Quarterly Journal of Hamedan Police Science

Journal homepage: http://hamedan.jrl.police.ir/

19 Vol.7, No.27, Winter 2021

Presenting a Solution to Deal with Economic Skimming Crimes; Emphasizing on E-Banking (Case Study: Hamedan Police)

Mehdi Rezaei
∗Master Student of Economic, Tarbiat Modares University, Tehran, Iran.
Mehdi_rezaei@modares.ac.ir
(Corresponding Author)

Mahdi Abbasi
Associate Professor of Computer Engineering, Bu-Ali Sina University, Hamadan, Iran.
abbasi@basu.ac.ir

Received: 2021/02/13
Accepted: 2021/03/17

DOI:
10.22034/HPSJ.2021.95884

ABSTRACT

Today, with the growth of technology and expansion of electronic banking equipment and services, the use of banking services has become very simple. The existence of this space has created an opportunity for financial crimes despite some social advantages. In the present study, we are going to present novel and efficient strategies in order to prevent skimming attacks by collecting information from the Fata Police of Hamadan Province as well as collecting various methods available and the methods used in this type of attacks and considering the existing infrastructure in the banking system, existing information and communication technology, and the prevailing sanctions that have made access to some technologies difficult. In this research, according to the studies, a practical and applicable design in the form of codes in Java space was presented as an applicable software for mobile phones in order to use NFC technology which can play an important role significantly in controlling and reducing skimming crimes, reducing the cost of issuing bank cards by banks, and reducing all kinds of risks and attacks by thieves.

Keywords: Skimming crimes, Economic crimes, Electronic banking, Banking information theft, Cyberspace.

►**Citation (Vancouver):** Rezaei M, Abbasi M. Ayatollah F. Presenting a Solution to Deal with Economic Skimming Crimes; Emphasizing on E-Banking (Case Study: Hamedan Police .Quarterly J Hamedan Police Sci. Winter 2021; 7(4): 19-30.

►**Citation (APA):** Rezaei, M., Abbasi, M., Ayatollah, F. (Winter 2021). Presenting a Solution to Deal with Economic Skimming Crimes; Emphasizing on E-Banking (Case Study: Hamedan Police) . *Quarterly Journal of Hamedan Police Science*, *7*(4), 19-30.

ارائه راهکاری برای مقابله با جرایم اسکیمینگ اقتصادی، با تأکید بر بانک‌داری الکترونیک (مورد مطالعه: پلیس همدان)

مهدی رضایی
* دانشجوی کارشناسی‌ارشد اقتصاد، دانشگاه تربیت مدرس، تهران، ایران.
(نویسنده مسؤول)
Mehdi_rezaei@modares.ac.ir

مهدی عباسی
دانشیار مهندسی کامپیوتر، دانشگاه بوعلی سینا، همدان، ایران.
abbasi@basu.ac.ir

نوع مقاله: پژوهشی
صص: ۱۹-۳۰
تاریخ دریافت: ۱۳۹۹/۱۱/۲۵
تاریخ پذیرش: ۱۳۹۹/۱۲/۲۷
شناسه دیجیتال (DOI):
10.22034/HPSJ.2021.95884

چکیده

امروزه، با رشد تکنولوژی و گسترش تجهیزات و خدمات بانکداری الکترونیک، استفاده از خدمات بانکی بسیار ساده شده‌است. وجود این فضا، با وجود برخی مزیت‌های اجتماعی، فرصتی برای جرایم مالی ایجاد کرده‌است. در پژوهش حاضر، با جمع‌آوری اطلاعات از پلیس فتای استان همدان، گردآوری انواع روش‌های موجود و انجام‌شده در این نوع حملات و باتوجه به زیرساخت‌های موجود در نظام بانکی، تکنولوژی‌های فناوری اطلاعات و ارتباطات موجود و شرایط تحریمی حاکم که دسترسی به برخی تکنولوژی‌ها را با مشکلاتی مواجه ساخته، درصدد ارائه راهکارهایی کارآمد و نو در جهت پیشگیری از حملات اسکیمینگ هستیم. در این پژوهش، باتوجه به مطالعات صورت‌گرفته، طرحی کاربردی و قابل اجرا در قالب رمزهایی در فضای جاوا به صورت نرم‌افزاری کاربردی برای تلفن‌های همراه به منظور استفاده از تکنولوژی NFC ارائه گردید که می‌تواند درجهت کنترل و کاهش جرایم اسکیمینگ و کاهش هزینه‌های ارائه کارت‌های بانکی توسط بانک‌ها و کاهش انواع خطرات و حملات سارقان به میزان قابل توجهی نقش داشته باشد.

کلیدواژه‌ها: جرایم اسکیمینگ، جرایم اقتصادی، بانکداری الکترونیک، سرقت اطلاعات بانکی، فضای مجازی

استناد (ونکوور): رضایی م، عباسی م. ارائه راهکاری برای مقابله با جرایم اسکیمینگ اقتصادی، با تأکید بر بانک‌داری الکترونیک (مورد مطالعه: پلیس همدان). فصلنامه علمی دانش انتظامی همدان. زمستان ۱۳۹۹؛ ۷(۴): ۱۹-۳۰.

استناد (APA): رضایی، م.، عباسی، م. (زمستان ۱۳۹۹). ارائه راهکاری برای مقابله با جرایم اسکیمینگ اقتصادی، با تأکید بر بانک‌داری الکترونیک (مورد مطالعه: پلیس همدان). *فصلنامه علمی دانش انتظامی همدان*، ۷(۴)، ۱۹-۳۰.

مقدمه

دو روش سرقت و نسخه‌برداری اطلاعات درج‌شده در نوار مغناطیسی پشت کارت‌های بانکی و رمز اول مرتبط به آن کارت‌ها (اسکیمینگ) و طراحی سایت و درگاه‌های جعلی در شبکه‌های اجتماعی(فیشینگ) ازجمله شیوه‌های پیش پاافتاده‌ی سارقان فضای مجازی برای سوءاستفاده از اطلاعات کارت‌های بانکی است (Oleksandr Ilchenko ,2019).

