Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Алфёрова А.Г., Иванова Я.С. Мошенничество с банковскими картами и способы безопасности // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2023. – №3 (март). – АРТ 12-эл. – 0,3 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННОСТИ

Алфёрова Алёна Геннадьевна,
студентка 2 курса, экономического колледжа
ГБПОУ «Южно-Уральский государственный колледж»,
38.02.07. Банковское дело
Иванова Яна Сергеевна,
студентка 2 курса, экономического колледжа
ГБПОУ «Южно-Уральский государственный колледж»,
38.02.07. Банковское дело
Научный руководитель: **Пылина Ирина Викторовна**,
председатель ПЦК Финансовых дисциплин
ГБПОУ «Южно-Уральский государственный колледж»
г. Челябинск, Российская Федерация
e-mail: pylinairina@mail.ru

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ И СПОСОБЫ БЕЗОПАСНОСТИ

Аннотация: Платежи с использованием банковских карт стали привычным делом для большинства населения России. Банковская карта является, чуть ли не универсальным средством в финансовом мире – на нее перечисляют заработную плату, выдают кредиты, ею рассчитываются в точках продаж и интернете. Одновременно растет и число преступлений, связанных с хищениями денежных средств. В статье рассмотрены основные виды мошенничества с банковскими картами

Ключевые слова: Банковская карта; банкомат; терминал; мошенничество; скиммер; фишинг; мобильный банк.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Alferova Alyona Gennadievna,
student 2 course of the College Economics
GBPOU "South Ural State College",
38.02.07. Banking
Ivanova Yana Sergeevna,
student 2 course of the College Economics
GBPOU "South Ural State College",
38.02.07. Banking
Scientific supervisor: **Pylina Irina Viktorovna**,
Chairman of the PCC of Financial Disciplines
GBPOU "South Ural State College"
Chelyabinsk, Russian Federation

BANK CARD FRAUD AND SECURITY METHODS

Abstract: Payments using bank cards have become commonplace for the majority of the Russian population. A bank card is almost a universal tool in the financial world – wages are transferred to it, loans are issued, it is calculated at points of sale and the Internet. At the same time, the number of crimes related to embezzlement of funds is also growing. The article discusses the main types of fraud with bank card

Keywords: Bank card; ATM; terminal; fraud; skimmer; phishing; mobile banking.

Несмотря на то, что банки уверяют своих клиентов в надёжности и безопасности использования пластиковых карт, мошенники находят новые способы незаконного списания средств. По данным ЦБ РФ в 2022 году объем операций без согласия клиентов увеличился по сравнению с 2021 годом на 4,29% на фоне активного развития новых дистанционных платежных сервисов

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

и роста объема денежных переводов (+39%, до 1458,6 трлн руб.) с применением электронных средств платежа (платежные карты и иные электронные средства платежа) [1].

Рассмотрим распространённые схемы мошенничества с банковскими картами, зная которые, можно предотвратить хищение средств со своего счёта.

Обмануть или взломать банковскую систему безопасности достаточно сложно, поэтому преступники стараются любыми способами выманить информацию о карте у самого держателя. Для достижения своей цели они используют все доступные ресурсы — телефон, интернет-сайты, онлайн-банк, мобильный банк и прочие каналы.

Мошенничество по телефону имеет множество вариаций, которые объединяет то, что владельцу карты звонят с незнакомого номера и под любым предлогом просят сообщить её реквизиты. В большинстве случаев злоумышленники используют следующие схемы [2]:

- Выигрыш в лотерею. Преступник представляется менеджером известной компании и сообщает, что клиент стал победителем розыгрыша. Для получения вознаграждения необходимо срочно выслать реквизиты своей банковской карты.
- Звонок из службы безопасности банка. Фальшивый «сотрудник» извещает клиента о том, что его карту пытались взломать и просит уточнить данные для исправления ситуации. Телефонные мошенники всегда говорят уверенно, имеют хорошо поставленный голос, а на любой вопрос клиента имеют заранее подготовленный ответ.

Схема мошенничества через СМС имеет много общего с предыдущим способом. Разница заключается в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера, но мошенники подписываются известной компанией. Распространённый пример

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

подобных фейковых сообщений: «Ваша карта заблокирована. Перезвоните по номеру +7926XXXXXXX. Ваш Сбербанк». Если клиент не реагирует, то преступники могут прислать повторное СМС с угрозой взыскания штрафа или комиссии. Перезвонившего просят сообщить данные карты, провести манипуляции в банкомате или интернет-банке.

