: Verizon business, 2008.

Ako pogledamo procenat napada koji dolaze iz eksternih i internih izvora kao i poslovnih partnera i klijenata (Slika 8.), možemo videti kako rizik koji donose osobe od poverenja beleži konstantan rast. Po podacima Verzion iz 2008. godine, napadi u 2004. godini koji su dolazili iz ove vrste izvora činili su svega 8% ukupnog broja napada, dok je u 2007. godini taj procenat porastao na 44%.



Slika 8. Promena udela izvora gubitaka podataka

Analiza načina proboja u sistem pokazuje kako najveći broj upada dolazi preko sticanja udaljenog pristupa i kontrole što predstavlja jedan od glavnih ciljeva tzv. socijalnog inženjeringa (SANS Institute, 2010). Procenat takvih napada, kojima prethodi sticanje prava pristupa je oko 42 % od ukupnog broja napada. Ostali podaci prikazani su na Slici 9.



Slika 9. Načini upada napadača
(Izvor: Verizon business, 2008.)

Po izveštaju o bezbednosnim pretnjama na Internetu organizacije X-Force iz 2009. godine, značajan deo pretnji pretstavljaju fišing napadi putem poruka e-pošte. Evidentno je da je udeo lažnih poruka znatan, pa se tako može zaključiti da fišing napadi nose visok rizik za bezbednost računarskih mreža i korisnika Interneta. Takođe, može se primetiti da broj fišing poruka raste pri kraju godine, gde sajber kriminalci pokušavaju da iskoriste praznike kako bi izveli napad (Slika 10.)

at the issue of resolving the identity in the digital space. The core of the solution is based on the public keys and the digital signature. The key elements of this infrastructure are the following: digital certificate, certification authorities and registration authorities. Digital certificate is an identity card in the electronic space. Certification Authority - CA is proving the identity of the client. The certificate must contain the following:

- Name of the organisation
- Additional data for identification
- Client's public key
- Date until the public key is valid
- Name of the CA issuing the certificate
- Single serial number

These data are ultimately encrypted with the secret CA key.

4. Smart cards

Authentication means proving the identity of the user. Identity within the Internet is most often proved by the user name and the password, i.e. by the secret key, and lately also by the smart cards as a more modern and efficient mechanism for data protection. Insertion of electronic chips in the plastic cards is a technology some twenty years old, but the mass production and application of smart cards is of a relatively later date. The core of smart card consists of a microprocessor and memory, where in addition to general data, one can inscribe also a secret key and such a key can be activated only with the aid of the owner of the card, in order to execute the corresponding encrypted algorithm.

5. Other protection mechanisms

In addition to the previously stated safety mechanisms, banks on their own side are applying new protection mechanisms from attacks, such as the deployment of virtual keyboards, although the Trojan horses are also adjusting to the new safety measures. When accessing a banking account through the system of Internet banking, some banks, such as the bank BNP Paribas, are using the insertion of a special number for the access to the virtual keyboard. On such virtual keyboards, the layout of number is changing every time when the user is accessing the webpage. An example of such keyboard is given on Figure 7.

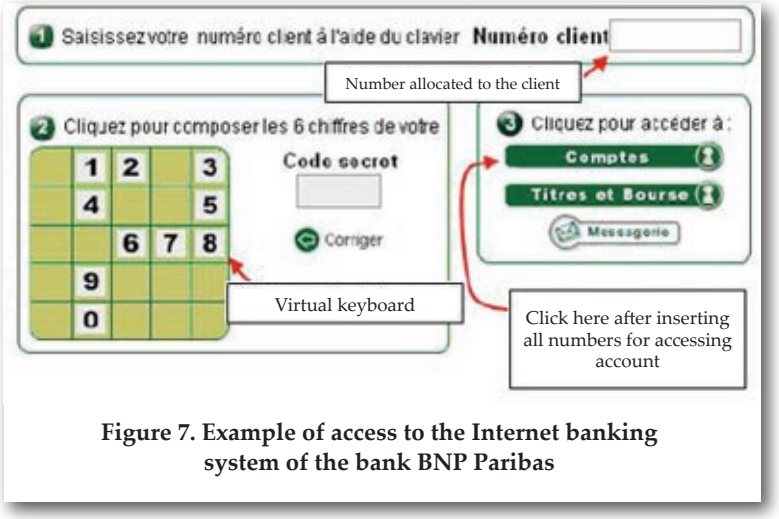


Figure 7. Example of access to the Internet banking system of the bank BNP Paribas