در روش "اسکیمینگ"، سارقان با دستگاه اسکیمر از اطلاعات نوار مغناطیسی کارت بانکی افراد نسخه‌برداری می‌کنند و با چاپ فیزیکی کارت و داشتن رمز کارت مبادرت به خالی‌کردن حساب کارت بانکی می‌کنند (Amy Hebert, 2014). اسکیمرها خوانندگان غیرقانونی کارت‌ها هستند که به پایانه‌های پرداخت متصل می‌باشند. این دستگاه‌های خوانندهٔ غیرقانونی کارت‌ها، بدون اطلاع فرد صاحب کارت و حساب متصل به کارت، اطلاعات را از نوار مغناطیسی دریافت می‌کنند. سارقان داده‌های مسروقه را می‌فروشند یا از آن برای خریدهای آنلاین استفاده می‌کنند (Colleen Tressler , 2018).

در این روش، کلاه‌برداران از دوربین‌ها، روکش‌های صفحه‌کلید و دستگاه‌های اسکیمر استفاده می‌کنند- دستگاهی که مانند یک کارت‌خوان واقعی روی دستگاه کارت‌خوان و دستگاه خودپرداز قرار می‌گیرد و بدون اطلاع قربانی نوار مغناطیسی کارت را نسخه‌برداری کرده و با در اختیارداشتن رمز کارت و نسخه‌برداری فیزیکی کارت بانکی به منابع مالی کارت دسترسی پیدا می‌کنند (Amy Hebert, 2014).

در این پژوهش، به بررسی مسأله و معضل جرایم اسکیمینگ در استان همدان پرداخته خواهد شد و با بررسی پرونده‌های موارد مشاهده و گزارش شده و با توجه به نحوهٔ انجام این جرم در استان، به ارائه‌ی راهکاری مبتنی بر استفاده از تلفن‌های همراه با استفاده از تکنولوژی NFC جهت کاهش این جرایم خواهیم پرداخت.

کاظمی و همکاران (۱۳۸۹) در پژوهشی باعنوان "بررسی عوامل کلیدی مؤثر بر موفقیت عرضه خدمات اینترنتی و ارائه‌ی یک الگو پیش‌بینی‌کننده با استفاده از درخت تصمیم‌گیری" به شناسایی مهم‌ترین ویژگی‌های تأثیرگذار بر تشویق و ترغیب افراد در استفاده از بانکداری اینترنتی پرداخته و یک الگو پیش‌بینی‌کننده برای موفقیت بانک‌ها در این عرصه ارائه کردند. پژوهش آن‌ها بیانگر این بود که متغیرهای رابطهٔ عضویت، سفارش‌پذیری، درجهٔ ضروری بودن، قیمت، اهمیت نیروی انسانی، دانش حرفه‌ای و درجهٔ تعامل، به ترتیب دارای همبستگی معنادار با متغیر وابسته تحقیق بوده‌اند. درخت تصمیم ارائه‌شده در پژوهش آن‌ها نیز نشان می‌دهد که با استفاده از این الگو می‌توان موفقیت ارائهٔ خدمات بانکداری اینترنتی را قبل از اجرا، پیش‌بینی کرد.

دیواندری و همکاران (۱۳۹۲) نیز پژوهشی با عنوان "ارائهٔ الگوی مفهومی برای تبیین عوامل کلیدی مؤثر بر کیفیت سیستم‌های ارائه‌دهندهٔ خدمات بانکداری اینترنتی؛ پیمایشی پیرامون بانک ملت" انجام دادند. الگوهای ارائه‌شده در پژوهش آن‌ها نشان‌دهندهٔ این مهم است که از بین عوامل مؤثر بر کیفیت سیستم‌های ارائه‌دهندهٔ خدمات بانکداری اینترنتی، سهولت استفاده از سیستم‌ها، دارای بالاترین درجه‌ی همبستگی با کیفیت سیستم‌های ارائه‌دهندهٔ خدمات بانکداری اینترنتی است. پس از آن به ترتیب جذابیت و سودمندی به‌کارگیری از سیستم‌ها به طور مشترک، سرعت سیستم‌ها در ارائهٔ خدمات، ثبات سیستم‌ها و در نهایت، امنیت سیستم‌ها قرار گرفته‌اند. نتایج حاصل از این الگو در خصوص شدت رابطهٔ هر یک از متغیرهای مشاهده‌شده نیز نشان می‌دهد که از دیدگاه مشتریان و کاربران سیستم‌های ارائه‌دهندهٔ خدمات بانکداری اینترنتی، سیستم‌هایی با کیفیت به‌شمار می‌آیند که امکان استفادهٔ آسان

از آن‌ها فراهم بوده و همچنین فرآیند اســـتفاده از خدمات بانکی اینترنتی با استفاده از آن‌ها، جذاب باشد.

پلیس فضای تولید و تبادل اطلاعات (۱۳۹۷) راه‌حل نصب یک قطعهٔ پلاستیکی در دریچهٔ ورود کارت دستگاه‌های خودپرداز را ارائه می‌دهد که هرگونه دستکاری در دریچهٔ کارت‌خوان به‌وجود آید و یا این‌که دریچه‌ی تحت فشار فیزیکی قرار گیرد، دستگاه خودپرداز از حالت سرویس‌دهی خارج می‌شود.

شوما ایلا، جان پالیستر و جردن. آر (۲۰۰۳) پژوهشی تحت عنوان "الگوی پیشنهادی برای امنیت در بانکداری الکترونیکی" انجام داده‌اند. آن‌ها در این پژوهش به بررسی میزان اهمیت بانکداری الکترونیکی و نقش و اهمیت اعتماد در بانکداری الکترونیکی پرداخته‌اند و اظهار می‌دارند که در یک معاملهٔ الکترونیکی که در یک محیط مجازی است: مانند بانکداری الکترونیکی، نسبت به یک معاملهٔ رودررو در یک محیط واقعی، اعتماد نقش مهم‌تری دارد و این می‌تواند به دلیل نگرانی افراد از امکان سوءاستفاده‌های مالی بیشتر باشد.

