Райффайзен БАНК

kaspersky

Тренды карточного фрода 2019:

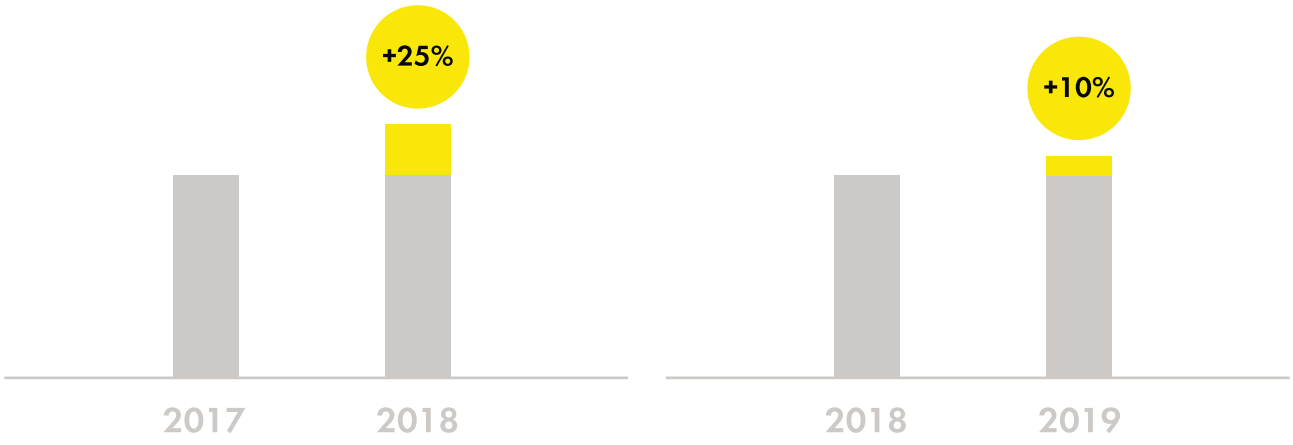
год социальной инженерии

Райффайзенбанк и «Лаборатория Касперского» проанализировали ключевые тренды мошенничества с банковскими картами в 2019 году. Выводы основаны на данных системы мониторинга карточных транзакций Райффайзенбанка, фрод-аналитиков «Лаборатории Касперского», а также данных ФинЦЕРТ Банка России.

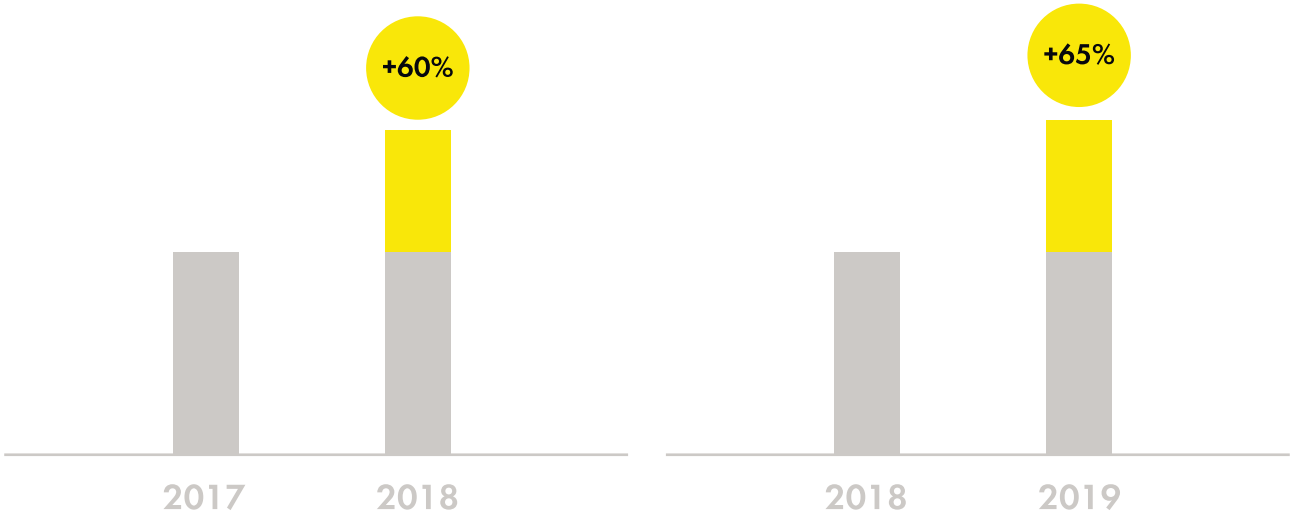
Несанкционированные CNP[1]-транзакции: смена вектора

