# Крадење на идентитет и методи за намалување на ефектите на овој напад

Јасмина Смиљаноска, Моника Јанкоска, Митко Богданоски,

***Апстракт*— Крадење на идентитет преставува измама која напаѓачот ја користи со цел да се здобие со лични податоци на друго лице, како што се матични броеви, броеви од кредитни картички, социјални броеви и слично, и со тоа да добие пристап до ресурсите или бенефициите во име на тоа лице. Главен мотив при крадење на идентитет е профитот. Информациите кои се незаконски добиени со помош на овој тип на напад се искористени директно од извршителот на нападот или се препродаваат на трето лице. Во денешно време, за успешно реализирање на вакви напади, се користат различни алатки и методи, од лажни пораки (spam), лажни интернет страници, па се до употреба на тројанци и црви. Предмет на овој труд е да се разгледаат нападите со крадење на идентитет и начинот на кој што функционираат овие напади, како и да се опишат и анализираат методите кои се користат за спречување или намалување на ефектите од ваквиот тип на напади.**

***Клучни зборови*— крадење на идентитет, напаѓач, фишинг, pharming.**

## 1 Вовед

Пред дваесет години, терминот „крадење на идентитет“ бил малку користен, бидејќи бил и малку познат. Денес, тоа е широко препознатлив термин, кој е поврзан со феноменот кој го привлекол вниманието на јавноста, медиумите и владата, бидејќи станал сериозен општествен проблем. Овој термин денес често се опишува и како - „криминалот на новиот милениум“, „кошмарот на крадење на идентитет“, „типичен криминал на информатичкото време“, а крадењето на идентитет стана една од најчестите видови на криминал. Неговите влијанија може да бидат катастрофални и трауматични, како за финансиите, така и за самата личност (жртвата), а неговите ефекти се долготрајни. Напаѓачите, нивното влијание може да го прошират не само на индивидуалните жртви, туку, исто така, и на владите, бизнисите и општеството во целина.

Терминот „крадење на идентитет“, генерално се однесува на комбинација на неовластено собирање и измамничко користење на туѓи лични информации. Овој напад опфаќа голем број на активности, вклучувајќи собирање на лични податоци кои најчесто се превземени преку нелегален пат, создавање на лажни документи за идентификација и лажно користење на личните информации. Многу аналитичари истакнуваат дека терминот „крадење на идентитет“ најчесто се користи за да се означи терминот „измама на идентитет“, па затоа сметаат дека термините „крадење“ и „измама“ треба да бидат одделени.[1]

## 2 Крадење на Идентитет

Што всушност претставува крадењето на идентитет? Дали е можно да се даде точна и широко применлива дефиниција за овој термин? На прв поглед, се чини дека ова е релативно лесна задача. Но, во реалноста, предизвикот е тежок и сериозен.

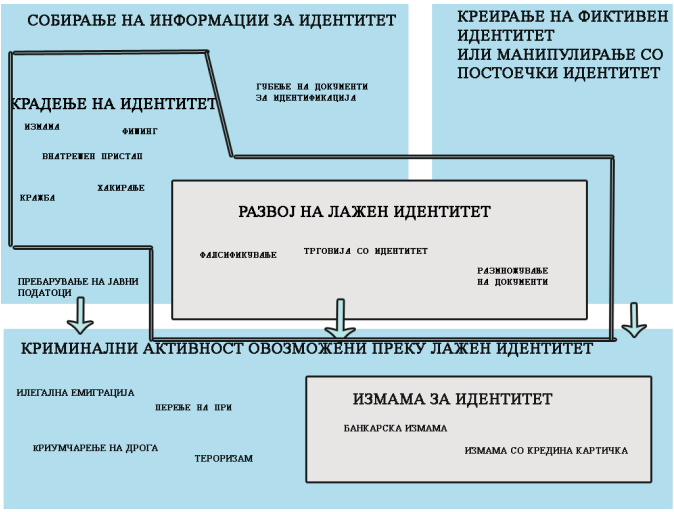
Авторот Lombardi го дефинира овој проблем на следниот начин: „Забуната во врска со дефиницијата на терминот *крадење на идентитет* расте со побрзо темпо отколку вистинската стапка на криминал, притоа заматувајќи ги вистинските причини и последици на поединците и бизнисите.“[2]

Крадење на идентитет, или измама за идентитет, се случува кога некој ги краде информациите што го дефинираат личниот идентитет, со тоа користејќи ги придобивките од украденият идентитет на жртвата. Тој може да се појави во многу форми. Една форма е кога се врши измамничка употреба на сметката на друго лице (на пример, број на кредитна картичка), со цел да се направат неовластени финансиски трансакции, без никакви дополнителни обиди да се имитира улогата на тоа друго лице. Овие видови на активности од страна на финансиската индустрија се класифицирани повеќе како измами со платежни картички, отколку како крадење на идентитет. Може да биде тешко да се направи разлика помеѓу обичните измами и она што е навистина крадење на идентитет.

