

Банкомати – АТМ (*Authomated Teller Machines*)

Развиените информациски мрежи овозможува употреба на информациската технологија во шалтерското работење преку банкоматите (АТМ) и POS терминалите со цел зголемување на квалитетот на услугите на банките и ориентација кон клиентите. АТМ се машини што се дислоцирани на поголем број места и поврзани со банкарската мрежа и овозможуваат клиентите сами да извршат низа функции што обично ги врши шалтерскиот работник со користење на платежна картичка како средство за идентификација.

Воведувањето на банкоматите е првиот чекор кон воведување електронско банкарство. Првите банкомати (*Cash Dispensing Machine*) овозможувале само автоматизација на подигнувањето на пари во фиксиран износ. Првиот банкомат се појавил во 1967 год. во филијалата на британската банка “*Barklays*” во форма на банкомат што овозможувал само исплата на готовина. Во тоа време банкарите очекувале дека нивните клиенти ќе го користат банкоматот само во случај кога банката е затворена.

Со воведувањето на новите типови услуги се создаваат комплетни самопослужни шалтери (АТМ - *Authomated Teller Machines*) што овозможуваат користење комплетни шалтерски услуги: депонирање и подигање пари, издавање чекови, начување и примање извештаи, трансфер на средства од една сметка на друга, плаќање сметки за одредени услуги (струја, вода и сл.) итн. Со помош на банкоматите клиентите моѓат да реализираат рутински трансакции надвор од просториите и локациите на банката, по принципот на самопослужување и независно од работното време на банката. Токму со ваквите карактеристики тие овозможуваат:

1. Продолжување на времето на достава на услугите што ги нуди банката бидејќи клиентите можат да ги користат во секое време од денот и
2. Сnižување на трошоците, елиминирање на потребите од отворање нови класични филијали и ангажирање дополнителни шалтерски работници

Значи, воведувањето на банкоматите на клиентите им овозможи пристап до нивните сметки 24 часа, брза услуга без чекање во редици пред шалтерите и многу поширок спектар на услуги. Од друга страна, воведувањето банкомати за банките значи

повеќекратно намалување на трошоците за процесирање на трансакцијата, намалување на гужвите во банките и задоволни клиенти. Исто така, тоа води кон рационализација на бројот на вработени и можност за остварување дополнителни приходи од надокнада за услугата од користење на картички издадени од други банки.