Несанкционированные онлайн-операции с использованием данных банковских карт клиентов на протяжении последних четырех лет стали значительным вызовом для финансовой отрасли. Основные причины — рост карточных транзакций, развитие дистанционных платежных сервисов, рост количества e-commerce-площадок в покупательской активности клиентов. Согласно «Обзору несанкционированных переводов денежных средств за 2018 год» ФинЦЕРТ Банка России, количество несанкционированных CNP-транзакций (без предъявления карты) в 2018 году выросло на 48,3%. ФинЦЕРТ отмечает, что доступность платежных услуг через интернет смещает интерес мошенников от банкоматов и торговых точек в сторону CNP-транзакций и дистанционного банковского обслуживания (ДБО). Регулятор прогнозирует сохранение восходящего тренда миграции несанкционированных операций в CNP-среду.

В 2019 году, по данным Райффайзенбанка, темпы роста несанкционированных CNP-транзакций замедляются. Несмотря на все еще большую долю в общем объеме мошеннических операций по отрасли, крупные банки научились их выявлять и предотвращать.



Динамика несанкционированных CNP-транзакций в Райффайзенбанке, 2017 – 2019 гг



Динамика блокировки несанкционированных CNP-транзакций в Райффайзенбанке, 2017 – 2019 гг

[1]Card not present

«При CNP-транзакциях атакующим важно действовать очень быстро. Если злоумышленнику удалось выманить необходимую информацию у жертвы с помощью социальной инженерии, он постарается вывести средства до того, как пользователь начнет в чем-то сомневаться и свяжется с банком», — подчеркивает Максим Федюшкин, менеджер по развитию бизнеса Kaspersky Fraud Prevention.

Примеры атак:

Кража учётной записи от интернет-банка.
Это самый опасный вариант для клиента финансовой организации. При получении доступа к личному кабинету и средствам подтверждения транзакций (коды в СМС или push-уведомлениях) злоумышленник может не только перевести средства со счетов клиента, но и попытаться воспользоваться предодобренными кредитами.

Обладая номером карты, получить доступ к учетной записи в интернет-банке атакующий может, только узнав код подтверждения, который придет на телефон владельцу аккаунта. Чаще всего выманить его злоумышленники пытаются с помощью социальной инженерии (для идентификации запрашивают номер карты, далее просят сообщить код, чтобы «отменить» мошеннический платеж и «сохранить» деньги или перевести их на «безопасный счет»; предлагают принять участие в акции, и просят подтвердить таким образом свою личность; и т.д.).

Привязка данных карты к магазину приложений или системе электронных платежей.
Зная номер банковской карты и один раз выведав у жертвы код подтверждения, злоумышленники могут привязать ее к магазину приложений и расплачиваться за покупки с помощью своего мобильного устройства. Также подход может использоваться для встроенных покупок в играх: артефакты или донаты оплачиваются с чужой карты, а потом перепродаются другим игрокам. Существуют примеры, когда злоумышленники создают приложение с высокой стоимостью (более 100 долларов), сами покупают его, оплатив чужой картой, после чего получают деньги от владельцев магазина приложений.

Оплата картой в онлайн-магазинах.
Иногда пользователи выкладывают в социальных сетях фото банковской карты, собственной или, например, найденной, чтобы вернуть владельцу.

Прогнозы на 2020 год

«Мы ожидаем, что в 2020 году мошенничества с CNP-транзакциями продолжат доминировать в масштабах рынка, однако многие банки будут блокировать большую часть таких транзакций, поэтому интерес мошенников, вероятно, сместится в сторону менее защищенных игроков рынка и e-commerce платформ», — говорит Виктория Александрова, руководитель операционного отдела банковских карт и эквайринга Райффайзенбанка.