Сегодня каждый банк при выдаче карты рекомендует подключить мобильный банк, с которым можно просто и удобно управлять своими средствами при помощи СМС-команд. Мошенники могут получить доступ к номеру, к которому привязан мобильный банк в случаях, когда:

- Телефон был утерян владельцем. До момента блокировки SIM-карты любой человек может списать деньги с карточки с помощью СМС-команд, перечень которых размещён на сайте любого банка.
- Клиент отказался от услуг конкретного сотового оператора и не отключил мобильный банк. В этом случае номер телефона попадёт в руки нового абонента, который может оказаться мошенником и списывать деньги посредством СМС-команд. Благодаря использованию мобильного банка злоумышленник также легко вычислит, в какой организации владелец телефона открыл карту.

Преступники не всегда преследуют цель узнать реквизиты карты. Самый простой способ незаконного обогащения — это убедить клиента в том, что он должен перевести деньги самостоятельно. Злоумышленники предлагают приобрести товары по выгодной цене и требуют перечисления аванса или всей суммы. Некоторые мошенники выступают в роли фиктивных компаний, которые предлагают удалённую работу в интернете с хорошим заработком. Соискателю необходимо лишь подтвердить серьёзность своих намерений и перевести определённую сумму на счёт или карту работодателя.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Распространённой схемой аферистов также является «помощь родным». Данный способ чаще всего применяется в отношении пожилых людей, которым звонят и сообщают о том, что их близкие попали в беду. Мошенники представляются сотрудниками правоохранительных органов или медицинскими работниками. Они настоятельно требуют перевести деньги, угрожая необратимыми последствиями для жизни и здоровья близких.

Преступники придумывают все новые способы обойти системы безопасности банков, используя в целях мошенничества даже банкоматы. По данным ЦБ РФ, в России установлено более 200 тысяч банкоматов, которые позволяют проводить различные операции с банковской картой [3]. Аферисты применяют всевозможные методы кражи средств с карты, например скимминг и трапинг [4].

В первом случае на банкомат устанавливается специальное оборудование, которое представляет собой накладку на клавиатуру и скиммер (вставляется в картоприёмник и позволяет считать данные магнитной полосы). С помощью полученных сведений мошенники изготавливают дубликат карточки и снимают с неё все средства.

Во втором – преступники вставляют в картридер кусок пластика с прорезью в центре. Клиент вводит карточку в банкомат, она попадает в прорезь и остаётся в устройстве. После этого подходит злоумышленник, якобы тоже побывавший в такой ситуации, и советует ввести ПИН-код. Когда это не помогает, клиент уходит, а преступник извлекает карточку с помощью заранее подготовленных инструментов. Мошенники, объединённые в организованные преступные группы, действуют более масштабно и создают целые поддельные банкоматы.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Постепенная информатизация мира привела к появлению мошенников в интернете [5]. В частности, на торговых площадках, таких, как Авито [6].

Данная процедура проводится следующим образом:

- Мошенник звонит автору объявления о продаже чего-либо и представляется заинтересованным покупателем.
- Продавец сообщает злоумышленнику номер своей карты для перевода средств в счёт оплаты товара.
- Фиктивный покупатель входит в интернет-банк по номеру карточки и списывает деньги со всех счетов. Для доступа требуется одноразовый СМС-пароль, который мошенник с помощью различных уловок выманивает у продавца. Последний этап может отличаться в зависимости от цели преступника. Некоторые хотят узнать конфиденциальные реквизиты карты, другие — просят провести определённые манипуляции через банкомат якобы для подтверждения платежа. В банкомате клиент под руководством мошенника подключает к своей карте посторонний номер телефона, после чего злоумышленник получает доступ к личному кабинету и мобильному банку.

Суть фишинга (с анг. «рыбная ловля, выуживание») заключается в том, что аферисты создают поддельный сайт популярного интернет-магазина или онлайн-банка, который внешне похож на оригинал, а его URL-адрес отличается от подлинного одним символом. Для оплаты покупки или входа в систему пользователь вводит на фиктивной странице конфиденциальные данные, которые попадают в руки злоумышленников. Ссылки на фишинговый сайт под видом акций и спецпредложений мошенники отправляют клиентам на электронную почту, в онлайн-мессенджеры или социальные сети.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Не все преступники используют изощренные способы мошенничества, некоторые предпочитают просто украсть карточку. Одни злоумышленники делают это открыто, угрожая жизни и здоровью владельца, другие — дежурят возле банкоматов и забирают потерянные карты. В большинстве случаев устройство возвращает пластик с задержкой. Клиент не дожидается и уходит или, получив наличные, вовсе забывает о карте. После этого мошенник может беспрепятственно её забрать и использовать в своих целях.

Помимо описанного выше, третьи лица воруют деньги с карт при помощи вирусного программного обеспечения. Вредоносная программа под видом полезного приложения устанавливается на компьютер, планшет или смартфон клиента. Её основное предназначение — украсть данные карты или перенаправить пользователя на фишинговый сайт.

Другой популярный вид мошенничества — сговор с сотрудниками банка или предприятий торговли [7]. Кассир может зафиксировать данные карты (например, провести её через скиммер) и передать их посторонним лицам.