در مطالعه‌ای که به منظور سنجش خدمات نوین بانکی توسط برخی اساتید دانشگاه چندرسانه‌ای[1] انجام شده‌است، توسعهٔ تکنولوژی‌های ارتباطی و مخابراتی عامل جهش و تغییر عمده در بخش بانکی مالزی معرفی شده‌است. نتیجهٔ این تغییر، استفاده‌ی گسترده از خدمات نوین بانکی مانند عابربانک، تلفن‌بانک و بانکداری خانگی بوده‌است. این تغییرات عمده به منظور جلب رضایت مشتریان بانک صورت گرفته‌است. در بین خدمات ذکرشده، بیشترین استقبال و استفاده از عابربانک و کم‌ترین آن از تلفن‌بانک بوده‌است. برطبق مطالعات این پژوهشگران، بانکداری اینترنتی هنوز در مالزی ایجاد نشده‌است، اما به نظر می‌رسد دولت درپی ایجاد شرایط پیاده‌سازی آن است (کریشنان گرو[2] و دیگران، ۲۰۰۴)

زورجا و باچ[3] (۲۰۱۶) در مطالعهٔ خود با استفاده از روش K-mean به بررسی اثر فناوری اطلاعات و ارتباطات بر رقابت‌پذیری اقتصادی در کشورهای اروپایی پرداختند. آن‌ها کشورهای اروپایی را براساس شاخص‌های فناوری اطلاعات و ارتباطات در زمینهٔ استفاده از اینترنت، آموزش الکترونیک، تجارت الکترونیک و دولت الکترونیک به چهار دسته تقسیم کردند و شاخص‌های رقابت‌پذیری را در این گروه‌ها با یک‌دیگر مقایسه کردند. بر این اساس، گروه‌های دارای وضعیت مناسب‌تر در فناوری اطلاعات از رقابت‌پذیری بیشتری برخوردار بودند.

کال و جون، در پژوهشی با عنوان "شناسایی عوامل کلیدی اثرگذار بر کیفیت خدمات بانکداری اینترنتی"، به‌دنبال شناسایی عوامل کلیدی اثرگذار بر کیفیت خدمات بانکداری اینترنتی، ازطریق روش تحلیل محتوای نظرات مشتریان بانکداری اینترنتی، در مورد تجربه‌های آن‌ها در بهره‌گیری از این خدمات بودند. پس از انجام بررسی‌های متعدد، هفده عامل مؤثر برکیفیت خدمات بانکداری اینترنتی شناسایی و در سه رده دسته‌بندی شدند. در این پژوهش، متغیرهای سهولت استفاده از سیستم‌ها، قابلیت اطمینان سیستم‌ها، ثبات و عدم خطای سیستم‌ها، جذابیت سیستم‌ها، امنیت سیستم‌ها و اطلاع‌رسانی در مورد خدمات ارائه‌شده، بررسی و به‌عنوان مبنایی برای طرح فرضیه‌ها در نظر گرفته شده‌اند (مینیجون[4]، ۲۰۰۱).

بریتین[5] (۲۰۱۸) با ارائهٔ ده پیشنهاد و ذکر نکات امنیتی ازجمله استفاده از کارت‌های بانکی EMV، با این توضیح که در طی یک معامله با قراردادن کارت در شکاف دستگاه کارت‌خوان معامله انجام می‌شود. استفاده از این نوع

1. Multi media
2. Krishnan Guru
3. Zoroja & Bach
4. Minijoon
5. Jac Brittsin

کارت‌ها امنیت بالاتری را ارائه می‌دهد، به این علت که برخلاف نوار مغناطیسی روی کارت، که حاوی داده‌های ثابتی است و در هر معامله یکسان است، کارت‌های EMV با هر تراکنش تغییر می‌کنند و اساساً پیش‌بینی آن‌ها غیرممکن است.

پتر[1](۲۰۲۰) با بررسی نحوهٔ عملکرد اسکیمرها، روش مقابله و جلوگیری از سرقت به روش اسکیمینگ به این نتیجه دست یافت که استفاده از کارت‌های اعتباری EMV دارای چیپ، که نسبت به کارت‌های اعتباری مغناطیسی امنیت بیشتری دارند. در این کارت‌های اعتباری، داده‌ها برای هر تراکنش منحصر در یک چیپEMV نگهداری می‌شود که باعث حفظ اطلاعات در برابر سارقان اطلاعات می‌شود.

در جدول(۱-۱) در زیر، مجموعه‌ای از جرایم سایبری شناخته‌شده، که در سال‌های اخیر مورد توجه سارقان اطلاعاتی بوده و بسیار زیاد به منظور کسب منافع مالی و سودجویی‌های اقتصادی مورد استفاده قرار گرفته و جمع‌آوری شده‌است.

جدول ۱- انواع جرایم سایبری در **فضای مجازی**[1]

جرایم سایبری	
بدافزارها	بدافزارها مثل ویروس‌ها و جاسوس‌افزارها پس از نصب فعالیت شما را رصد می‌کنند و به سیستم شما آسیب می‌زنند
فیشینگ صوتی	یک حملهٔ فیشینگ صوتی است که در آن یک تماس صوتی از مهاجم به قربانی مورد نظر گرفته می‌شود تا به نوعی وی را متقاعد به ارائهٔ اطلاعات شخصی کند
اسکیمینگ	نسخه‌برداری‌کردن غیر قانونی داده‌های کارت بانکی روی یک کارت خام دیگر به وسیلهٔ دستگاهی به نام اسکیمر
فیشینگ سایبری	روشی که مجرمین از طریق آن اطلاعات شخصی شما را اعم از اطلاعات مالی یا غیر مالی به‌دست می‌آورند
فارمینگ	مجرم ازطریق نصب یک رمز بر روی سیستم قربانی، او را هنگام اتصال به سایت‌های قانونی مثل سایت بانک به سایت‌های تقلبی و جعلی هدایت می‌کند
حملات DDOS	حملات متعددی از سوی سیستم‌های مختلف بر روی یک شبکه صورت می‌گیرد. حمله‌ای که کامپیوتر یا سایت شما را غرق در داده می‌کند و مانع از فعالیت مناسب آن می‌شوند
اسمیشینگ	اسمیشینگ استفاده از پیام متنی (SMS) برای فریب‌دادن قربانیان جهت دانلود بدافزار موبایلی، بازدید از یک سایت مخرب یا تماس با یک شماره تلفن جعلی می‌باشد
ترمینیشن و اورجینیشن	ترمینیشن انتقال تماس‌های تلفنی اینترنتی از خارج به داخل کشور و اورجینیشن انتقال تماس‌های تلفنی اینترنتی از داخل به خارج از کشور می‌باشد

در تشریح روش "اسکیمینگ" از طریق کارت‌خوان‌ها، فروشنده (یا گاهی همان سارق) کارت‌خوان را پشت پیش‌خوان قرار می‌دهد و کارت مشتری را به‌جای پوز، بر روی دستگاه اسکیمر می‌کشد، رمز نیز توسط فروشنده وارد می¬شود و به همین سادگی تمام اطلاعات فرد در اختیار سارق قرار می‌گیرد. کلاه‌برداران در این روش، پس از نوار مغناطیسی که در پشت کارت بانکی قرار دارد، نسبت به تهیهٔ یک نسخه از کارت بانکی اقدام کرده و از آن در تراکنش‌های بانکی استفاده می‌کنند.