Рекомендации по предотвращению мошенничества

Несколько простых правил помогут вам обезопасить свои средства от мошенников:

1. Заведите отдельную карту для покупок онлайн; если для покупок используется кредитная карта, лучше оформить карту с небольшим кредитным лимитом.
2. Заведите расчетный счет и храните основную часть средств на нем, а на счете, к которому выпущена карта, которой вы пользуетесь ежедневно, держите сумму, необходимую для расходов на несколько дней. В мобильном банке перевод между своими счетами занимает от нескольких секунд до нескольких минут.
3. Перед покупкой сделайте хотя бы минимальную проверку интернет-магазина — изучите сайт, почитайте отзывы клиентов и т.д. Проверьте, как осуществляется доставка из интернет-магазина, ее сроки, есть ли пункт самовывоза товаров.
4. Подключите оповещения или регулярно просматривайте транзакции по карте в интернет-приложении банка. Это снизит риск того, что сумма будет списана незаметно, так как зачастую мошенники проверяют правильность карточных данных, совершая транзакции на небольшие суммы. Это также поможет предотвратить дальнейшие списания при своевременной блокировке карты.
5. Никому не отдавайте свою карту. Помните, что для оплаты счета в ресторане официант не должен забирать вашу карту.
6. Для Android-устройств установите антивирусное ПО.
7. Для мобильных устройств установите приложение для определения номера. Такое ПО информирует о названии организации и категории звонка: «займы», «служба доставки» и т.д., а также уведомляет, были ли жалобы на спам с этого номера.

Социальная инженерия: от вспышки к эпидемии

В 2019 году российский банковский рынок столкнулся с эпидемией социальной инженерии. Причинами стали относительная легкость и масштабируемость сценариев атаки, а также утечки данных. По данным отчета ФинЦЕРТ, в 2018 году 97% всех несанкционированных переводов с платежных карт было совершено путем мошенничества методами социальной инженерии, а также из-за нарушения клиентом правил использования электронного средства платежа. Для борьбы с эпидемией ФинЦЕРТ считает необходимым повышать киберграмотность населения.

По данным Райффайзенбанка

более 70%

мошеннических действий в отношении частных лиц в 2019 году были спровоцированы социнженерией.

«Всплеск социальной инженерии в 2019 году заставил многих пользователей запомнить, что нельзя сообщать по телефону коды подтверждения и CVV, поэтому злоумышленники придумывают новые способы получения необходимой информации, — комментирует Максим Федюшкин, менеджер по развитию бизнеса Kaspersky Fraud Prevention. — Теперь звонящий может сообщать, что пользователь не должен называть сотрудникам банка пароль, который придет в СМС, поэтому необходимо ввести его в тональном режиме. Однако этого будет достаточно, чтобы злоумышленники смогли вывести средства со счета или завладеть данными учетной записи».

Примеры мошенничества

Звонок клиенту банка.

Обычно звонящий представляется сотрудником авторитетной организации (банка, ЦБ, пенсионного фонда и т.д.) и объясняет, что хочет предотвратить неприятное событие (подозрительную транзакцию, попытку нелегитимного до-

ступа к счету). Злоумышленник чаще всего говорит быстро, делает все возможное, чтобы человек не повесил трубку, требует от пользователя максимально быстро выполнять полученные команды. Часто используются технологии для подмены телефонного номера, так на экране телефона может высвечиваться телефон банка или очень похожий номер. После этого можно привести пример нескольких сценариев:

1. Пользователя просят назвать приблизительный остаток средств на счету и одноразовый пароль или сообщить их другим образом (например, ввести в тональном режиме). Узнав необходимую информацию, злоумышленники могут вывести средства со счета или завладеть данными учетной записи.
2. Злоумышленник сообщает о предотвращении подозрительной операции, ничего не просит сообщать, но настоятельно рекомендует установить защиту на своё устройство. Для этого предлагают скачать программу по ссылке, которая придет в СМС, и установить ее на телефон. Если пользователь выполнит эти «рекомендации», то на его телефон будет скачана программа для удаленного доступа к устройству или вредоносное ПО (например, шифровальщик с требованием выкупа за расшифровку или банковский троянец). Другой сценарий — пользователя просят зайти в магазин приложений и скачать определенное ПО, которое можно найти по запросу «удаленная помощь», скорее всего, это будет также программа для удаленного управления устройством.
3. Злоумышленник просит установить программу из магазина приложений (Google Play Market или AppStore), введя в поиск слово «поддержка» или близкие смысловые аналоги. В топе результатов поиска будут легитимные приложения для удаленного подключения с оценками и количеством установок, что играет на руку злоумышленникам, так как это вызывает у пользователей позитивный отклик. После установки мошенник просит запустить банковское приложение и перевернуть телефон экраном вниз, так как будет осуществлен перевод на «безопасный счет». В это время злоумышленник переводит деньги на подконтрольные счета.