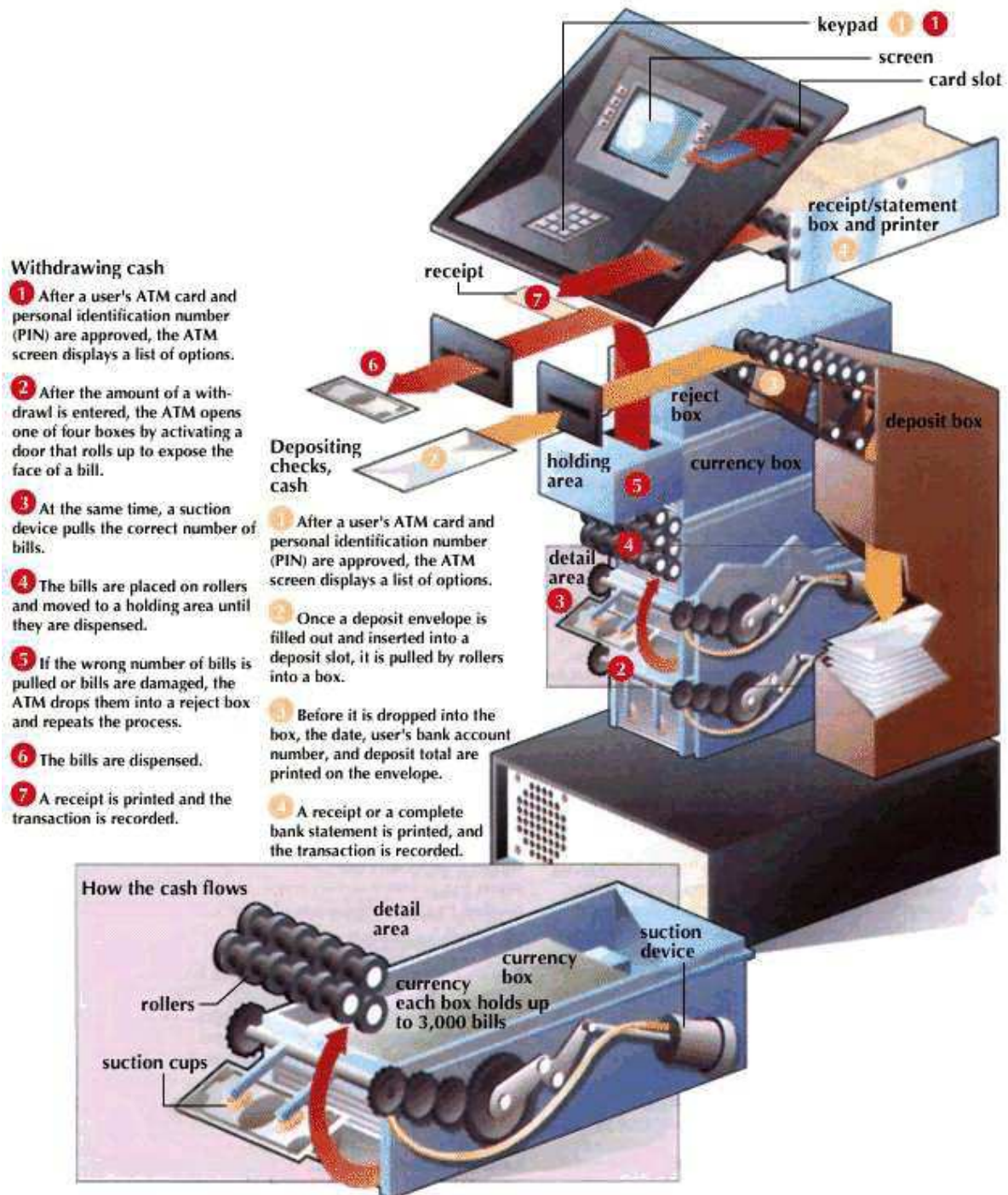
Основни технички компоненти на банкоматот се (види слика):

- Конзола за корисникот
- Дел за чување готовина
- Дел за прием на депонираните средства
- Централен контролер
- Механизам за печатење
- Софтверска поддршка

Дел од овој систем се смета и идентификациската картичка на корисникот бидејќи системот без неа не може да функционира. Преку корисничката конзола се воспоставува врска со корисникот и се даваат упатства со кои тој се води преку процесот на самопослужување. Кога корисникот на системот ќе ја уфрли својата картичка и ќе го впиши PIN бројот, од неа се читаат сите релевантни податоци како: бројот на сметката, датумот на истекување на картичката, дозволеният број на дневни користења (или дозволената сума за тој ден) и сл.

Како што е прикажано на сликата, типичната трансакција преку банкоматот се одвива во фази односно чекор по чекор. Значи, откако клиентот ќе ја уфрли картичката во читачот, банкоматот бара да се внесе PIN бројот (најчесто во рок од 30 секунди од внесувањето на картичката) на нумеричката тастатура. Доколку бројот е неточен, дозволено е истиот да се внесе најмногу три пати. Доколку и по третиот пат клиентот внесе неточен PIN, банкоматот ја задржува картичката, за чие подигнување клиентот е должен да се обрати во некоја од филијалите во чијашто сопственост е банкоматот. Доколку, пак, идентификацијата е успешна, клиентот се логира во системот и комуницира преку дисплејот за услугата што сака да ја користи.

How An Automated Teller Machine (ATM) Works



The components of an automated teller machine (ATM).

