

БАНК ТИЗИМИДА СОДИР ЭТИЛГАН ФИРИБГАРЛИКНИ ТЕХНИК УСУЛЛАРИНИНГ ТАҲЛИЛИ

Юлдашева Нафиса Салимовна

Тошкент Ахборот Технологиялари Университети

e-mail : yuldashevanafisaxon16@gmail.com

Холимтаева Иқбол Убайдуллаевна

Тошкент Ахборот Технологиялари Университети

e-mail: iqbola.ubaydullayevna@gmail.com

АННОТАЦИЯ

Мақолада ахборот хавфсизлигининг глобал муаммолари, масалан, онлайн-дўконларнинг мисоллари ёрдамида Internet орқали фирибгарлик ва бошқалар ҳақида сўз боради. Замонавий ахборот ҳамжамиятининг энг заиф қисмига айланган фирибгарлик турлари ва хусусиятлари санаб ўтилган. Кўриб чиқилиши керак бўлган энг муҳим масалалар банк карталаридаги молиявий ресурсларни ҳимоя қилиш ва электрон пул соҳасидаги кибержиноятчиликка қарши курашдир.

Калит сўзлар: СМС-огоҳлантиришлар, *skimming*, Ливан сиртмоғи, биометрия, траппинг.

ABSTRACT

The article will talk about global problems of information security, for example, fraud via the Internet using examples of online stores, etc. Listed are the types and features of fraud that have become the most vulnerable part of the modern information community. The most important issues to consider are the protection of financial resources on bank cards and the fight against cybercrime in the field of electronic money.

Key words: SMS alerts, *skimming*, Lebanese correspondence, biometrics, trapping.

Ахборот хавфсизлиги нафақат технология ва ахборот соҳасида, балки молиявий воситаларни ва инсон маблағларини ҳар қандай тажовуздан ҳимоялашда муҳим ўрин тутди. Компьютер тизимларининг ривожини, хизматларга ҳақ тўлаш ва маблағ ўтказиш билан боғлиқ имкониятлар ҳар бир инсон ҳаётида ва иқтисодиётнинг молия соҳасида самарали натижани намоён этади. Электрон тўлов тизими, интернет-дўконлар, маблағ воситалари билан

масофавий муомила, онлайн-банкинг ва онлайн-савдо каби имкониятларнинг пайдо бўлиши нафақат қулайликни, балки фирибгарлик деб аталувчи муаммони ҳам туғдиради.

Интернет тармоғи орқали (масалан, “Интернет-дўконлар”лар), мобил қурилмалар ёрдамида электрон фирибгарлик, молиявий амаллар учун иловалар ва ҳ кенг тарқалган.

Электрон-тўлов тизими соҳасида ахборот технологияларининг ривожини аҳоли ҳаётини енгиллаштиради. Яъни, аҳоли нақд пул ўрнига пластик карточкалардан фойдаланади. Шу сабабли, кредит ва дебет карточкаларга эҳтиёж борган сари ортиб бормоқда. Бу эса барча молиявий жараёнларнинг соддалашишига олиб келади [1].

Қуйида банк карточкалари билан боғлиқ, кенг тарқалган фирибгарлик турлари келтирилган.

Скимминг. Ушбу фирибгарлик, “Оқ карточкалар” ёки “клон-карточкалар” деб ҳам аталади. Скимминг (кичик накладка) терминалга ёки магнит ҳошияни ўқиш учун банкоматга ўрнатилади. Накладка мижоз банк карточкаси лентасидан ахборотни кўчиради. Жиноятчи карточкадан олинган ахборот нусҳасини, “клон”ни яратади. Пин-кодни билиш учун рақамлар комбинациясини хотираловчи маҳсус накладка ёки камера ўрнатилади. Аммо, чипли банк карточкалари пайдо бўлиши билан ушбу ўғирлаш усули жуда кам учрайди, чунки маълумотларни ўғирлаш жараёнини амалга ошириш мураккаблашади.