СМС-клиенту банка.

Сообщение будет содержать информацию, побуждающую клиента перезвонить по указанному номеру. Например, «Ваша карта заблокирована, для восстановления доступа позвонить в службу безопасности банка по телефону XXX XXXXXXX» или «Зафиксирована подозрительная транзакция по вашей карте, для отмены позвоните по тел. XXX XXXXXXX». Чтобы убедить пользователя, в тексте может содержаться имя и отчество пользователя, название банка, несколько цифр с номера карты. Позвонив, пользователь столкнется с одним из сценариев, описанных выше.

Прогнозы на 2020 год

«Противостоять социальной инженерии можно только с помощью масштабной информационной кампании, направленной на повышение кибер- и финансовой грамотности, — уверена Виктория Александрова, руководитель операционного отдела банковских карт и эквайринга Райффайзенбанка. — Мы ожидаем, что в течение 2020 года социальная инженерия останется основным вектором мошеннических атак, однако на горизонте трех лет совместные усилия регулятора, банковского сообщества и производителей решений по информационной безопасности должны повысить сопротивляемость сценариям, которые используют мошенники».

Рекомендации по предотвращению мошенничества

Для того, чтобы обезопасить себя и близких от уловок мошенников, можно придерживаться следующих правил:

1. Обращайте внимание на попытки психологического воздействия. Сотрудники банка никогда не будут оказывать на вас давление во время звонков, такое как нагнетание беспокойства, ощущения, что вас постоянно торопят и ждут немедленного решения;
2. Не сообщайте коды подтверждения операций по телефону и перезванивайте в банк самостоятельно при возникновении малейших подозрений. Если возможно, сделайте это с другого телефона;
3. Следуйте требованиям безопасности при использовании карт и ДБО (их можно найти на сайте банка);
4. Устанавливайте защитные решения проверенных производителей на собственных устройствах самостоятельно, не следуйте «рекомендациям» по телефону;
5. Всегда обращайтесь в банк и полицию при подозрении на мошенничество;
6. Установите ПИН-код на сим-карту телефона. В случае утери телефона мошенники не смогут перехватить СМС для подтверждения операций, совершенных за вас;
7. Если вы публикуете свои персональные данные (например, ФИО и номер телефона), будьте готовы к тому, что их смогут использовать мошенники, чтобы повысить ваше доверие к ним. Для разовых операций (продажа авто или товаров на торговых Интернет-площадках, получения услуг) используйте временный номер телефона.

Кража персональных данных и вымышленные личности

Мошенничества с использованием реальных персональных данных и выдуманных личностей — растущий тренд и на мировом, и на российском рынке. В США проблема synthetic identity fraud, в рамках которого мошенники создают поддельные личности с кредитной историей и потом получают кредиты, набирает обороты. Но в России этот сценарий пока не так актуален, однако использование персональных данных клиентов — реальность, с которой отрасли приходится иметь дело.

Основными причинами этого тренда стали утечки клиентских данных из разных источников, а также нехватка киберграмотности. Среди источников утечек в 2018 году ФинЦЕРТ выделяет несанкционированный доступ к данным сайтов, по продаже товаров и услуг, где пользователи оставляют платежную информацию, наблюдение за массовыми торговыми площадками, получение данных карт из переписки, а также продажу данных в Telegram-ботах.

«Кража или подделка цифровых личностей стала очень актуальной проблемой последних лет. Злоумышленники используют их для нелегитимного доступа к различным сервисам, кражи денег и обхода систем защиты. поэтому пользователям важно не только следить, где они оставляют данные, где они оставляют свои данные в цифровом мире, но и внимательно относиться к своим документам и оффлайн — не передавать их другим людям, не позволять уносить и делать копии без острой необходимости», — уточняет Максим Федюшкин, менеджер по развитию бизнеса Kaspersky Fraud Prevention.

Примеры атак

Сервисы такси:

в мессенджерах существуют каналы, где можно заказать такси с большой скидкой. Схема выглядит примерно так: пассажир отправляет сообщение в такой канал с указанием деталей поездки, а злоумышленник вызывает такси с помощью украденного аккаунта. Завершив поездку, водитель получает деньги от владельца украденного аккаунта, а пассажир переводит деньги напрямую злоумышленнику. Чтобы как можно дольше оставаться незамеченными, злоумышленники могут отслеживать владельца взломанного аккаунта в социальных сетях и организовывать такие поездки ночью, когда велика вероятность, что человек спит, или во время путешествий жертвы за границу.