Во случај на вистинско крадење на идентитет, крадецот ги проневерува информациите кои се однесуваат на идентитетот на едно лице - информации како што се име, адреса, телефонски број, датум на раѓање, моминско презиме на мајка, број на социјално осигурување (SIN), возачка дозвола или број на здравствена картичка, за потоа да се претстави во име на жртвата, ефикасно преземајќи го украденият идентитет. Крадецот може да извршува најразлични финансиски трансакции, да добива најразлични бенефиции, да обезбеди вработување, да врши кривични дела, па дури и да започне нов живот, најчесто во други земји, притоа користејќи го идентитетот кој го украл. Во некои случаи, со користење на украдени идентитети, може да бидат извршени уцени, тероризам, перење пари, шверц на луѓе, имиграција, разни измами меѓу кои и измами поврзани со дрога, при што криминалците се кријат позади некој туѓ идентитет со цел

избегнување на откривање на нивниот вистински идентитет. Е-поштата на жртвата, исто така, може да се користи за испраќање заканувачки пораки или пораки со клевети. Сето ова е различно од едноставното користење на личните информации за сметката, како што е бројот на кредитната картичка, за да се направат неовластените трансакции.

На следната слика е прикажан модел за дефинирање на терминот крадење на идентитет, кој е предложен од Sproule и Archer [3]. Крадење на идентитет опфаќа собирање на лични податоци и развој на лажни идентитети. Измамата за идентитет пак, се однесува на употребата на лажен идентитет за извршување на измама.




Слика 1 – Модел на крадење на идентитет

Така, според овој предложен модел, крадењето на идентитет се дефинира како процес кој вклучува две фази:

1) Неовластено собирање на лични информации: крадењето на идентитет започнува со отуѓување на лични информации на поединец, без согласност и често без знаење и тоа помош на крадење, измама или залажување. Информациите може да се користат веднаш, да се чуваат за подоцнежна употреба или да се предадат за употреба од страна на некој друг.
2) Лажното користење на тие лични информации, за да се здобијат со корист од сметката на поединецот на кој припаѓаат украдените информации: крадењето на идентитет продолжува со лажно користење на личните информации, обично за финансиска добивка. Крадецот го присвојува идентитетот на жртвата, со цел да добие кредит или друга корист во нејзино име. Главен белег на крадењето на идентитет е повторувачка виктимизација – каде крадецот обично ќе се вклучи во серија на измами користејќи го истиот присвоен идентитет.

Според ова, може да се каже дека терминот крадење на идентитет може да се користи и за двата случаи, и кај неовластено собирање на лични информации, како и при употребата на тие информации за измама/серија на измами, користејќи го истиот присвоен идентитет.

## 3 Значењето на Крадење на Идентитет

Зошто прашањето околу терминот крадење на идентитет стана толку интересно прашање, во споредба со другите видови на криминал? Секој облик на криминал има негативни финансиски и други последици за своите жртви, но оние последици поврзани со крадење на идентитет може да нанесат особено тежок удар. Идентитетот на една личност е уникатен и многу личен. Да се има информации за идентитетот на една личност, и истите да бидат отуѓени од друга личност, е повреда на приватноста од највисок ред, слично на, па дури и потешка од, кражбата на лични предмети при упад во нечиј дом.

Финансиските трошоци од крадење на идентитет може да бидат значајни. Со користење на отуѓените лични информации на една индивидуа, крадецот може да направи финансиски трансакции, да ги испразни банкарските сметки, да купува и да прави долгови. Тоа може да биде некое време пред жртвата да сфати што се случило. Загубите од измама со кредитна картичка во 2009 година во Англија изнесувала 440,3 милиони фунти [4].

Меѓутоа, ефектите од крадење на идентитет може да бидат поголеми од само обична финансиска загуба. Жртвите на традиционалните кражби обично може да ги заменат своите имоти и со тоа да ја надоместат претрпената штета, но жртвата на крадење на идентитет може да страда од губење на угледот и статусот во заедницата, како и оштетување на нејзиното кредитно реноме. По ова жртвата ќе треба да потроши многу време и финансиски средства за да ги реши настанатите проблеми, кои се последица од крадењето и незаконското користење на нејзиниот идентитет.

Владите во Канада, САД и во другите земји превзеле акција за борба против она што стана кривично дело од меѓународни димензии. Јавната свест и програмите за помош на жртвите се зголемија. Но, и покрај новите закони, политики и практики, сепак, крадењето на идентитет продолжува да ги преиспитува најдобри напори на владите, на корпоративниот сектор и на граѓаните. Овие методолошки предизвици се дополнително комплицирани од фактот дека постои големо заостанување во времето помеѓу крадењето на информации за идентификување и откривањето на настанатата штета. Многу од жртвите откриваат дека нивните информации за идентитет биле украдени само кога тие аплицираат за кредит или се обидуваат да добијат кредит на основ на хипотека, според информациите за повлекувања од нивните банкарски сметки, или доколку примат ненаплатени сметки за стоки и услуги кои тие самите не ги купиле. Во просек, постои една година доцнење во откривањето дека е направено крадење на идентитет. Ова значи дека појавите за кражба најчесто не можат да се пријават веднаш по извршениот настан. По ова е потешко да се намалат загубите и да се фатат и осудат криминалците.

## 4 ВИДОВИ НА НАПАДИ

Нападите со крадење на идентитет во последните години стануваат се поголем проблем. Имајќи го тоа во предвид, а со цел превземање на навремени и соодветни контрамерки, треба да се знаат методите и техниките кои ги користат напаѓачите за реализрање на успешен напад. За жал, тие на располагање имаат бројни методи – од старомодните, како што се крадење на вашиот паричник и диверзија на сандачето на жртвата, па се до високо-технолошки методи, како што се повреди на податоците и измамите преку електронска пошта.