1. Poyush Pater

مسـألهٔ قابل طرح این اسـت که با چه اقدام یا اقداماتی می‌توان در مرحلهٔ اول سرعت رشد این جرایم را کاهش و در مرحلهٔ بعد تحت کنترل داد؟

به گفتهٔ سردار حسین رحیمی، رئیس پلیس پایتخت، در سال ۱۳۹۸، ۶۷ درصد از جرایم فضای مجازی مربوط به حوزهٔ اقتصادی بوده و ۱۷ درصد از جرایم مربوط به موضوعات اخلاقی و مابقی اجتماعی بوده‌است. این درحالی است که وقوع این جرایم نسبت به مدت مشابه در سال گذشته، ۱۳۰ درصد افزایش داشته‌است. این مقدار نشان از سرعت و شیب رشد صعودی این‌گونه جرایم دارد که به منظور کنترل و تقلیل اینگونه جرایم باید اقداماتی به‌صورت فنی و الکترونیکی صورت گیرد (The Islamic Republic News Agency, 1398).

از طرفی، با توجه به به‌کارگیری رمز دوم پویا برای تراکنش‌های بانکی، درصد جرایم اقتصادی فیشینگ استان همدان در فضای سایبری، کاهش چشم‌گیری را داشته که حاکی از کاهش دسترسی سارقان به اطلاعات بانکی افراد از روش فیشینگ دارد. اما با این شرایط و محدودیت‌های اعمال‌شده در تراکنش‌های اینترنتی با وجود رمز دوم پویا، سارقان چه روش جایگزینی را انتخاب می‌کنند؟

با توجه به جدول ۱-۱ روشی که سارقان در کوتاه‌ترین زمان، بدون به‌جاگذاشتن ردپایی از خود و با جامعهٔ آماری قربانیان بالا می‌توانند مبادرت به سرقت اطلاعات و سودجویی‌های خود کنند، روش "اسکیمینگ" است (پلیس فضای تولید و تبادل اطلاعات).

مفهوم بانکداری الکترونیک

بانکداری الکترونیک، عبارت است از، فراهم‌آوردن امکاناتی برای کارکنان درجهت افزایش سرعت و کارایی آن‌ها در ارائهٔ خدمات بانکی در محل شعبه و هم‌چنین فرآیندهای بین شعبه‌ای و بین‌بانکی در سراسر دنیا و ارائهٔ امکانات سخت‌افزاری و نرم‌افزاری به مشتریان که با استفاده از آن‌ها بتوانند بدون حضور فیزیکی در بانک‌ها، در هر ساعت از شبانه روز و به‌صورت ۲۴ ساعته ازطریق کانال‌های ارتباطی امن، عملیات بانکی دل‌خواه خود را انجام دهند. به عبارت دیگر، بانکداری الکترونیک استفاده از فناوری‌های پیشرفته سخت‌افزاری و نرم‌افزاری مبتنی بر مخابرات و شبکه برای تبادل اطلاعات و منابع مالی به‌صورت الکترونیکی است و نیازی به حضور فیزیکی مشتری در شعبه بانک نیست. بانکداری الکترونیک از دیدگاه افراد بسیاری، تنها شامل بانکداری اینترنتی می‌شود، درحالی که مفهوم بانکداری الکترونیک بسیار گسترده‌تر می‌باشد (عنداله، ۱۳۹۶).

انواع حملات اسکیمینگ

این نوع از حملات بانکی به دو طریق صورت می‌گیرد:

۱- ازطریق عابربانک

۲- ازطریق دستگاه‌های کارت‌خوان (POS)

روش سرقت از طریق عابربانک‌ها شیوه‌ای بسیار ساده و البته حرفه‌ای است. در این نوع از سرقت، سارق یک بخش جدیدی را به خودپرداز متصل می‌کند که تفاوت بسیار کمی با شکل اصلی عابربانک دارد (یک قسمت جدید به بخش کارت‌خوان افزوده می‌شود). از طریق این بخش، کاربری که کارت خود را وارد دستگاه می‌کند تا کارهای مورد نظر خود را انجام دهد، سارق می‌تواند تمام اطلاعات کارت را ذخیره کند. اکنون، نوبت به رمز می‌رسد. برای این کار دو روش در اسکیمینگ وجود دارد. در روش اول، یک دوربین بسیار ریز (در حد سوراخی به اندازه کبریت) زیر دستگاه فوق‌الذکر قرار می‌گیرد، که در حین وارد کردن اطلاعات توسط کاربر، آن‌ها را ضبط می‌کند و در اختیار سارق قرار می‌دهد. روش دوم در خودپردازها به این صورت است که در آن یک صفحه‌کلید جدید را روی صفحه‌کلید قبلی دستگاه قرار می‌دهند که از لحاظ ظاهری بسیار شبیه به نسخهٔ اصلی است و این پنل جدید اطلاعات

واردشده توسط کاربر را ذخیره می‌کند که این اطلاعات شامل رمز عبور وی نیز می‌شود. حال، اطلاعات لازم و کافی در اختیار سارق قرار دارد. در وهلهٔ بعد، سارق اطلاعات را روی کارت خام جدیدی می‌ریزد و سپس با این کارت به‌سراغ یک خودپرداز می‌رود و خیلی طبیعی پول موجود را تا سقف مورد قانونی در روز دریافت می‌کند یا از طریق کارت‌خوان‌های فروشگاهی کالایی را خریداری می‌کند.