Credit: Sources: Citibank, NCR Corp., American Bankers Association. Illustration: Courtesy Chicago Tribune

Веќе беше посочено дека продолженото работно време и намалувањето на трошоците преставуваат основа на целокупната филозофија на воведување на банкоматите. Праксата покажала дека банкоматите многу повеќе се користат за подигање готовина отколку за депонирање средства. Имено, депонирањето средства клиентите најчесто го реализираат на банкарските шалтери. Но, исто така особено постарата популација се уште повеќе преферира директен контакт со шалтерските работници отколку со машина.

Во почетокот на работењето со АТМ, поседувањето мрежа на банкомати било прашање на престиж меѓу банките па некои банки постојано ја разгранувале сопствената мрежа на банкомати и нуделе услуги само на сопствените клиенти. Покасно банките ја увиделе нецелисходноста на самостојното развивање банкомати, па отпочнале процес на нивна интеграција, при што две или повеќе банки се договараат за меѓусебно користење на своите мрежи банкомати.

Посебно ограничувачки фактор при користењето АТМ е несигурноста. Во САД е познат случајот на две банки коишто во 2001 и 2002 год. доживеале такво крадење на готовина што едната од нив банкротирала. Тие имале договор со сопственикот на банкоматите да управува со целиот ланец банкомати и да обезбедува транспорт на готовина во блиндирано возило. Но, се случило сопственикот на банкоматите да прикрива дел од готовината заради покривање на сопствените трошоци и да биде откриен дури по една година откако банката претрпела големи губитоци по тој основ.

Најчеста злоупотреба на картичките преку банкоматите е т.н.скиминг (eng. skimming). Со скиминг се означува чинот на користење скимер (eng. skimmer) за нелегално прибирање податоци од магнетната лента на кредитните или дебитните картички. Под скимер се подразбира електронски уред што се поставува на банкоматите со цел да се украдат информациите од картичката и истите да се копираат на картички со празна магнетна лента. Скимингот функционира на тој начин што се заменува читачот на картичката со камуфлиран, фалсификуван читач на картички т.е. скимер. Скимерот ги запишува сите податоци на картичката кои потоа можат да се употребат за нелегални цели. Покрај на

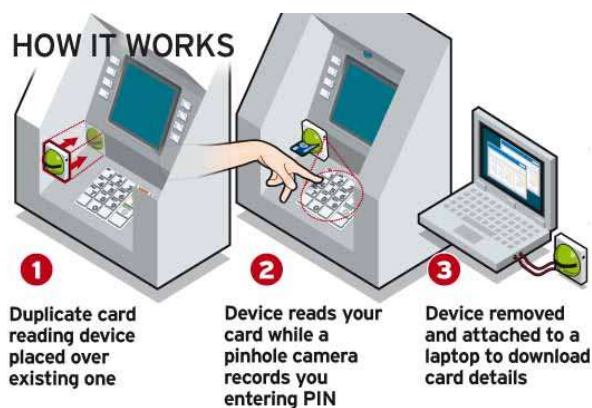
АТМ скимингот често се користи и во ресторани, такси или други бизниси каде што може да се употреби платежна картичка.



Скимер - тастатури инсталирана на банкомат



Скимер – читачи на картички за банкомат



Начин на функционирање на скиминг процесот

НАПИСИ ВО МЕДИУМИТЕ ЗА ЗЛОУПОТРЕБА НА БАНКОМАТИТЕ И ПЛАТЕЖНИТЕ КАРТИЧКИ

На Македонец му одзеле 14 читачи на картички. Картичките ги користел во Танзанија

6.8.2012. 14:00Poslovni dnevnik (<http://www.poslovni.hr>)

Државјанин на Република Македонија уапсен е на поширокото сплитско подрачје бидејќи во јули минатата година на банкомат на ОТП банка во Задар во Макарска поставил уред за снимање магнетни записи од платежни картички т.н. скимер (eng. skimmer), и камера со коишто прибирал податоци за броевите на сметките од поголем број платежни картички како и PIN – овите на клиентите.