Ливан сиртмоғи. Ушбу усулнинг сири ўзига ҳос блокиатор (оддий фотоплёнка асосидаги) ўрнатиш билан боғлиқ. У банкомат картридерига ўрнатилади ва карточкаларнинг эгасига қайтарилишига тўсқинлик қилади. Карточкани ўғирлаш схемаси қуйидагича: пул маблағини олиш учун карточка эгаси карточкани картридерга киритади ва, табиийки, бефойда. Чунки, карточкадаги магнит ҳошияси ахборотни ўқувчи қурилма билан уланмайди. Ўрнатилган “ливан сиртмоғи” туфайли карточка эгаси карточкасини қўлга киритаолмайди. Инсон ўйлайдики, банкомат тизимида янгиланиш содир бўлди ва ҳаяжонлана бошлайди, саросимага тушади. Шу вақтда қўшни банкомат олдидаги “яхши одам” келиб, у билан ҳам шундай вазият содир бўлганлигини айтади. У карточкани қайтариш учун яна бир марта пин-кодни теришга, сўнгра “кириш” тугмачасини босишга маслаҳат беради. Табиийки, натижа бўлмайди ва “яхши одам” карточкани қайтариш учун банкга мурожаат аризасини ёзишни таклиф этади. Карточка эгаси аффект ҳолида кетиши биланоқ фирибгар карточкани олади ва унинг олдида терилган пин-код туфайли маблағни олади. Фирибгарлик етарлича самарали ва оддий.

Траппинг. “ливан сиртмоғи”га ўқшаш, аммо шаттер банкоматдан карточкани эмас, балки маблағни чиқармайди. Карточка эгаси ҳодисани аниқлаш учун кетади, шу вақтда фирибгар ўзининг ноқонуний амалини бажаради.

Контактсиз ўғирлаш. Ҳозирда товар ёки хизмат учун тўловни амалга ошириш учун карточкани ҳамёндан чиқариш зарурияти йўқ, чунки VISA (PayWave), Mastercard(PayPass), Humopay ёки Uzcard (NFC) тўлов тизимларида нақд пулсиз тўловнинг соддалигини ва тезлигини таъминлаш мақсадида контактсиз тўлов усули яратилган. Ушбу тўлов тизимлари чипли ва магнит ҳошияли карточкаларда ишлайди. Бундай карточка билан ишлаганда, агар амал миқдори 50 минг сўмдан ошмаса, пин-кодни киритиш зарурияти йўқ. Фирибгар буни билган ҳолда, ўзининг найрангини одамлар тўпланган жойларда амалга оширади. У кийим чўнтақларига ва баданнинг бошқа қисмларига терминални ёки контактсиз ўқиш воситаларини билдирмасдан теккизади, шу онда ҳеч нарсадан шубҳаланмаган қурбоннинг банк карточкасида маблағ кўчирилади [2].

Фирибгарлар доимо одамларнинг карточкаларидан маблағ ўғирлашнинг янги усулларини ўйлаб топадилар. Банкларнинг техник ва инновацион ривожига параллель ҳолда фирибгарлик ҳусусидаги мурожаатлар сони ортиб бормоқда. Шундай вазиятлар бўладики, хатто юқори малакали мутахассислар ҳам қурбон аҳволига тушиб қолишлари мумкин.

Фирибгарлар етарлича яхши психологдир. Банк мижозларни фирибгарлардан ҳимоялаш имконига эга эмас. Аксарият ҳолларда банк карточкасидаги маблағни ҳавфсиз сақлаш карточка эгасига боғлиқдир.

Банк технологияларининг дунё миқёсидаги ривожига кредит ташкилотларининг нафақат шаклланган молия технологияларидан фойдаланишлари, балки банк мижозларини идентификациялашнинг янги усулларини жорий этишга ва нияти бузуқлардан ҳимоялашга мажбур этади.