شکل ۱- شمای نصب دوربین در بالای صفحه کلید خودپرداز

خودپرداز تنها جایی نیست که سارقان می‌توانند ازطریق اسکیمر وارد عمل شوند. کارت‌خوان‌های فروشگاهی(POS) نیز امکان نصب اسکیمر را دارند که در ایران نیز مواردی از این نوع سرقت کشف شده‌است. دستگاه‌های کارت‌خوان سیار نسل جدیدی از دستگاه‌های کارت‌خوان هستند که از طریق خدمات سامانه‌ی تلفنی همراه به شبکه‌های بانکی متصل می‌شوند و تمامی تراکنش‌های بانکی را توسط شبکه‌ی تلفن همراه و استفاده از سرویس‌های GMS و GPRS انجام می‌دهند. سرقت اسکیمینگ از طریق کارت‌خوان‌ها بدین شکل است که سارق، اسکیمر را روی دستگاه نصب می‌کند و سپس فروشنده (یا گاهی همان سارق) که کارت‌خوان را پشت پیش‌خوان قرار داده، کارت مشتری را روی آن می‌کشد و سپس رمز نیز توسط فروشنده وارد می‌شود و به همین سادگی تمام اطلاعات فرد در اختیار سارق قرار می‌گیرد.

به گفتهٔ پلیس فتا، در شایع‌ترین روش اسکیمینگ فرد کلاه‌بردار از دستگاه کارت‌خوان برای نسخه‌برداری اطلاعات کارت مشتریان استفاده می‌کند. در این روش، مغازه‌دار،

فروشنده یا هرکسی که در پشت صندوق قرار دارد به بهانه‌های مختلف اقدام به گرفتن کارت از مشتری کرده و به دور از چشمان مشتری، اول کارت را به روی دستگاه اسکیمر کشیده و پس از کپی‌برداری از اطلاعات داخل کارت آن را در دستگاه کارت‌خوان (pos) کشیده و رمز چهار رقمی را می‌پرسد؛ عملاً با گفتن رمز کارت این فرد می‌تواند کارت دیگری را ساخته و حساب فرد مشتری را خالی کند (پلیس فضای تولید و تبادل اطلاعات).

اهداف پژوهش

هدف کلی

شناخت و ارائهٔ راه‌کارهای عملی جهت کاهش جرایم "اسکیمینگ اقتصادی"

اهداف جزئی

در این پژوهش، قصد داریم با مطالعه و بررسی پرونده‌های جرایم اقتصادی استان همدان در فضای سایبری، به‌خصوص جرایم "اسکیمینگ"، به ارائهٔ راه‌کارهایی جهت پیشگیری، کنترل و کاهش این جرایم بپردازیم.

همچنین، در این پژوهش به دنبال دستیابی به اهدافی از قرار زیر هستیم:

۱- شناخت زیرساخت شبکه‌های فناوری اطلاعات و ارتباطات مورد نیاز جهت راه‌اندازی بستری امن برای تراکنش‌های کارتی،
۲- تبیین و شناسایی تهدیدات آسیب‌رسان به شبکهٔ بانکی کشور در حوزهٔ کارت‌های بانکی،
۳- ارائهٔ ساختار مقابله با جرایم اسکیمینگ، با توجه به مؤلفه‌های سخت‌افزاری، نرم‌افزاری و بسترهای ارتباطی.

سؤال پژوهش

راه‌های مقابله با جرایم اسکیمینگ اقتصادی در بانکداری الکترونیک ایران با توجه به زیرساخت‌های نظام بانکی و فناوری اطلاعات و ارتباطات، شرایط تحریمی حاکم بر کشور و با توجه به نمونهٔ مطالعاتی استان همدان چیست؟

روش پژوهش

در تحقیقات توصیفی، محقق به دنبال چیستی و چگونگی موضوع است و می‌خواهد بداند ماهیت پدیده، متغیر، شیء یا مطلب چیست و چگونه است. به عبارت دیگر، این تحقیق وضع موجود را بررسی می‌کند و به توصیف منظم و نظام‌مند وضعیت فعلی می‌پردازد و ویژگی‌ها، صفات، ماهیت، فرآیندها و روندهای آن را مطالعه و در صورت لزوم ارتباط بین متغیرها را بررسی می‌نماید (حافظ‌نیا، ۱۳۹۹). در این روش، محقق الزاماً در پی کشف و توضیح روابط، همبستگی‌ها و احتمالا آزمودن فرضیه‌ها و پیش‌بینی رویدادها نیست، بلکه توجه او بیشتر در جهت توصیف‌کردن و گزارش‌نویسی از موقعیت‌ها و وقایع بر اساس اطلاعاتی است که صرفاً جنبه وصفی دارند (علی‌احمدی و نهائی، ۱۳۸۶).

تحقیقات توصیفی هم جنبهٔ کاربردی دارند و هم جنبه‌ی مبنایی؛ در بعد کاربردی (که مدنظر تحقیق پیش رو است) از نتایج این تحقیقات در تصمیم‌گیری و سیاستگذاری‌ها و همچنین برنامه‌ریزی‌ها استفاده می‌شود. در این تحقیقات، نوعاً از روش‌های مطالعهٔ کتابخانه‌ای و بررسی متون و محتوای مطالب و همچنین روش‌های میدانی نظیر پرسش‌نامه، مصاحبه و مشاهده استفاده می‌شود (حافظ‌نیا، ۱۳۹۹).

داده‌های پژوهش(پرونده‌های موردنظر)، از پلیس فضای تولید و تبادل اطلاعات استان همدان به‌دست می‌آید و جامعهٔ آماری مورد بررسی به‌عنوان نمونه‌ای از کل کشور، استان همدان خواهد بود.

یافته‌های تحقیق

- **RFID و NFC**

یکی از فناوری‌های شبکه‌های نسل جدید (NGN)، RFID و NFC است. ارتباط میدان نزدیک NFC (near field communication)، یک فناوری ارتباطی بی‌سیم با فرکانس بالا و دامنهٔ کوتاه است که انتقال داده بین دستگاه را تا فاصله‌ای در حدود ۱۰ سانتی‌متر با فرکانس ۱۳,۵۶MHZو بدون نیاز به تنظیمات کاربر، امکان‌پذیر می‌نماید. برای این‌که دو دستگاه بتوانند ارتباط برقرارکنند، کافی است آن‌ها را در نزدیکی یکدیگر قرارداده که در این حالت اینترفیس NFC موجود در دستگاه‌ها به‌صورت خودکار تنظیمات مورد لازم را انجام می‌دهد و ارتباط به‌صورت peer-to-peer بین دو دستگاه برقرار می‌گردد.