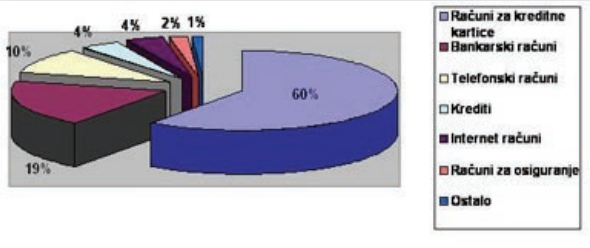
As the battle between banks and cyber criminals is still going on and it can well be said that it shall continue to eternity, so the final users of the Internet banking must protect their computers through which they are having access to the banking system on the net. In order to achieve this, users must master certain knowledge and skills about computers and apply the recommended protection measures. Some of them are the following:

- Avoidance of opening link sites in suspicious e-mail messages (they are usually those messages asking for the disclosure of personal data, PIN codes, etc.),
- Use of spam filters for undesired e-mails,
- Use of anti-virus programmes,
- Use of the firewall,
- Application of the latest updates and installation of programmes with corrected safety errors,
- Use of antispyware programmes,
- Frequent check-ups on the bank account balance, and
- Education on the Internet safety.

Education on the safety may be even the most important advise to be given to the users as the number of Internet scams is growing every day and the users must be well aware of the dangers that are present, but also of the ways they can use for protecting themselves.

Slika 10. Učešće fišing napada u neželjenim porukama e-pošte

Ukradene informacije i podatke napadači - sajber kriminalci najčešće koriste za oponašanje legitimnih korisnika i lažno predstavljanje. Prema izveštaju organizacije HIPAA, čak u 20 % slučajeva napadači su koristili podatke za stvaranje lažnih korisničkih računa u ime žrtve. Lažni korisnički računi su najčešće korišćeni kod prevara sa kreditnim karticama (60 %) i lažnim bankarskim računima (19 %) (Slika 11.)



Slika 11. Upotreba ukradenih podataka

Zaključak

Na osnovu svega prethodno iznetog, možemo zaključiti da osnova uspešnog upravljanja operativnim rizikom u Internet bankarstvu leži u kvalitetno sprovedenim merama i kontroli bezbednosti, kako na novou zaštite sistema banke tako i na nivou zaštite računara korisnika ovog vida bankarskih usluga. Kontrola bezbednosti obuhvata odgovatrajuću proveru identiteta, autorizacije, kontrolu logičkog i fizičkog pristupa, bezbednu infrastrukturu i verodostojnost podataka o transakcijama, dokumentacije i informacija. Pod pojmom provera identiteta podrazumevaju se tehnike, postupci i procesi za proveru identiteta i ovlašćenja klijenata. Identifikaciju čine tehnike, postupci i procesi u cilju utvrđivanja identiteta klijenta pri otvaranju i korišćenju bankarskog računa. Autorizacija predstavlja tehnike, postupke i procese za utvrđivanje legitimnosti pristupa klijenta ili zaposlenog određenom računu ili ovlašćenje za obavljanje transakcija na tom računu. Uzimajući u obzir činjenicu da se propisi o zaštiti privatnosti razlikuju od jedne države do druge, insistira se na pružanju određenog nivoa sigurnosti u pogledu objavljivanja ili deljenja informacija o klijentu sa trećom stranom. Utvrđivanje identiteta klijenta pri otvaranju računa smanjuje dejstvo eksternih rizika kao što su krađe identiteta, lažne prijave i pranja novca.