Крадењето на идентитет може да биде поделено на три различни фази [5] :

1) Задржување на податоците, на пример, преку физичко крадење, преку интернет пребарувачи, надворешни напади (нелегален пристап до компјутерскиот систем, тројанци, злонамерни софтвери), преку phishing или други техники;
2) Продажба на личните податоци, каде што основна цел на крадецот на податоците е остварување на профит;
3) Користење на лични податоци со цел да се изврши криминал, односно да се искористат личните податоци за да се украдат парични средства на жртвата.

Според истражување спроведено од страна на Identity Theft Resource Centre (ITRC), најчеста причина на крадењето на идентитет е од финансиски аспект (66%) [6].

## 5 ФИШИНГ

Фишинг (Рибарење) преставува онлајн метод кој што го користат престапниците за да дојдат до лични информации користејќи техники како што се лажна електронска пошта, или на пример, лажни страни, кои што на прв поглед изгледаат дека се легитимни. Престапникот испраќа електронска пошта до одредени личности преставувајќи се, на пример, како легитимна банка која нуди нова услуга, при што, за да се проба новата услуга, треба да се дадат лични податоци (број на кредитна картичка, матичен број итн.). На прв поглед пораката изгледа легитимна, затоа што напаѓачот користи исти бои, слики, лого, кои се карактеристични на легитимната банка. Според *OECD Anti-Spam Toolkit of Recommended Policies and Measures* (OECD, 2006c, p. 25), фишинг се смета дека е главен метод кој им овозможува на сајбер криминалците да извршат крадење на идентитет [7].

Во светот, една од најпознатите измами преку електронска пошта е таканаречената „419 измама“ (попозната како Нигериска измама), во која престапниците бараат однапред уплата на одредена финансиска сума од нивните жртви.

Напаѓачите и нудат на жртвата можност да биде префрлена поголема сума на пари и при тоа се бара од нејзина страна да плати одредена такса за да се изврши трансакцијата. Денеска оваа измама е многу позната меѓу интернет корисниците, поради што бројот на напаѓачи кои го користат овој метод за крадење на идентитет е сè помал.

Од самата појава и заради се поголемото влијание на Интернетот, формирани се групи, меѓу кои што најпозната е Anti Phishing Working Group (APWG) [8] асоцијацијата, чија главна цел е објавување на податоци за начините за намалување на ефектите на крадењето на идентитетот, како и објавување на податоци од крадење, пронаоѓање на напаѓачи (лажни страни и лажна електронска пошта) и начини за заштита од нив.

Овие напади може да се поделат во три групи, односно *лажни напади*, со кои што жртвата, преку лажни пораки, се наведува да даде лични податоци, *злонамерни напади*, каде што напаѓачот употребува злонамерни софтвер со цел да дојде до посакуваните информации, како и *DNS базирани напади*, во кои се врши измена на доменот, при што корисникот се упатува на лажна интернет страна.[9]

### *5.1 Фишинг со залажување*

Најчести примери преку кои што напаѓачот пронаоѓа начин да превземе лични податоци од жртвата се тие каде што жртвата се известува преку лажна електронска порака дека има одредени проблеми со неговата банкарска сметка, при што му е понудено линк со пристап до одредена веб страна преку која што може да се реши проблемот, или пак понуда да се приклучи на одредена програма која што преставува решение за проблемот. Напаѓачите користат и други методи за да привлечат жртви, како што се електронски пораки во кои што нудат услуги од финансиски институции (за многу пониски цени, камати), известувања дека некој извршил нелегитимни измени на нивната сметка, нудејќи линк за да се спречи тоа, како и известување дека е направена нарачка од страна на одредена веб страна на име на жртвата и дека треба да биде откажана таа нарачка. Напаѓачите во многу случаи, за да дојдат до посакуваните информации, користат комбинација од повеќе методи на напади, сèсо цел да дојдат до посакуваните податоци. Тие лесно може да извршат копирање на HTML кодот на легитимна страна за логирање и да го пратат преку електронска порака на жртвата за да може директно да се логира, при што податоците дирекно влегуваат во рацете на напаѓачот.

### *5.2 Злонамерен софтвер*

Денеска, примарно оружје кое што се користи при крадење на идентитет од страна на крадците на идентитет се злонамерните софтвери (вируси, тројанци). Злонамерниот софтвер претставува софтверски код или програма која што може да му наштети на компјутерскиот систем, како и да извршат пренамена на самиот систем. При вршење на нелегални активности од страна на престапникот, за да се дојде до целта, може да се употребат повеќе злонамерни апликации. Нападите можат да бидат извршени преку веб страница која е легитимна, но во која престапникот има вметнато свој злонамерен софтвер, при што на овој начин поголем број на корисници можат да бидат нападнати, или пак, доколку напаѓачот се концентрира на поединци, односно на помали фокусни групи, тогаш напаѓачот преку електронска пошта одредува на кое лице ќе го изврши нападот.

Крадењето на идентитет може да се базира и на употребата на злонамерен софтвер кој што се вметнува во персоналниот компјутер на корисникот/жртвата. Злонамерниот софтвер може да биде пренесен на повеќе начини, од кои најупотребуван од страна на престапниците е преку праќање на одреден документ преку електронска пошта која треба да се отвори, превземе, или преку употреба на тројанци и црви кои што овозможуваат инсталирање на злонамерниот софтвер во корисничкиот компјутер. Исто така, може да се користат и спам пораки со линкови од страни кои што нудат примамливи содржини.