این فناوری مبتنی بر RFID بوده و نمونهٔ سادهٔ توسعه یافته‌ای از استاندارد ISO14443 است که استانداردی برای سیگنال‌های RFID و کارت‌های contact less است که در واقع ترکیبی از اینترفس کارت‌های هوشمند و خواننده (raeder) در یک دستگاه تشکیل شده‌است. این فناوری همان‌طور که قادر است با سایر دستگاه‌های NFC ارتباط برقرار نماید، این توانایی را نیز دارد که با خواننده‌های دیگر و کارت‌های هوشمند منطبق با استاندارد ISO14443 ارتباط برقرار کند. بنابراین، دارای قابلیت سازگاری بالایی هستند و برای استفاده از آن می‌توان از زیرساخت‌های contact less موجود برای سیستم‌های حمل و نقل و پرداخت استفاده کرد. بنابراین، هزینهٔ راه‌اندازی آن بسیار پایین و به‌صرفه است. نرخ تبادل اطلاعات آن به ۴۲۴Kb/s می‌رسد که همین امر قابلیت آن را برای پرداخت‌های با حجم بالا بسیار مناسب ساخته است.

- **ساخت نرم‌افزار NFC READER برای اندروید**

Android SDK[1] پشتیبانی‌ای را برای خواندن برچسب‌ها و کارت‌های NFC به‌صورت استاندار ارائه می‌دهد. در این بخش، به‌دنبال ایجاد برنامه‌ای برای خواندن برچسب‌ها و کارت‌های NFC با Android Studio [2]هستیم. ابتدا باید مجوز NFC را در Android Manifest برنامه خود اضافه کنیم. همچنین، تعریف می‌کنیم که برنامه از ویژگی NFC بهره می‌برد. برای تجزیه و تحلیل داده‌ها، از برچسب NFC خوانده‌شده از برخی کلاس‌های ایجادشده توسط google برای پروژه open source اندروید در نسخه‌های نمایشی بهره می‌بریم که نحوهٔ استفاده از NFC را نشان می‌دهد. رابط تجزیه‌کنندهٔ NDEF Record اطلاعات خوانده شده از NFC Card را بازگردانده و نشان می‌دهد:

۱. یک پکیج برای URI Record با اجرای روش STR، اجازه می‌دهد تا بفهمیم آیا داده‌های خوانده‌شده از کارت NFC یا Tag، می‌تواند به‌عنوان URI درنظر گرفته‌شود؟
۲. مورد دیگر برای TextRecord برای مبنای همین اصل است.
۳. مورد دیگر برای پوسترهای هوشمند که ترکیبی از URI و Text است به قرار زیر است.
۴. ایجاد یک تجزیه‌کننده‌ی پیام NDEF.

داده‌های ردوبدل‌شده ازطریق NFC ازقالب Ndef استفاده می‌کنند. Ndef به معنی قالب تبادل دادهٔ NFC است. بنابراین، برای تجزیه و تحلیل داده‌های ردوبدل‌شده، مامی‌خواهیم یک کلاس NdefMessageParser ایجاد کنیم. این یک روش تجزیه و تحلیل ثابت است که پارامتر NdefMessage را می‌گیرد و محتوای این پیام را به‌عنوان فهرستی از موارد Parsed Ndef Record بازمی‌گرداند.

برای کلاس Parser Message Ndef، رمزی را از Google برای پروژه منبع باز اندروید تطبیق می‌دهیم.

- **ایجاد رابط کاربری**

اکنون می‌توانیم رابط کاربری برنامهٔ NFCReader خود را ایجاد کنیم. این رابط کاربری فقط با یک ImageView نشان‌دهندهٔ یک آرم و یک که برای نمایش داده‌های خوانده‌شده از برچسب NFC یا Tag اسکن‌شده استفاده می‌شود.

- **رمز جاوای برنامه NFCReader**

اکنون رمز فعالیت اصلی را می‌نویسیم. در کلاس MainActivity از برخی روش‌های ارائه‌شده توسط Google برای پروژه OpenSource اندروید استفاده خواهیم کرد.DumpdataTag یک شیء Tag را در یک پارامتر مشخص می‌گیرد و داده‌های ریخته‌شده در این Tag را در قالب String برمی‌گرداند:

۱- toHex، toReversedHex، toDec و toReversedDec از روش‌های ایستا استفاده می‌کنند که به ما امکان چاپ بایت با فرمت Hexadecimal یا Decimal را از داده‌های خوانده شده در Tag یا Card می‌دهد.
۲- در کلاس MainActivity، برخی ازخصوصیات را تعریف می‌کنیم.
۳- یکی با هدف NFCAdapter از SDK استاندارد اندروید استفاده می‌کنیم.
۴- یکی برای PendingIntent که برای راه‌اندازی برنامه ما هنگام اسکن Tag یا SmartCard استفاده می‌شود.

۱. SDK شامل مجموعه‌ای از ابزارها (مثلاً کتابخانه‌ها، توابع کامپایل شده و...) است که جهت راحت‌تر کردن برنامه‌نویسی برای یک محیط یا پلتفرم خاص طراحی شده و در اختیار برنامه‌نویس قرار داده شده‌است.

۲. نرم‌افزار Android Studio یک محیط توسعهٔ یکپارچه (IDE) رسمی برای توسعه پلتفرم و برنامه‌نویسی اندروید است.

آخرین مورد برای TextView به‌منظور نمایش اطلاعات خوانده شده استفاده می‌شود

۵- در روش Oncreate، ما مرجع را از Text View دریافت می‌کنیم. سپس با خواندن روش استاتیک get Default Adapter نمونه پیش‌فرض NFC Adapter را از شیء NFC Adapter دریافت می‌کنیم.

اگر NfcAdapter برگردانده‌شده خالی باشد، ما toast را برای کاربر نمایش می‌دهیم و فعالیت فعلی را به پایان می‌رسانیم. در غیر این صورت، ما یک نمونه Pending Intent ایجاد می‌کنیم که به فعالیت فعلی اشاره دارد.