Na nivou banke, dokumentovana i pristupačna politika bezbednosti i standardizacija predstavljaju ključ dobre bezbednosne strategije bankarske institucije. Politika treba jasno da definiše opseg i sadržaj za svako područje poslovanja na koje se odnosi. Zajedno sa svakom politikom potrebno je specifikovati standarde koje treba uvesti kako bi se sprovele odredbe politike. Neki od uobičajenih delova sigurnosne politike u borbi protiv napada i prevara u Internet bankarstvu su:

- klasifikacija i rukovanje informacijama - osigurati pravilnu klasifikaciju poverljivih informacija kako bi one bile zaštićene od neovlašćenog pristupa,
- lična bezbednost - provera novih zaposlenih, kako bi banka bila sigurna da ne predstavljaju sigurnosnu pretnju,
- fizička bezbednost - obezbediti objekte znakovima i sigurnosnim uređajima za nadzor i sl.,
- pristup informacijama - procesi za generisanje sigurnih lozinki, udaljeni pristup i sl.,
- zaštita od virusa - sprovesti mere zaštite sistema od virusa i drugih zlonamernih pretnji
- treninzi za podizanje svesti zaposlenih o IT bezbednosti - kontinuirano informisati zaposlene u banci o pretnjama i merama zaštite,
- upravljanje kvalitetom - osiguravanje usklađenosti sa zakonima i standardima,
- politika o lozinkama - definisanje standarda za osiguravanje lozinki,
- reagovanje na incident - definisanje postupka reakcije i prijave incidenta,
- distribucija dokumentacije - rukovanje poverljivim podacima.

Jednom definisana politika mora biti lako

Internet banking scams in the world

According to the reports of organisations engaged in statistical monitoring of the internet scams and attacks on computer systems, such as **Verizon** and **APWG Committed to Wiping Out Internet Scams and Fraud,** the major number of attacks and scams comes from external sources, i.e. from external attackers, and this up to 73% in 2008. Their data shows that the largest number of data losses is the result of errors (62%) and external attacks and also penetration into systems by cyber criminals or hackers (59%). Other data presented in Table 1 indicate the importance of threats form various forms of attacks, such as phishing, pharming, etc.

Table 1 Sources and forms of data loss causes

Sources of data loss	Types of data loss causes
External sources 73%	Errors 62%
Internal sources 18%	Hacker attacks and penetration 59%
Business counterparts (clients) 39%	Malignant programmes 31%
Several sources 30%	Vulnerability exploited 22%
	Physical threats 15%

Source: Verizon business, 2008

If we are to look at the percentage of attacks coming from external and internal sources, and from the business counterparts and clients (Figure 8), we can see that the risk brought in by persons of confidence is recording a constant growth. According to the Verizon 2008 data, the attacks in 2004 coming from this type of sources amounted to only 8% of the total number of attacks, while in 2007 this percentage grew to 44%.

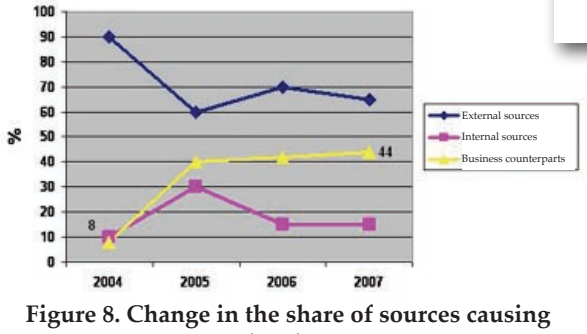


Figure 8. Change in the share of sources causing data loss

Analysis of the manner of system penetration shows that the largest number of attacks comes from acquiring remote controlled access which is one of the main targets of the so-called social engineering (SANS Institute, 2010). Percentage of such attacks, which are preceded by acquiring the right of access, is some 42% from the total number of attacks. Other data is presented in Figure 9.