### *5.2.1 Keylogger-и*

Keylogger-ите се шпиунски програми кои го следат и бележат секој знак кој корисникот ќе го притисне на тастатурата. Нивната поделба е сведена на две групи:

- Алати во облик на софтверски пакети и
- Уреди кои се вградуваат во состав на компјутерскиот систем.

Keylogger-ите ги следат сите знаци кои се внесуваат од страна на корисникот преку татстатурата. Напаѓачот, со цел да дојде до доверливи информации, може да се послужи со следниве начини:

Употреба на видео надзор, вметнување на уред за прислушкување во тастатурата, вршење на промена на управувачките програми на тастатурата, или преку пресретнување на .dll датотеки (библиотека која се користи во оперативниот систем Windows). Уредите кои се вградуваат за да се врши прислушкување најчесто имаат многу мали димензии и се поставуваат во кабелот на тастатурата, додека пак алатките се софтверски програми кои што ги следат активностите на тастатурата и доколку забележат дека се внесуваат информации од висока корист веднаш ги меморираат и потоа ги доставуваат до посебни компјутерски системи (dropzones), наменети за собирање на тие податоци, од каде напаѓачот може лесно да ги превземе меморираните податоци 10]. Овој начин на собирање на податоци има и свои негативности, пред се поради тоа што се собира голема количина на податоци, од кои што напаѓачот треба да ги издвои корисните, т.е. треба да утврди во кој контекст се притиснати тие знаци од тастатурата. Со други зборови, напаѓачот треба да утврди дали корисникот кога ги запишувал тие знаци ја пишувал својата лозинка или пак пишувал обичен документ.

### *5.2.2 Тројански коњи (Trojan horses)*

Овие напади се едни од наједноставните и најупотребуваните од страна на напаѓачите. Напаѓачот може сам да ги создаде или пак да ги купи од друго лице. Тие најчесто се преставуваат кака програми со одредени функционалности кои што на прв поглед изгледаат примамливи и корисникот наседнува на тоа. Со самото навлегување на овие програми во компјутерскиот систем, напаѓачот лесно може да дојде до личните податоци кои што корисникот ги чува во својот компјутер или, во краен случај, да предизвика и превземање на целосна контрола над компјутерскиот систем на жртвата. Напаѓачот користи различни тројанци, во зависност од тоа како сака да ги превземе саканите податоци. Како пример за тројанец може да бидат наведени банкарските тројанци, кои се користат како за напади во банкарските системи, така и за напади во берзанските системи. Напаѓачот користи различни техники, како што е HTML инјектирање, со што се врши внесување на HTML код во оригиналната интернет страница која што корисникот ја посетува, и на тој начин врши измена на содржината. Така, напаѓачот може да дојде до информации како што се пин броеви на картички, лозинки, броеви на трансакциски сметки и останати податоци кои се високо чувствителни на кражба.

Најголемиот проблем е што моментално не постои целосна и ефикасна заштита од овие напади, така да, сите интернет корисници можат да бидат жртви на овие напади.

Банкарските тројанци најчесто се изработуваат од страна на професионални сајбер крадци кои што имаат големо искуство и компјутерско и програмерско познавање. Една од најпозните групи на напаѓачи е руската група RBN (Russian Business Network) [11]. Пример за овие напади е познатиот тројанец Haxdoor.ki кој, во 2006 година, нападнал голем број на шведски и германски банки во тие земји [12], при што биле собрани голем број на банкарски податоци. Во случај кога корисникот се логира на страната на банката тројанецот во позадина се активира и го предупредува корисникот дека неговата лозинка и корисничко име се погрешни, со што, додека корисникот ги внесува повторно своите податоци, тројанецот веќе ги превзел и ги пренел податоците до напаѓачот. Банките можат да ги спречат овие напади доколку постојано прават попис на лозинките и преку следење на неправилности на нивните интернет страници. Исто така, банките имаа превземено и други чекори за заштита, меѓу кои може да се издвои двојната автентикација. Во првата автентикација корисникот внесува текстуална лозинка, а во втората визуелна, со што на напаѓачот само му се отежнува работата при нападот. Причина за ова е тоа што, иако пристапот кон текстуалната лозинка може да се реализира, превземањето на графичката лозинка од жртвата е многу потежок процес. Поради ова, злонамерните напаѓачи при избор на жртви, најчесто избегнуваат клиенти на банки кои како метод на заштита ја користат двојната автентикација.

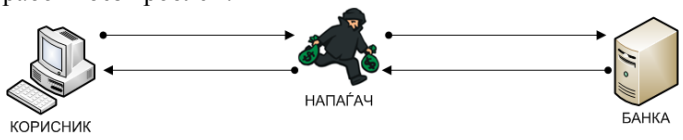
### *5.3 Pharming – употреба на DNS сервери*

Овој вид на напад и не се случуваат многу често, но сепак претставуваат закана за корисниците. Доколку корисникот сака да посети одредена интернет страница, како на пример www.mybank.com, при самото вчитување на интернет страната во позадина се врши DNS пребарување, со што се бара IP адресата која што е директно мапирана на интернет страната www.mybank.com. Напаѓачите можат да манипулираат со DNS серверите, со што корисникот смета дека ја посетува www.mybank.com, но всушност клиентот е препратен преку друг сервер на друга интернет страна во голема мера идентична на www.mybank.com. Постојат повеќе техники за реализирање на овие напади. Еден метод на реализирање на овие напади е со употреба на тројанците, со чија помош може да се изврши измена во IP адресата при пребарувањето на посакувата интернет страница, со што корисникот се води кон лажната интернет страна. Добар

пример за овие напади е пресретнувањето на „wininwt.dll“ датотеката, кога се врши пребарување преку Internet Explorer. Одредени интернет пребарувачи имаат опција да го предупредат корисникот дека интернет страната која ја посетува нема дигитален сертификат, но, доколку напаѓачот употреби тројанец, тој може да изврши измени при пребарувањето на wininet.dll датотеката и при тоа да биде заобиколено предупредувањето. Исто така, напаѓачот, користејќи тројанци, може сам да си креира свои сертификати и истите да ги инсталира, со што се избегнува појавувањето на предупредувања до корисникот.