در روش on Resume، ما با فراخوانی روش is Enabled در نمونه‌ی NfcAdapter بررسی می‌کنیم که آیا NFC فعال باشد یا خیر. اگر فعال نیست، صفحه تنظیمات بی‌سیم را به کاربران نمایش می‌دهیم تا اجازه دهیم آن را فعال کنند. برای این منظور ما باید فقط یک دستور با عملکرد ACTION_WIRELESS_SETTINGS ایجاد کنیم و سپس فعالیت مرتبط را راه‌اندازی کنیم. اگر NFC قبلاً فعال شده باشد، ما با استفاده از روش enable Foreground Dispatcher در نمونهٔ NfcAdapter با Pending Intent که قبلاً ایجاد شداست، ارتباط برقرار می‌کنیم. در روش on Pause، مهم است که با فراخوانی روش disable Foreground Dispatch در نمونهٔ NfcAdapter، امکانات پیش‌زمینه را غیرفعال کنیم.

مرحلهٔ بعدی، لغوکردن روش on New Intent است که وقتی سلول NFC کارت یا برچسب NFC را تشخیص می‌دهد، فراخوانی می‌شود. در این روش، ما با استفاده از روش resol Intent فراخوانی می کنیم. به این معنا که ما با آزمایش عکس‌العمل دریافت‌شده ازطریق Intent شروع می‌کنیم. اگر عکس‌العمل دریافت‌شده _TAG_ ACTION_ DISCOVERED،ACTION_TECH_DISCOVER ED یا ACTION_NDEF_DISCOVERED باشد، ما داده‌های موجود در Intent را دریافت می‌کنیم.

برای این منظور، روش get Parcelable Array Extra را در Intent با پارامتر ثابت _NDEF_ EXTRA_ MESSAGES فراخوانی می‌کنیم.

اگر EXTRA_NDEF_MESSAGES خالی نباشد، ما از این داده‌ها، Ndef Message ایجاد می‌کنیم. در غیر این صورت، با فراخوانی روش get Byte Array Extra سعی می‌کنیم داده‌ها را از محتوای EXTRA_ID از Intent دریافت کنیم، همچنین، موضوع Tag را نیز دریافت می‌کنیم. سپس، ما روش dump Tag Data را با این نمونه برچسب در پارامتر فراخوانی می‌کنیم. سپس، با خواندن محموله، یک Ndef Record ایجاد می‌کنیم. از این Ndef Record، یک Ndef Message ایجاد می‌کنیم. در پایان روش، ما با استفاده از پارامتر Ndef Message، متد display Msgs را فراخوانی می‌کنیم.

آخرین مرحلهٔ نوشتن رمز روش display Msgs است. در این روش، ما اولین پیام فهرست را تجزیه می‌کنیم. سپس، آن را بر روی Parsed Ndef Record تکرار می‌کنیم. برای هر رکورد، با روش str آن را می‌خوانیم تا محتوای آن را به‌دست آوریم. در پایان، می‌توانیم داده‌ها را در Text View از رابط کاربری خود نمایش دهیم. در آخر برنامه NFC Reader که ساختیم را روی گوشی همراه اندروید نصب کرده و کارت NFC یا Tag را اسکن می‌کنیم تا اطلاعات آن خوانده شود.

نتیجه‌گیری

مصاحبه‌ها و مراجعات صورت‌گرفته با صاحبان کارت‌های بانکی و بانک‌ها در راستای انجام پژوهش حاضر گویای این مطلب بود که عموم مردم نسبت به این نوع از سرقت‌ها به‌خصوص حملات اسکیمینگ اطلاع و شناختی ندارند که سارقان نیز از این ناآگاهی صاحبان کارت‌های بانکی و برخی مسؤولین سوءاستفاده کرده و برای کسب منافع

شخصی، اطلاعات کارت مشتریان را به روش‌های ذکرشده در پژوهش حاضر سرقت می‌کنند. در نتیجه، افزایش سطح آگاهی مشتریان و بانک‌ها در پیشگیری از وقوع جرم مؤثر است. لذا، پیشنهاد می‌شود، جهت افزایش سطح آگاهی مشتریان از رسانه‌های ملی و فضاهای مجازی استفاده گردد. برای نیل به این هدف می‌توان با تهیهٔ انیمیشن‌های مرتبط با این نوع حملات اقدام به افزایش سطح آگاهی صاحبان کارت‌ها و مراجع مربوط از جمله بانک‌ها و سازمان فناوری اطلاعات و ارتباطات نمود.

مطابق یافته‌های Whitty (2017) قربانیان جرایم اقتصادی فضای سایبری اغلب دارای ویژگی‌های مشترکی چون پیری، عدم رشد فکری و بی‌تجربگی در استفاده از اینترنت، بی‌توجه به نکات امنیتی، زودباور و ساده‌لوحی هستند که کلاه‌برداران می‌توانند بر آن‌ها تأثیر بگذارند و اطلاعات مالی و شخصی آن‌ها را سرقت کنند (Monica T.Whitt, 2017). همچنین، بررسی پرونده‌های موجود در پلیس فتای استان همدان، نشان می‌دهد افرادی که مورد هدف سارقان هستند، افراد مسنی هستند (افراد بالای ۵۰ سال) که آگاهی نسبت به این نوع حملات بانکی ندارند. همچنین، از نظر سارقان احتمال اینکه افراد مسن متوجه سرقت انجام‌شده بشوند و به مراجع ذیربط اطلاع دهند کم‌تر است. سارقان برای سرقت از این افراد، بیشتر از دستگاه‌های POS استفاده کرده‌اند.

علاوه‌بر این، با توجه به این‌که امروزه اکثر تلفن‌های همراه و تبلت‌ها به فناوری NFC مجهز شده‌اند و تعداد ابزارهای هوشمندی که از این فناوری استفاده می‌کنند به‌سرعت در حال افزایش است. این فناوری بستری امن را برای انجام خدمات پرداخت و بانکداری همراه فراهم می‌کند. در این پژوهش نیز، باتوجه به مطالعات صورت‌گرفته طرحی کاربردی و قابل اجرا در قالب نرم‌افزاری کاربردی ارائه گردید که می‌تواند درجهت کنترل و کاهش جرایم اسکیمینگ و کاهش هزینه‌های ارائهٔ کارت‌های بانکی توسط بانک‌ها و کاهش انواع خطرات و حملات سارقان، به‌شدت نقش داشته باشد.