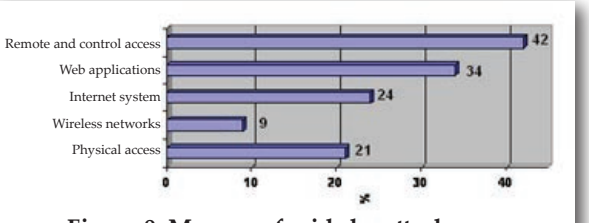


Figure 9. Manner of raids by attackers
(Source: Verizon business, 2008)

According to the report on security threats on the Internet, presented by the organisation X-Force in the year 2009, significant part of threats are the phishing attacks by means of e-mail messages. It was recorded that the share of scam messages is substantial so that it may be concluded that the phishing attacks are carrying a high risk for security of computer networks and Internet users. In addition, it can be observed that the number of phishing messages is growing by the end of each year, where the cyber criminals are trying to take the opportunity of the holiday season for perpetrating their cyber attacks (Figure 10).

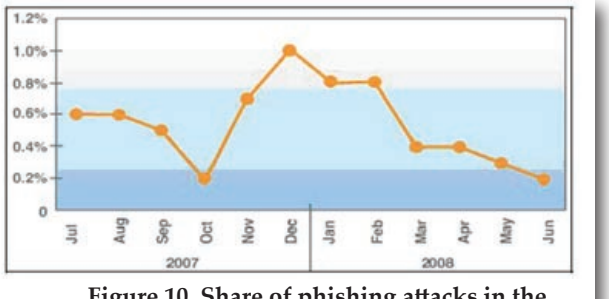


Figure 10. Share of phishing attacks in the scam e-mail messages

Stolen data and information the attackers - cyber criminals are most often using for copying legitimate users and for presenting themselves under false pretences. According to the report of the HIPAA organisation, even in as much as 20% of cases the attackers use data for creating false user accounts in the

dostupna svim zaposlenima. Takođe, potrebno je sprovoditi stalno ažuriranje i proveravanje bezbednosne politike kako bi se načinile nužne promeneu skladu sa novim odredbama ili pretnjama.

Sa aspekta zaštite korisnika usluga Internet bankarstva potrebno je istaći sledeće. Svaki korisnik Interneta može sprovesti određene mere zaštite od napada kao što su:

- upoznavanje značaja i vrednosti podataka - napadači se obično usmeravaju na korisnička imena lozinke i brojeve kreditnih kartica pa je potrebno oprezno rukovanje s tim podacima;
- provera identiteta sagovornika - napadači se obično usmeravaju na sticanje poverenja korisnika uveravajući ih kako se radi o njima poznatim osobama, saradnicima, nadležnim osobama, službenicima banke i sl.;
- zadržavanje tajnovitosti lozinke - lozinke treba čuvati u tajnosti i izbegavati njihovo zapisivanje ili otkrivanje drugim osobama;
- proveravanje poruka e-pošte - proveriti izvor poruke, sprovesti skeniranja antivirusnim alatom i sl.;
- izbegavanje upisivanja značajnih podataka na nesigurnim web stranicama - proveriti validnost web stranice pre upisa lozinke preko URL i drugih indikatora;
- neotkrivanje ličnih informacija - saznavanjem informacija o nekom korisniku sajber kriminalci se mogu fokusirati na njegove navike i hobije kako bi ga naveli na posećivanje lažnih web stranica;
- korišćenje *anti-phishing* zaštite - postoje alati koji proveravaju poruke e-pošte kako bi otkrili izraze koji su karakteristični za *phishing* poruke.