Как мошенники снимают деньги с банковской карты? Способ незаконного вывода средств с карты зависит от того, какой информацией завладел злоумышленник. Основные варианты получения выгоды следующие:

•Если карта считана через скиммер, то жулики изготавливают её дубликат.

ПИН-код вычисляется благодаря использованию накладки на банкомат или скрытой камеры на устройстве.

•Зная только номер карточки, преступники проводят процедуру

регистрации в онлайн-банке. Остаётся только обманным путём узнать у владельца одноразовый пароль. После входа в систему аферисты переводят на свои счета средства не только с карт, но и со всех вкладов клиента.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

•Если мошенник знает реквизиты карты (номер, срок действия и код безопасности), то её можно использовать для оплаты в интернет-магазинах, которые не требуют СМС-подтверждения

Одним из способов списания средств также выступает опция «Мобильный банк».

В связи с развитием новых технологий меняются и виды краж с банковских карт. В 2023 году с фактами мошенничества всё чаще сталкиваются владельцы пластика с опцией бесконтактных платежей. Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено. Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам. Также в текущем году злоумышленники продолжают активно использовать фишинг в социальных сетях и онлайн-мессенджерах. Наибольшую выгоду мошенникам приносят махинации через Авито, с помощью которых они получают доступ в онлайн-банк [8].

Куда же обращаться в случае хищения средств?

После выявления факта незаконного списания денег с карты необходимо срочно её заблокировать и обратиться в ближайшее отделение банка-эмитента. Дальнейшая процедура включает следующие этапы:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- Клиент пишет заявление о несогласии с конкретной расходной операцией.
- Банк проводит служебное расследование по факту хищения средств.
- В установленные сроки (до 30 дней) владелец карточки уведомляется о решении.

Банк может вернуть деньги только в том случае, если пользователь не нарушал правила безопасности, то есть добровольно не сообщал конфиденциальную информацию третьим лицам. Независимо от решения эмитента, владелец карточки имеет право обратиться в правоохранительные органы и написать заявление о краже денег.

Предупреждён — значит вооружён. Чтобы не стать жертвой мошенников, необходимо придерживаться следующих рекомендаций [9]:

- не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код);
- подключить услугу СМС-уведомлений для контроля за счётом;
- ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;
- установить расходные лимиты в интернет-банке или мобильном приложении;
- никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);
- немедленно блокировать карту в случае утраты, кражи или захвата её банкоматом, а также при утере телефона с привязанным номером.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Ежедневно злоумышленники изобретают новые способы хищения средств с банковских карт, поэтому невозможно предугадать все сценарии развития событий. Однако при соблюдении указанных элементарных мер безопасности любой пользователь сможет предотвратить нанесение ущерба от действий мошенников [10].

Список использованной литературы:

1. Официальный сайт Центрального Банка Российской Федерации – [Электронный ресурс] – Режим доступа: https://cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения 20.03.2023).
2. Галанов В. А. Финансовая грамотность, финансовая вера и финансовое мошенничество / В. А. Галанов, А. В. Галанова // Вестник Российского экономического университета имени Г. В. Плеханова. - 2022. - Т. 17, № 3. - С. 157-165.
3. Сайт Banki. ru – [Электронный ресурс] – Режим доступа: https://www.banki.ru/info/about/news/?id=9992130 (дата обращения 20.03.2023).
4. Банковское дело. Интернет журнал – [Электронный ресурс] – Режим доступа: https://prpr.su/stati/kraja-s-bankovskoi-karty-rasprostranennye sposoby/ (дата обращения 20.03.2023).
5. Басова М. Е. Финансовое мошенничество / М. Е. Басова // Право и экономика. - 2022. - № 2. - С. 72-76.
6. Сайт ЮрСовет – [Электронный ресурс] – Режим доступа: http://juresovet.ru/moshennichestvo-na-avito (дата обращения 20.03.2023).
7. Жилякова Е. Финансовые и налоговые потери из-за мошенничества в отделе продаж / Е. Жилякова // Финансовый директор. - 2022. - № 5. - С. 60-67.
8. Сайт Сравни – подробно и сравнение кредитных карт, вкладов, кредитов – [Электронный ресурс] – Режим доступа: https://www.sravni.ru/text/5-populjarnykh-sposobov-moshennichestva-na-avito/ (дата обращения 20.03.2023).
9. Официальный сайт Банка России – [Электронный ресурс] – Режим доступа: https://cbr.ru/information_security/pmp/ (дата обращения 20.03.2023).
10. Кредитная история – [Электронный ресурс] – Режим доступа: https://kredit-on.ru/cb-predupredil-o-distancionnom-sposobe-hisenia-deneg-s-bankovskih-kart/ (дата обращения 20.03.2023).

Дата поступления в редакцию: 23.03.2023 г.
Опубликовано: 31.03.2023 г.