محدودیت‌ها و راه‌کارهای طرح جهت استفاده از فناوری NFC

در این بخش، درصدد ارائهٔ طرح‌ها و پیشنهادهایی درخصوص پرداخت‌های سیار یا Mobile Payment هستیم، که هدف از آن‌ها ایجاد یک بستر پرداخت مناسب، امن، مقرون به‌صرفه و قابل گسترش با حداکثر بهره‌گیری از امکانات ارتباطی موجود، اپراتورهای همراه و شبکه NGN می‌باشد.

اولین مسأله‌ای که بانک‌ها را در به‌کارگیری فناوری NFC در گوشی‌های همراه به چالش می‌کشد، امنیت حساب مشتریان در زمان استفاده از NFC است، که این موضوع با طراحی نرم‌افزاری کاربردی که با فناوری NFC سازگار بوده و با واردکردن رمز تعریف‌شده توسط کاربر(مشتری) اجرا می‌شود و NFC مربوط را جهت استفاده فعال می‌کند، قابل تعریف است. دارندگان تلفن همراه هوشمند با نصب نرم‌افزار کاربردی موردنیاز می‌توانند در زمان خرید، گوشی را به دستگاه کارت‌خوان مجهز به‌NFC نزدیک کرده و عملیات پرداخت انجام شود، البته ویژگی مهم در استفاده از NFC تضمین حفظ اطلاعات کاربر است؛ زیرا پیغام‌ها به‌صورت رمزنگاری‌شده به دستگاه ارسال می‌شود، دستگاه گیرنده نیز دارای نرم‌افزار کاربردی مشخصی است که می‌تواند پیغام‌ها را دریافت و به مرکز ارسال نماید.

مسألهٔ بعدی، استفاده از یک شبکهٔ جامع بانکی برای تمامی بانک‌ها است که بتوان تحت پوشش آن، با حساب‌های تمامی بانک‌ها تراکنش‌ها را به‌وسیلهٔ فناوری NFC انجام داد. برای تحقق این مهم (یک‌پارچه‌سازی حساب‌های بانکی)، باید یک کیف پول مرجع در یک سیستم جامع تعریف شود، به‌طوری‌که فعالیت‌های سایر

کیف‌پول‌ها (از هر حساب و از هر بانکی) در این سیستم انجام پذیرد. البته، باید بدانیم که این فناوری تنها در کیف پول الکترونیک کارایی ندارد؛ بلکه بلیط‌های مترو و اتوبوس و ژتون غذا در دانشگاه هم نمونه‌هایی از فناوری NFC هست.

نکتهٔ دیگر، باتوجه به این‌که، اکثر حملات اسکیمینگ در تراکنش‌های فروشگاهی و خریدهای خرد اتفاق می‌افتد و جهت امن‌تر شدن تراکنش‌ها، باید برای کیف‌های پول همراه یک سقف (فرضا ۵۰۰ هزارتومان) تعریف گردد.

نکته‌ی حائز اهمیت در این پژوهش این است که، برخی معتقدند علت عدم استفاده از فناوری NFC، ضعف شبکه‌های مخابراتی است. اما، حقیقت نشان می‌دهد که این فناوری همچون بلوتوث و Wi-Fi نیازی به خدمات مخابراتی ندارد و شرایط استفاده باید توسط بانک‌ها و مؤسسات مرتبط ایجاد شود، اقدامی که ظاهراً در بایگانی بانک‌ها خاک می‌خورد.

منابع

۱. پلیس فضای تولید و تبادل اطلاعات ناجا (cyberpolice.ir/ https://www.)

۲. حافظ‌نیا، محمدرضا. (۱۳۹۹). *مقدمه‌ای بر روش تحقیق در علوم انسانی*. نشر سازمان مطالعه و تدوین کتب علوم‌انسانی دانشگاه‌ها (سمت).

۳. دیواندری، علی؛ عابدی، احسان و ناصرزاده، سیدمحمدرضا. (۱۳۹۲). ارائه الگوی مفهومی برای تبیین عوامل کلیدی مؤثر بر کیفیت سیستم‌های ارائه‌دهنده خدمات بانکداری اینترنتی (پیمایشی پیرامون بانک ملت). *نشریه مدیریت فناوری اطلاعات. دوره۵*، شماره۱، صفحات۳۶-۱۹.

۴. عندالله، باقر. (۱۳۹۶). *بررسی شیوه‌های مختلف بانکداری الکترونیک و تأثیر آن بر افزایش درآمد بانک ملی ایران*. رساله دوره کارشناسی ارشد، دانشگاه آزاد اسلامی واحد نراق

۵. احمدی، علی؛ علیرضا، سعید و نهایی، وحید. (۱۳۸۶). *توصیفی جامع از روش‌های تحقیق (پارادایم‌ها، استراتژی‌ها، طرح‌ها، رویکردهای کمی، کیفی و ترکیبی)*. نشر تولید دانش.

۶. کاظمی، مهدی؛ کرد، باقر و مهرورزی، محمد. (۱۳۸۹). بررسی عوامل کلیدی مؤثر بر موفقیت عرضه خدمات اینترنتی و ارائه یک الگو پیش‌بینی‌کننده با استفاده از درخت تصمیم‌گیری. *پژوهش‌های مدیریت عمومی، سال سوم*، شماره دهم، ۴۵-۲۹.

7. Alachandher, K., & Santha, V. (2004). Electronic Banking in Malaysia: A Note on Evalution on Evaloution of services and Consumer Reactions. *Journal of Internet Banking and Commerce*, *1*(2), 56-70.
8. Brittain, J. (2018). *10 Tips to help cardholders steer clear of credit card skimmer fraud*. Loos Prevention Magazine.
9. Hebert, A. (2014). *A scam-free vacation*. Federal trade commission.
10. Ilchenko, O. V., Chumak, V. V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. V. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects.
11. Jun, M., & Cai, S. (2001). The key determinants of internet banking service quality: a content analysis. *International journal of bank marketing*.
12. Pater, P. (2020). *How does credit card skimming work?*. Science ABC.
13. Tressler, C. (2018). *Watch out for card skimming at the gas pump*. Federal trade commission.
14. The Islamic Republic News Agency. (1398).
15. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*.
16. Zoroja, J., & Pejić Bach, M. (2016). Impact of information and communication technology to the competitiveness of European countries-cluster analysis approach.