Каршеринг:

подделанные или украденные личности, которые имеют доступ к сервисам каршеринга, пользуются большой популярностью по нескольким причинам. Если к украденному аккаунту привязана банковская карта, то злоумышленник может совершить поездку за чужой счет. Также в сервисах каршеринга действуют определенные ограничения на возраст или стаж вождения при аренде некоторых видов автомобилей, чтобы обойти их, используются украденные личности или аккаунты.

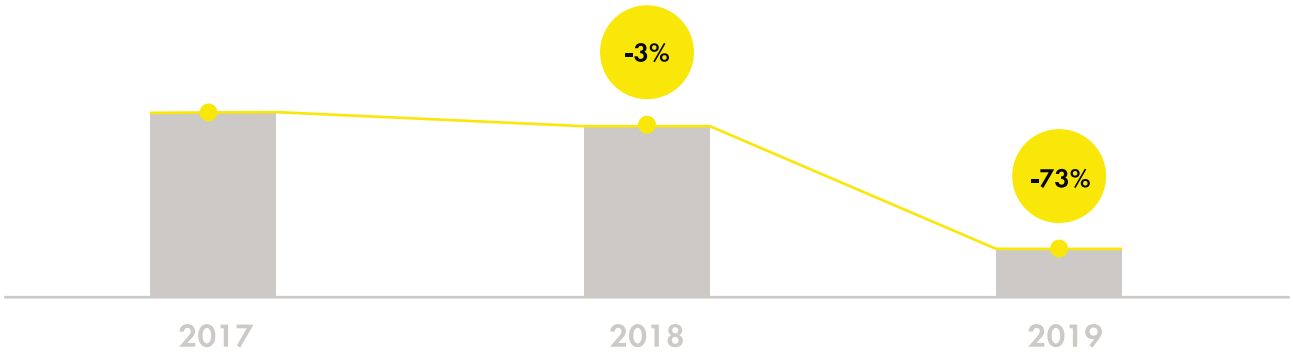
Рекомендации по предотвращению мошенничества

1. Не используйте одинаковые пароли для разных интернет-сервисов, особенно — для клиент-банка.
2. Используйте password-менеджеры, чтобы создавать надежные пароли, эффективно их хранить и своевременно менять.
3. Регулярно меняйте пароли.
4. Внимательно относитесь к своим документам (паспорту, правам, СНИЛС и т.д.), не сообщайте их номера без острой необходимости, сканы храните только на хорошо защищенных носителях информации.

Снижение объемов POS- и ATM-мошенничеств

Использование поддельных карт в ATM и торговых точках по итогам 2019 года стремительно сокращается. К этому приводят увеличение популярности безналичных операций без предъявления карты, в том числе с использованием электронных кошельков, упрощение сервисов переводов средств между частными лицами, переход на карты с микропроцессором (чипом) по всему миру и рост защищенности ATM & POS систем.

По данным Райффайзенбанка, объем мошенничеств с использованием поддельных карт в ATM и POS-терминалах неуклонно снижается.



Использование данных карт, скомпрометированных на POS и ATM

Прогнозы на 2020 год

«Мы ожидаем дальнейшего уменьшения активности мошенников в использовании карт, скомпрометированных в ATM и торговых точках, так как бесконтактные платежи получают все более широкое распространение по всему миру. При этом стандарты информационной безопасности розничных сетей повышаются», — прокомментировала Виктория Александрова, руководитель операционного отдела банковских карт и эквайринга Райффайзенбанка.

Рекомендации по предотвращению мошенничества:

1. Следуйте рекомендациям банка по безопасности при использовании банковских карт.
2. Не прибегайте к помощи незнакомых лиц при операциях с картами.
3. Перед тем, как вставить карту в банкомат, несколько раз нажмите кнопку «Отмена».
4. Внимательно осматривайте устройство перед вводом карты – любые подозрительные объекты могут оказаться скиммерами.
5. Прикрывайте рукой клавиатуру при вводе пин-кода.
6. Старайтесь снимать деньги в банкоматах, расположенных в отделениях банка и других охраняемых местах.
7. Не позволяйте уносить свою карту или при оплате сканировать ее магнитную полосу. Используйте карты с чипом.

Райффайзен БАНК