Na kraju možemo zaključiti da koliko je modernizacija bankarskog poslovanja doprinela poboljšanju fleksibilnosti i jednostavnosti pružanja usluga korisnicima, toliko je dovela do povećanja rizika u poslovanju koji svoje efekte imaju kako na banke tako i na klijente. Osvajanjem Internet prostora i pojavom ponude Internet bankarskih proizvoda i usluga, banke se suočavaju sa povećanim operativnim rizikom, javljaju se rizici nepredviđenih događaja kao i mnogobrojni problemi na strani korisnika. Javljaju se tzv. sajber pljačkaši koji su zamenili one tradicionalne, sve je veći broj proboja u sisteme i prevare korisnika usluga Internet bankarstva na bazi fišinga, farminga, ubacivanja zloćudnih programa itd. Rezultat toga svakako jeste gubitak novca za banku i za klijenta, a neretko i gubitak dobre reputacije i imidža banke. U svakom slučaju, danas postojeći sistemi i mehanizmi pružaju visok nivo zaštite od Internet bankarskih prevara i pljački, ali nijedan od njih ne može stopostotno zaštiti banku i klijenta.

name of the victim. False user accounts were most often used in scams with credit cards (60%) and false bank accounts (19%) (Figure 11).

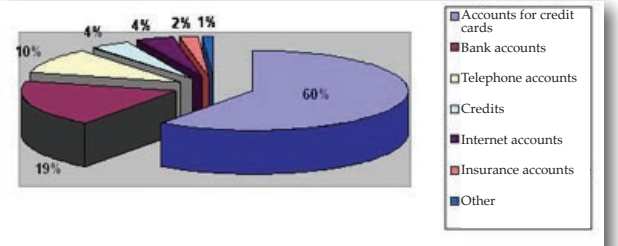


Figure 11. Use of stolen data

Conclusion

In the light of the above stated we are led to the conclusion that the basis for successful operational risk management in internet banking lies in qualitatively implemented measures and control of security, both at the level of the bank system protection and at the level of user computer protection in this type of banking services. Security controls cover appropriate verification of identity, authorisation, and control of logical and physical access, safety of infrastructure and credibility of data on transactions, documentation and information. The term identity verification covers techniques, procedures and processes for the check up on identity and authorisation of clients. Identification consists of techniques, procedures and processes aimed at establishing identity of the client during opening and using bank account. Authorisation comprises techniques, procedures and processes for establishing legitimate access of client or employee to a certain account or authorisation for executing transaction on that account. In view of the fact that privacy protection regulations differ from one country to another, the focus is placed on providing a certain level of security and safety when disclosing or sharing client information with a third party. Establishment of client identity during opening of the account reduces the impact of external risks such as identity theft, false applications and money laundering.

At the level of the bank, documented and accessible security and standardisation policy is the key to good safety strategy of the banking institution. Policy should clearly define the scope and contents for every area of operation where it is to be applied. Together with each policy it is also necessary to specify standards that are to be introduced in order to enable implementation of the policy provisions. Some of the typical parts of safety policy in the fight against attacks and fraud in internet banking are the following:

- Information classification and management - provide correct classification of confidential information in order to have them protected from unauthorised access;
- Personal safety - checking up of new employees in order to ensure that they are not a security and safety threat to the bank;
- Physical safety - secure buildings with signs and security surveillance devices, and similar;
- Access to information - processes for generating safety passwords, remote controlled access, etc.;
- Virus protection - measures to be implemented for the system virus protection and protection from other malicious threats;
- Trainings organised for raising awareness of employees about the IT safety - keeping the bank staff continuously informed of threats and protection measures;
- Quality management - ensuring compliance with laws and standards;
- Password policy - defining standards for password security;
- Incidents response - defining procedures in response to and reporting of incidents;
- Documentation distribution - handling of confidential data.

Once the policy is defined it must be made easily accessible to all the employed work force. In addition, it is necessary to conduct continuous updating and checking up on security policies and safety measures in order to make necessary changes in accordance with new regulations or threats.