Дури 14 скимери се пронајдени во сопственото возило што го возел Македонецот, што е најголема заплена на такви уреди досега во Хрватска. Пронајдени се и четири прилагодени делови на банкомати за излез на пари со вградени микрокамери, маски за банкомати со отвори за микрокамери, поголем број електрични кола што служат за изработка на скимери и друга пропратна опрема.

Податоците што ги добил од макарскиот банкомат, минатото лето ги користел за подигање пари и тоа во Танзанија, користејќи фалсификувани платежни картички. Токму големиот број трансакции во толку далечна држава им бил сомнителен на банкарите. Засега е утврдено дека штетата што ја претрпела ОТП банка Задар изнесува 14 629 куни (околу 2000 евра). Симнати се пари од две картички во сопственост на двајца хрватски државјани. Меѓутоа, со оглед на количината пронајдена и одземена опрема, полицијата се сомнева дека отуѓениот износ би можел да биде далеку поголем што ќе се утврди по добивањето на информациите од повеќе странски банки и клиенти за кои се верува дека се оштетени.

За 4 часа снимиле 100 пина

Дневен весник Вечер - 12.07.2010www.vecер.com.mk

Полицијата привела двајца скопјани, во момент кога од банкомат го подигале скимерот што за 4 часа од тастатурите на банкомат на домашна банка снимил 100 пин-кодови

За четири часа двајцата скопјани со помош на специјален апарат, скимер, успеале да приберат податоци од околу 100 платежни картички од банкомат на домашна банка. Но пред да ги употребат собраните податоци, полицијата успеала да ги приведе. Единицата за борба против компјутерски криминал при Одделот за организиран криминал ги сомничи за сторени кривични дела правење, набавување или отуѓување средства за фалсификување, изработка и употреба на лажна платежна картичка и соизвршителство.

Двајцата пријавени, како што е наведено во соопштението, на почетокот на месецов набавиле опрема за прибавување банкарски податоци за изработување лажни платежни картички, скимери, како и уред за снимање на видеозаписи од пин-кодовите од платежните картички. Потоа го монтирале скимерот на банкомат на домашна банка во Скопје со цел да ги преснимаат податоците од вистински платежни картички и податоци на сопствениците.

Полицијата утврдила дека скопјаните работеле по претходен договор, па за да приберат податоци на 8 јули во два наврати го монтирале уредот на банкомат во Скопје, а околу 17:30 часот истиот ден при обидот да го подигнат, биле приведени.

Со судски наредби полицијата извршила претреси кај пријавените, во возилото што го користеле и во домовите во кои живеат. Во автомобилот бил најден уредот за прибавување банкарски податоци и уредот за снимање на видеозапис од пин-кодовите од платежни

картички, мемориски дел со приклучок, преносен компјутер и усб-кабел со наменски направен приклучок што служи за поврзување на уредот со компјутер. Во домот на едниот пронајдена е фалсификувана платежна картичка. Тоа била оригинална картичка издадена од домашна банка и гласела на име на македонски државјанин, а на магнетната лента биле вметнати податоци од картичка во сопственост на странски државјанин.

Од извршеното исчитување на мемориските картички од пронајдените уреди за снимање видеозаписи од пин-кодовите и банкарски податоци од платежни картички утврдено е дека во временски период од околу четири часа додека бил монтиран уредот на него биле снимени околу 100 записи од внесени пин-кодови на тастатурата на банкоматите каде што биле поставени. Од Одделот на компјутерски криминал во првото полугодие од годинава регистрирани се 26 кривични дела извршени од вкупно 36 сторители.

Со фалсификувани платежни картички со податоци на странски државјани се извршени 17 дела, а 9 дела се извршени со кредитни картички со податоци на македонски државјани, при што сторителите се стекнале со вкупна противправна имотна корист од околу 18,7 милиони денари.