## 6 Посредник при Крадење на Идентитет(Man in the Middle)

Посебен тип на крадење на идентитет кој се користи е кога напаѓачот делува како „посредник“ помеѓу корисникот и страната што ја посетува. Кога корисникот сака да добие информации од некоја легитимнна веб страна, тогаш „посредникот“ настапува на сцена и ги пренесува информациите од клиентот до легитимната страна и потоа од легитимната страна до корисникот. Овие напади се многу тешки за откривање од страна на корисникот, пред сè поради тоа што интернет страната ќе работи без проблем.




Слика 2 - Посредник при крадење на идентитет

Останати методи кои би требало да се напоменат се:

• Веб страни за социјално вмрежување - Со толку многу популарност околу страните за социјално вмрежување, понекогаш е лесно да се заборави дека луѓето надвор од кругот на пријатели често може да пристапат до личните информации на жртвата. Со обезбедување на детали како што се име, датум на раѓање, податоци за контакт и работодавецот, крадците лесно може да го состават мозаикот на информации кои им се потребни за да го украдат идентитетот на жртвата.

• Wardriving - Крадците, исто така, се обидуваат да ги украдат личните податоци на жртвата со помош на техника наречена wardriving, каде што крадците се возат наоколу барајќи необезбедени безжични мрежи. Ако домашната безжична конекција не е обезбедена, хакерите можат да пристапат до податоците на сите компјутери кои се поврзани со безжичната пристапна точка на жртвата, како и да ги видат информациите што се внесуваат при логирање на банкарската сметка или користењето на кредитните картички.

## 7 МЕТОДИ ЗА НАМАЛУВАЊЕ НА ЕФЕКТИТЕ ОД КРАДЕЊЕ НА ИДЕНТИТЕТ

Целосна заштита од нападите на идентитет не е можна, но сепак, има одредени техники и методи кои што можат да се употребат за да се намалат ефектите од овие напади. Најдобар начин да се започне самата заштита е да се набљудуваат злонамерните активности, како што се регистрирање на домен направено од страна на корисникот, да се забележи самиот напад уште пред да започне, како и да се попречи/прекине напаѓачот во неговата подготовка.

Безбедност преставува комбинација на технологиии, мерки и постапки кои што обезбедуваат заштита од неовластен пристап во системот.

Основни начини кои што се користат како сигурносни системи за заштита се [13]:

- ***Тајност на податоците*** - се остварува преку шифрирање, односно преку употреба на криптографски алгоритми.
- ***Автентикација*** - односно проверка на идентитетот на корисникот. Една од позначајните техники за заштита претставува автентикација на ID на испраќачот. Се врши автентикација на електронски пораки, со што се утврдува дали пораката е навистина пратена од лицето кое што тврди дека е испраќачот на истата. Оваа техника овозможува проверка на DNS серверите за да се утврди дали IP адресата од која се испраќа пораката се совпаѓа со доменот на испраќачот. Yahoo користи криптографски потписи на ниво на домени кои може да бидат потврдени од страна на DNS серверот.
- ***Интегритет на податоците*** - преставува безбедно пренесување на податоците помеѓу две или повеќе личности. Техники кои се користат за заштита се SSL - Secure Socket Layer, S-HTTP - Secure HyperText Transfer Protocol и др.
- ***Потврдување*** - потврда за да се знае кој е праќачот, а кој е примачот на пораката.

### *7.1 Шифрирање – криптографија*

Шифрирањето преставува трансформација на пораката во форма која што е нечитлива за сите останати ученици во Интернетот, освен за корисникот за која е наменета пораката, кој го има и механизмот за дешифрирање. До корисникот за кого е наменета пораката се испраќа оригиналната шифрирана порака, како и специјален клуч за да може да ја дешифрира пораката. Со помош на клучот и методите за дешифрирање пораката се трансформира во форма која што корисникот може да ја разбере. При процесот на шифрирање може да се употребат два методи [14]: *симетрично шифрирање*, каде што клучот за шифрирање и дешифрирање е ист и, *асиметрично шифрирање*, каде што има јавни клучеви, со кои се шифрираат пораките и тајните клучеви, со чија помош пораките се дешифрираат и кои клучеви ги поседува само крајниот примател на пораката.

### *7.2 Дигитални потписи*

Кога се испраќа порака може да се изврши нејзино заверување, со што, испраќачот користи приватен клуч кој не дозволува да се врши измена во пораката. Преку овој метод, со помош на hash функцијата, крајниот примател

може да утврди дали има измени во пораката. Со јавниот клуч испраќачот ја шифрира пораката, а примачот со приватниот клуч ја дешифрира и при тоа ја применува hash финкцијата и утврдува дали има измени во hash вредноста. Во случај некој да извршил измена на пораката, примачот ќе добие друга вредност која е различна од таа која што ја има добиено од испраќачот.