From the aspect of internet banking services user protection, it is necessary to underline the following. Every user of the Internet may implement certain protection measures from possible attacks, such as follows:

- Getting to know the significance and value

Literatura / References

1. Basel Committee on Banking Supervision (BCBS), (2003), *Sound practices for the management and supervision of operational risk*, Bank for International Settlements (BIS), Basel http://www.bis.org/publ/bcbs96.pdf
2. Basel Committee on Banking Supervision (BCBS), (2003), *Risk Management Principles for Electronic Banking*, Bank for International Settlements (BIS), Basel, (http://www.bis.org/publ/bcbs98.pdf? noframes=1)
3. Basel Committee on Banking Supervision (BCBS), (1998), *Risk Management for Electronic Banking and Electronic Money Activities*, Bank for International Settlements (BIS), Basel http://www.bis.org/publ/bcbs35.pdf?noframes=1
4. Crouhy M., Galai D., Mark R., (2006), *The Essentials of Risk Management*, McGraw-Hill, New York
5. *CWSandbox program*, (2010) http://mwanalysis.org/
6. Data Breach Investigations Report (2008), Verizon business, http://www.verizonbusiness.com/resources/security/databreachreport.pdf
7. Đukić, Đ. (2007), *Upravljanje rizicima i kapitalom u bankama*, Beogradska berza, Beograd
8. Holtz, T., Elgenberth, M., Freiling, F., (2009) "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones", *Computer Security - ESORICS 2009*, Springer Berlin / Heidelberg, pp. 1-18.
9. Phishing, (2010) http://www.banksafeonline.org.uk/faq.html
10. Phishing Scams (2010), http://antivirus.about.com/od/emailscams/ss/phishing_5.htm
11. RBN, http://republicbroadcasting.org/, januar 2010.
12. Swedish bank hit by 'biggest ever' online heist (2007) ZdNet, http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm
13. Study of banking malware analyzes underground economy (2008), http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1343766,00.html
14. Vuksanović, E. (2006) *Elektronsko bankarstvo*, Beogradska bankarska akademija, Beograd
15. The Threat of Social Engineering and Your Defense Against It (2010) SANS Institute, http://www.sans.org/reading_room/whitepapers/engineering/the_threat_of_social_engineering_and_your_defense_against_it_1232
16. Turner, P., Wunnicke, D. (2003) *Managing the Risk of Payment Systems*, John Wiley & Sons Inc.

of data - attackers are usually focusing on the user names, passwords and credit card number, so it is necessary to exert caution in handling these data;

- Verification of the counterpart's identity - attackers are usually focused on gaining confidence of the users assuring them that they are well known persons by the users, their assistants, superiors, bank employees, and similar;
- Keeping password confidential - password must be guarded confidential and its writing down or disclosure to other persons must be avoided;
- Checking up on e-mail messages - check the source of the message, make scanning with anti-virus tools, and similar;
- Avoid writing significant data on unsecured web pages - check validity of the web page before inserting password through the URK or other indicators;
- Not disclosing of personal information - knowledge of information about a given user allows cyber criminal to focus of his habits and hobbies in order to induce him to visit false web pages;
- Using *anti-phishing* protection - there are tools for checking up on e-mail in order to discover terms characteristic for the *phishing* messages.

Finally, we can conclude that in as much as the modernisation of the banking operations has contributed to the flexibility and simplicity in offering services to users, so much has it also brought about a growth of risks in banking, having their impact both on banks and on bank clients. Mastering of the Internet space and the emergence of the offer for the internet banking products and services has forced the banks to face a growing operational risk, where risks appear from unanticipated events, but also many problems on the side of the users. The so-called cyber criminals are now surfacing to replace those traditional ones, and a growing number of hacking into systems and scams of users of the internet banking services, based on phishing, pharming, injection of malignant programmes, and other are occurring. The result is certainly the loss of money for the bank and for the client, but what also often ensue are a loss of reputation and a tarnished image of the bank. In any case, there are systems today and such mechanisms that are offering a high level of protection from the internet banking scams and fraud, but none of them is capable of offering a hundred percent protection for either the bank or its client.