ДОМАШНИ КРИМИНАЛЦИ СО МЕЃУНАРОДНИ ВРСКИ. ФАЛСИФИКУВАНИ КРЕДИТНИ КАРТИЧКИ ОД МАКЕДОНИЈА СЕ ПРАЗНЕЛЕ ВО ПЕРУ. НЕ ВАДЕТЕ ПАРИ АКО ЗАБЕЛЕЖИТЕ СКИМЕР

Дневен весник Дневник, 04.07.2013, www.dnevnik.com.mk

Најчесто податоците од кредитните картички се крадат кога корисниците ги користите при вадење пари од банкомат. На нив криминалците поставуваат таканаречени скимери, апарати за копирање информации од кредитни картички. Ваквите уреди постојано се усовршуваат и се потешко може да се забележат дека се прикачени на АТМ-машините бидејќи често изгледаат како да се дел од вистинскиот уред. Кога ќе ја ставите картичката во банкоматот, апаратот ги копира основните податоци, кои потоа се искористуваат за изработка на фалсификат платежни картички со кои се повлекува кеш. Најчесто се

употребува заедно со камера, која го снима заштитниот PIN-код на платежната картичка кога некој ќе извади пари од банкомат. Податоците од скимерот и од камерата се читаат преку компјутер. Од Europol предупредуваат секој корисник на банкомат да внимава максимално. Некои од советите што ги предлагаат е да се засолните и да не дозволувате да бидете забележани од оние што стојат во ваша близина и додека го внесувате PIN-бројот да се заштитите со раката. Се предлага и симулирање дека притискате и на други копчиња за да не може евентуално камерата да открие кој број точно го внесувате. Потребно е добро да се забележи дали уредот од кој вадите пари е сомнителен, односно дали на него има некој дел што не сте го забележале претходно ако вадите пари на ист банкомат. Ако случајно ви заглави картичката, веднаш треба да ја известите банката.

РАСТЕ КРИМИНАЛОТ СО ПЛАСТИЧНИТЕ ПАРИ

Дневен весник ВЕСТ 14.01.2011, www.vest.com.mk

Сумата на проневерени пари со овие кривични дела се пресметува во милиони, и тоа за само деветте месеци од минатата година

Со лажна кредитна картичка извадил пари од банкомат, со пробиен пин празнел туѓи сметки, изработувале лажни платежни картички...Полициските билтени лани беа преполни со извештаи за вакви кривични дела кои се класифицираа во делото изработка и употреба на лажна платежна картичка.

Во 2010 година во Македонија се откриени над 34 дела оштетување и неовластено навлегување во компјутерски систем, девет дела изработка и употреба на лажна платежна картичка, четири дела изработување, набавување или отуѓување средства за фалсификување, и по едно дело компјутерски фалсификат и издавање чек без покритие и злоупотреба на службена картичка. Сумата на проневерени пари со овие кривични дела се пресметува во милиони денари, а статистиката покажува дека компјутерскиот криминал, кој е најдиректно врзан со изработката и употребата на лажна платежна картичка, е во пораст во Македонија. Според МВР, сторители на овие дела се и поединци и групи, но се

работи и за организирани меѓународни криминални мрежи. Во сите категории сторители поврзани со овој тип криминал, полицијата за девет месеци во 2010 година евидентирала и поднела пријави за над 70 осомничени.

Според експертите за платежни картички, најкарактеристична е појавата на фалсификување на популарните пластични пари и празнењето сметки со фалсификатите, а особено начините на изработка на лажните картички. Најчестите начини на злоупотреба и фалсификување се скиминг, потоа крадење податоци на Интернет или при плаќање други трошоци каде картичката не мора физички да е присутна, велат од "Дајнерс клуб Македонија".

Еден од најраспространетите начини за добивање податоци за кредитни картички, а што подоцна се злоупотребува за фалсификување, е скиммингот. Се работи за снимање на магнетниот запис на картичката со помош на мали магнетни читачи. Со добиените податоци, се прават фалсификат картички. Ова најчесто го прават продавачи или вработени во ресторани, кафулиња, во хотели..