Қуйида шундай усуллардан баъзилари келтирилган.

Биометрик ҳимояли карточка. Ушбу усулга биноан карточка эгаларининг бармоқ изларини аниқлаш технологияси билан жиҳозлаш таклиф этилади. Банк амалларини бажариш учун карточкадаги махсус ажратилган қисмига бармоқни теккизиш лозим. Бу ҳаракат ПИН-кодни киритиш ўрнига ўтади.

Дисплейли карточка. Карточкаларнинг бу тури янги технологияли янги авлод карточкалари ҳисобланади. Бунда Интернетда амалларни ҳавфсиз бажариш учун бир мартали пароллардан фойдаланилади. Карточкада, чип ва магнит ҳошияси билан бир қаторда, микродисплей ва сенсорли клавиатура

жойлашган. Шу тўфайли, карточка эгаси, амалларни онлайн режимда бажарганида, ўзининг бир мартали паролини генерациялаши мумкин.

Хавфсизлик коди ўзгарувчан карточкалар. Интернет-магазинларда харид қилинганида, харидни тасдиқлаш учун карточканинг тескари томонидаги уч ҳонали код киритиш лозим. Янги карточкаларда маълум вақтдан сўнг ўзгарувчи уч ҳонали кодни махсус дисплейни жорий этиш таклиф қилинади.

Қуйида карточкаларни нияти бузуқлардан асрашдаги хавфсизликнинг стандарт қоидалари келтирилган:

- карточкаларни назоратсиз қолдириш ва шубҳаи шахсларга бериш мумкин эмас;

- банк карточкаси маълумотларини, унинг реквизитларини, логинларини, шахсий кабинет паролини ва ҳ. ҳеч кимга маълум қилиш мумкин эмас;

- Банк карточкаси ПИН-кодини ёдда сақлаш, уни бошқа одамлар кўз ўнгида қолдирмаслик ва банк карточкасининг ўзида ёзмаслик лозим. Банкоматда ва бошқа жойларда амаллар бажаришда ПИН-кодни, хатто банк ходими ҳузурида, овоз чиқариб ўқиш керак эмас;

- товар ёки хизмат учун нақд пулсиз ҳисоб бўйича амаллар бажарилишида барча жараёнларда мижоз иштирок этиши шарт;

- ҳисоблашларда карточкани қўлдан чиқармаслик лозим. Интернетдаги харид тўлови учун алоҳида ҳамён ёки шундай амаллар учун алоҳида карточка бўлиши керак;

- шубҳали ва унчалик таниш бўлмаган ресурсларда онлайн-харидлар қилмаслик лозим;

- икки марта бир хил миқдорли амал ўтганида банкга мурожаат қилиш лозим;

- карточка йўқолганида ёки ўғирланганида, карточкани блокировкалаш илтимоси билан дарҳол банкга мурожаат этиш лозим. Бу билан пул маблағининг ҳисобдан чиқариш эҳтимоллигини пасайтиришга эришиш мумкин [3].

Фойдаланилган адабиётлар рўйхати: (REFERENCES)

- 1. Александров, П. О. Противодействие кибермошенничеству: разработка платформы обнаружения, мониторинга и блокировки фишинговых интернет-ресурсов / П. О. Александров, Л. К. Орлик // Современные тенденции развития науки и образования: теория и практика: сборник материалов 3-й международной научно-практической конференции (Москва, 20 июня 2019 года). – Москва: ВИПО, 2019. – С. 13- 21.

-2. Асаул В. В., Михайлова А. О. Обеспечение информационной безопасности в условиях формирования цифровой экономики // Теория и практика сервиса: экономика, социальная сфера, технологии. – 2018. – №4 (38). – С. 5–9.

-3. Бугаев Д. П. Определение готовности национальной платежной системы в обеспечении безопасности с учетом мировых тенденций // Инновации и инвестиции. – 2021. – №1. – С. 80-84