Дигиталните сертификати преставуваат идентификациска карта за фирмата во електронска форма . Овие сертификати најчесто се користат од банките со цел да се утврди идентитетот на клиентите.

Друга техника која што може да се искористи за подобрување на безбедноста во случај на вакви напади е со подобрување на безбедносниот систем. Нападите што се базираат на употреба на злонамерен софтвер се инсталираат во системот на жртвата преку искористување на одредени пропусти и ранливости на безбедносниот систем. Решение за овој проблем е да се пренесат криптирани симетрички клучеви за одредени сигурносни слабости на системот; откривање на лажни интернет страници и нивно пријавување до легитимни институции и организации одговорни за овие прашања; користење на заеднички протоколи за идентификација; воспоставување на безбеден пат помеѓу корисникот и интернет страната, сè со цел да се утврди дека информациите ќе бидат користени само од лицето за кое што се наменети.

Голем број на веб страници, за да се овозможи серверска автентикација, користат SSL криптографија, каде што адресата на веб страната преставува идентификатор. Проблемот тука е што корисниците најчесто не можат сами да одредат дали ја посетуваат вистинската веб страна. Решение за ова има понудено веб пребарувачот Mozilla, кој што нуди додаток [15] со кој се додава дополнително име на секоја веб страна, при што, кога корисникот повторно ќе ја посети истата страна ќе може да знае дека е на вистинското место. Доколку страната не е препозната, тогаш оваа програма (додаток) ќе го извести корисникот.

Добро решение за борба против фишинг преставува и можноста на некои веб пребарувачи да прават листа на сите лажни и злонамерни веб страни, така што, пребарувачот ќе прави споредба со таа листа. Оваа опција е поддржана од страна на повеќе веб пребарувачи, како што се, Mozilla Firefox, Opera, Microsoft's IE browser, Google Chrome.

Ефикасен начин за утврдување на легитимноста на одредена форма за логирање кај некои веб страни е со употреба на одредена слика која што корисникот ја избира при логирањето, со што при секое следно најавување на таа страна на корисникот мора да му се појави истата слика. Целта на овој метод е да се утврди автентичноста и легитимноста на страната.

Денес има компании чија што примарна дејност е мониторинг, анализирање, како и вклучување во борбата за затворање на лажните страни. PhishTank е една од многуте интернет страни која помага во намалување на ризикот од фишинг. Функционира на тој начин што секое физичко или правно лице може да пријави лажна интернет страна која влегува во базата на податоци на оваа компаниија и што ќе биде искористено за превземање на соодветни мерки за оневозможување на регистрираната веб страна успешно да реализира вакви напади.

Најуспешен метод за заштита од ваквите напади е навремено искористување на достапните безбедносни механизми, т.е., одбранбените механизми секогаш да се активираат уште пред да започне нападот. Напаѓачот, во зависност од тоа на кој начин го врши нападот, треба да изврши регистрација на домен преку кој ќе ги прима украдените податоци. При процесот на регистрирање на домен има „период на чекање“, период во кој фирмите можат да поднесат пријава за пријавување на лажен домен.

Во случајот на фишинг преку испраќање на електронски пораки може да се искористат други методи за да се спречи пораката да дојде до жртвата. Главна цел на напаѓачите кога испраќаат електронски пораки до жртвата е тие пораки да бидат што е можно поидентични на оригиналот, при што еден начин за да се спречат овие пораки е да се пронајдат неавтентични слики (изворниот код на сликата не се совпаѓа со легитимната веб страна).

Напаѓачите кога крадат информации најчесто сакаат да дојдат до корисничката лозинка, при што, за да се спречи напаѓачот во собирање на кориснички лозинки, потребно е да се врши кодирање на лозинката. Корисникот може да користи иста лозинка за повеќе интернет страни, но секоја страна да прими различна кодирана лозинка. Овој метод е познат како *password hashing*. Со овој метод се овозможува кодирање на секоја лозинка во зависност од доменот за кој е наменет и како таква, лозинката може да се користи само за доменот за кој е наменет. Оваа опција може да биде понудена како дел од интернет пребарувачот.

### *7.3 Како крадењето на идентитет влијае на жртвата*

За разлика од крадењето на часовникот или било кој друг предмет, крадењето на идентитет може да резултира со сериозни последици, за кои се потребни и време и пари за да се решат, а да не зборуваме на емоционалниот стрес и притисок кои може да ги почуствува жртвата. Подолу е даден опис за тоа како крадењето на идентитет може да влијае на животот и иднината на жртвата.

#### *7.3.1 Финансиска загуба*

Се разбира, најочигледната загуба е финансиската. Ако крадецот има пристап до заштедите, инвестициите или сметките, тогаш тој може да украде пари од сметката на жртвата.

#### *7.3.2 Губење на кредитна способност (Лош кредит)*

Бидејќи крадците на идентитет отвораат лажни сметки на платежни адреси кои се различни од тие на жртвата, тоа им овозможува полесно да направат долгови во име на жртвата без нејзино знаење. Доколку овие трошоци останат неплатени, тогаш ваквите заостанати сметки може да се појават во кредитниот извештај на жртвата. Жртвата не може да сфати дека во банката се смета како кредитно неспособна се додека не се обиде да земе кредит за

автомобил или хипотека и нејзиното барање за кредит не биде одбиено.
Кредитната штета особено е опасна кога тоа се случува со украдени идентитети на децата, бидејќи може да поминат години пред тие да се обидат да ја направат својата прва финансиска трансакција и да сфатат дека нивниот кредит е уништен.