Еден од омилените начини за фалсификување на пластичните пари е и изработувањето на дупликат врз основа на виден слип или картичка. Фалсификаторот, според белешката што се добива при користење на картичката или според податоците од самата картичка, прави идентичен фалсификат. Сопственикот најчесто до добивање на првиот извештај не е ни свесен дека е измамен. Помодерните фалсификатори користат видеотехника за да изработат лажна картичка и со неа да извлекуваат пари од банкомат. Тоа е т.н. видеокрадење на записот и пин бројот при внесување на банкомат. Се поставуваат мали камери на самиот влез од банкоматот, и така се снимаат основните податоци кои подоцна се користат за вадење пари од таа сметка со лажна картичка. Во подем е Интернет кражбата на пари од кредитни картички. Тоа се случува при плаќање на Интернет. Компјутерции прават програми кои можат да го видат бројот на картичката и информациите за сопственикот, и подоцна со тие податоци купуваат на Интернет од името на вистинскиот корисник. Експертите велат дека дури и обичните продавачи прават обичен криминал со картичките, но, сепак, и тоа е криминал. Се случува при наплата да

внесат поголема сума, а сопственикот да ја потврди со пинот без да види, а белешката да ја фрлат веднаш, па што направиле да откријат дури следниот месец кога ќе им дојде извештајот.

Хакери на процент

Во овој криминал се вклучени и хакери. Според оперативните одделенија на МВР, хакерите работат на процент, пробивајќи податоци на корисници на картички преку Интернет.

"Често се случува да се појават погрешни картички со погрешни пинови, па таквите измамници најчесто паѓаат во мрежата на полицијата. Откако повеќепати ќе се обидат на банкоматите да извадат пари со погрешен пин кој не соодветствува на картичката, полицијата брзо им влегува во трага", објаснуваат инспекторите и оперативците.

Купувајте од проверени Интернет сајтови

"Треба да се внимава на сомнителни апаратчиња кај продавачите, и уплатата секогаш да се врши пред вашите очи. Сливовите да се чуваат и да се поништуваат лично. Пинот да се чува, да се внимава кога се вадат пари од банкомат и дали на банкоматот има некои невообичаени камери или апаратчиња. Многу важно е да се користат сесиге сервер сајтови на Интернет, да се купува кај проверени продавачи и податоците за картичката не треба да се испраќаат по e-mail", предупредуваат од "Дајнерс Македонија".

Нови финти

Според полициската истрага на еден од тие случаи, осомничените податоците од кредитните картички на неколку странски државјани не ги вметнувале на бланко пластика, што е вообичаен метод, туку броевите на сметките и пин кодовите ги снимале на нивните оригинални картички. Во истрагата приведените детаљно го опишале начинот на кој цели три месеци оперирале со лажна пластика.

Издавачите гарантираат заштита

"Комерцијална банка АД Скопје има оперативно опкружување кое го поддржува и штити целиот систем за работење со картички на сите три нивоа на безбедност - хардверски, софтверски и физички. Овој систем опфаќа сигурна комуникација и следење за цело времетраење на трансакциите, податоците и персонализирање на картичките, но и соодветни модули за делотворно и навремено следење на невообичаени активности со платежните картички. Покрај официјалните процедури на меѓународните компании за работење со картички, Банката има воспоставено интерни процедури и мерки, првенствено за заштита на клиентите од можни злоупотреби или фалсификати на платежните картички", изјавуваат од Комерцијална банка АД Скопје. Од "Дајнерс Македонија" велат дека во несакани случаи застануваат во финансиска заштита на нивниот член, поднесуваат кривична пријава и одржуваат тесна соработка со МВР кое, според "Дајнерс", сега има одлична екипа за борба со ваквиот криминал. "Дајнерс има многу методи за заштита. Од заштитни физички елементи на самата картичка, преку проверка на апликантите, до real-time мониторинг систем, најава на Интернет трошоци и други видови ризично трошење, проверка на трошоци и нивна потврда, ако не се најавени. Нашиот 24-часовен мониторинг центар, со правилно сетирање на алерти ни овозможува превенција и рана детекција", велат од "Дајнерс".