*7.3.3 Губење на бенефиции*

Крадците на идентитет често се заинтересирани за други информации кои не се поврзани со броевите на банкарските сметки, а тоа се датумот на раѓање, адресата и бројот на пасош. Откако ќе ги добијат овие податоци, тие, преставувајќи се во име на жртвата, може да се стекнат со возачка дозвола, бенефиции, па дури и вработување .

*7.3.4 Криминално досие*

Ако крадецот украдениот идентитет го искористи за извршување на кривично дело, може да добие криминално досие. Крадецот може да добие лична карта со податоци на жртвата и кога истиот е уапсен за кривично дело, обвинението одат на досие со податоци за жртвата на крадење на идентитет. Ако крадецот не ја плати кауцијата или не се појави пред судот, тој проблем не се поврзува со него, бидејќи властите имаат налог за апсење за жртвата. Полош дел е кога жртвата и не знае дека има криминално досие, сè додека не направи некој сообраќаен прекршок или пак не биде лишен од слобода или кога ќе аплицира за работа и по проверката ќе биде одбиена.

*7.3.5 Трошоците за поправка на штетата*

Бидејќи често е потребно долго време за жртвата да разбере дека нејзиниот идентитет е искористен за разни цели од друго лице, штетата може да биде многу голема. Пред жртвата тоа да го дознае, таа може да се соочува со повеќе лажни обвинението, оштетување на кредитната репутација, како и други прашања кои бараат многу труд и трошоци за нивната поправка. Може да потроши часови во телефонски разговори, занимавајќи се со корпорации и владина бирократија и обидувајќи се да ги поправи нанесените штети на нејзиниот идентитет, па дури може и да одлучи и да ангажира услуга за поправка на нанесените штети по нејзиниот буџет и углед. Дури и тогаш, може да бидат потребни години пред навистина да е во можност да ја исчисти штетата на нејзината репутација.

*7.4 Општи совети*

Најважно од сè е тоа како корисникот ќе постапува за да се заштити од ваков вид на криминално дејствие. Препознатливи и ефективни методи кои може секој корисник да ги спроведува без некои преголеми познавања на информатичките технологии се:

• ***Свест и едукација*** - Познавањето на триковите и измамите кои крадците ги користат за да се обидат да ги добијат личните информации на жртвата, претставуваат долгорочни мерки кон спречување на крадење на идентитет. Корисниците треба да бидат внимателни при споделувањето на нивните лични податоци и да се обидат да бидат во тек со најновите измами.

• ***Здрав разум*** - Корисниците треба да ги чуваат личните податоци во приватност. Кога една личност, веб-страна, или електронска пошта прашува за личните информации, корисниците треба да се запрашаат дали тоа е стандардна пракса да се бараат таквите информации. Здравиот разум ќе каже дека банката на корисникот никогаш не би испратила електронска пошта со барање да ги потврдите бројот на вашата сметка, корисничкото име и лозинка или да побара други детали, како на пример бројот на пасош или пак бројот на возачката дозвола.

• ***Свесност за опкружувањето*** - Корисниците треба да бидат свесни за нивната околина и сите други кои можат да бидат во близина кога ќе купуваат преку телефон или преку преносен компјутер користејќи јавни безжични (мобилни) мрежи, ќе го внесат нивниот ПИН во банкоматот, ќе го внесат бројот на нивната кредитна картичка додека купуваат онлајн, или пак ќе внесат текстуални лични информации. Корисникот треба да е свесен дека никогаш не треба да ги испраќа броевите од неговата кредитна картичка или сметки преку било која електронска пошта.

• ***Заштита на интернет*** - Кога сурфаат на Интернет, корисниците треба да користат сеопфатен пакет за безбедност, кој не само што заштитува од вируси, spyware, и другите нови закани, но, исто така, обезбедува безбедна технологија на пребарување, која ќе помогне за полесно препознавање на лажните веб-страни кои се обидуваат да ги соберат нивните информации. Покрај тоа, корисниците треба да се осигураат дека нивниот firewall е вклучен, за да го блокира неовластениот пристап до нивниот компјутер или мрежа.

• ***Користење на силни лозинки*** - Лозинките треба да бидат најмалку 10 карактери долги и треба да се состојат од комбинација на букви, бројки и специјални знаци. Исто така, се смета дека периодичната промена на лозинки ја намалува веројатноста крадците да ги украдат личните информации на корисниците и истите да ги злоупотребат во своите криминални планови. Корисниците треба да избегнуваат користење на исти лозинки или споделување на истите со било кого, па дури и со пријателите и семејството.

• ***Практично безбедно сурфање на јавни места*** - Ако корисниците користат јавен компјутер или пристап до Интернет од јавно место или необезбедена безжична конекција, треба да избегнуваат да се вклучуваат на нивните банкарски сметки или да користат кредитни картички за онлајн купување. Побезбеден начин за вакво користење на Интерентот е преку приватните домашни компјутери кои се поврзани на домашна безбедна мрежа.

• ***Обезбедување на домашната безжична мрежа*** - За да се спречат напаѓачите кои ја користат wardriving техниката за остварување на личен профит или нанесување на штета на легалните корисници, потребно е да се вклучи firewall-от на безжичната пристапна точка (безжичен рутер) и да се промени администраторската лозинка. Повеќето рутери доаѓаат со стандардно корисничко име и лозинка, овозможувајќи им на корисниците самостојно да го постават и да го

конфигурираат рутерот, но хакерите често се запознаени со ваквите стандарди. Исто така, пожелно е да се промени стандардниот идентификатор на пристапната точка кој се користи за да го објави присуството на уреди во непосредна околина и да дозволи пристап само од компјутери или уреди кои ќе ги одреди легалниот корисник на таа пристапна точка. Корисниците треба добро да го проучат упатството на нивните безжични пристапни точки за да дознаат како да ги променат овие стандардните поставувања.

## 8 ЗАКЛУЧОК

Денес, се повеќе организации и индивидуи објавуваат информации за себе на Интернет, со што преставуваат лесна мета за напаѓачите на идентитет, кои што користат различни методи за да можат да дојдат до лични информации. Иако од една страна се наоѓаат напаѓачите кои што постојано изнаоѓаат нови начини за да нападнат, од друга страна пак, организациите се обидуваат на најдобар начин да се одбранат од овие напади.

Како што напаѓачите прават комбинации на повеќе техники на напади, така од другата страна се применуваат комбинирани методи за заштита. Голема улога во спречување на кражбата на идентитетот игра и самата едукација и тоа колку се граѓаните информирани за методите за заштита од овие кражби.

Корисниците, пред сè, треба да бидат внимателни кога пребаруваат информации преку Интернет и на кого и каде ги оставаат своите лични податоци. Почеток за заштита на личните податоци може да преставува добра антивирусна апликација, како и добра malware апликација кои би работеле во позадина на системот. Денес постојат голем број на додатоци на интернет пребарувачи
кои што можат да помогнат околу заштитата на информациите, кои се многу корисни, а лесни за користење.

## БИБЛИОГРАФИЈА


[1] Wendy Parkes, Thomas Legault, "Identity Theft: Introduction and Background", CIPPIC Working Paper No.1 (ID Theft Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

[2] Lombardi, Rosie, “Myths about identity theft debunked by experts”, IT World Canada, 22 March 2006

[3] Susan Sproule and Norm Archer, “Defining and Measuring Identity Theft”, presentation to the second Ontario Research Network in Electronic Commerce (ORNEC) Identity Theft Workshop, (Ottawa, 13 October 2006)

[4] IDTheft_eguide_UK.pdf, “What You Need to Know to Avoid Identity Theft”, Copyright © 2010 McAfee, Inc.

[5] Demosthenes Chryssikos, Nikos Passas, Christopher D. Ram, „„The evolving challenge of identity-related crime:addressing fraud and the criminal misuse and falsification of identity“International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme ‚Selected papers and contributions from the International Conference on“The evolving challenge of identity-related crime:addressing fraud and the criminal misuse and falsificationof identity”Courmayeur Mont Blanc, Italy30 November − 2 December 2007

[6] US victimisation survey conducted by the Identity Theft Resource Centre (ITRC, 2005, p. 6) 2004.

[7] OECD Anti-Spam Toolkit of Recommended Policies and Measures (OECD, 2006c, p. 25)

[8] Извор: http://www.antiphishing.org/ Anti-Phishing Working Group е глобална пан-индустриска и правна асоцијација фокусирана на елиминирање на кражба на идентитет како резултат на phishing, pharming и лажни е-пошти од сите типови.

[9] Aaron Emigh ‚Radix Labs„„ Online Identity Theft:Phishing Technology, Chokepoints and Countermeasures“October 3, 2005

[10] Holtz, T., Elgenberth, M., Freiling, F., “Learning More About the UndergroundEconomy: A Case-Study of Keyloggers and Dropzones”, Computer Security - ESORICS 2009, Springer Berlin / Heidelberg, pp. 1-18.

[11] "Russian Business Network (RBN): RBN - Georgia CyberWarfare." Russian Business Network (RBN). 5 Nov. 2008 http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html

[12] Swedish bank hit by ‘biggest ever’ online heist (2007) ZdNet, httpp://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm

[13] Turner, P., Wunnicke, D. “Managing the Risk of Payment Systems”, John Wiley & Sons Inc, (2003)

[14] Vuksanović, E. “Elektronsko bankarstvo”,Beogradska bankarska akademija, Beograd, (2006)

[15] Извор.https://addons.mozilla.org/enus/firefox/addon/petname-tool/


- - - - - - - - - - - - - - - - - - - - - - -

Summary

# Identity theft and methods to mitigate the effects of this attack

Jasmina Smiljanoska, Monica Jankoska, Mitko Bogdanoski

European University - Skopje, R. Macedonia
smiljanoska.jasmina@live.eurm.edu.mk, jankoska.monika1@live.eurm.edu.mk, mitko.bogdanoski@eurm.edu.mk

***Abstract* – Identity theft is fraud used by an attacker to gain personal information of another person, such as identification numbers, credit card numbers, social numbers, etc., and thereby gain access to resources or benefits on behalf of that person. The main motive of the identity theft attack is the profit. The informations which are illegally obtained using this type of attack are directrly used by the attacker or reselled to third person. Nowadays, for successful implementation of such attacks, different tools and methods are used as a fake emails (spams), fake websites, trojans,worms etc. The subject of this paper is to discuss the identity theft attacks and the way they operate, as well to describe and analyze the methods used to prevent or mitigate the effects of this type of attacks.**

***Keywords* – identity theft, attacker, phishing, pharming**