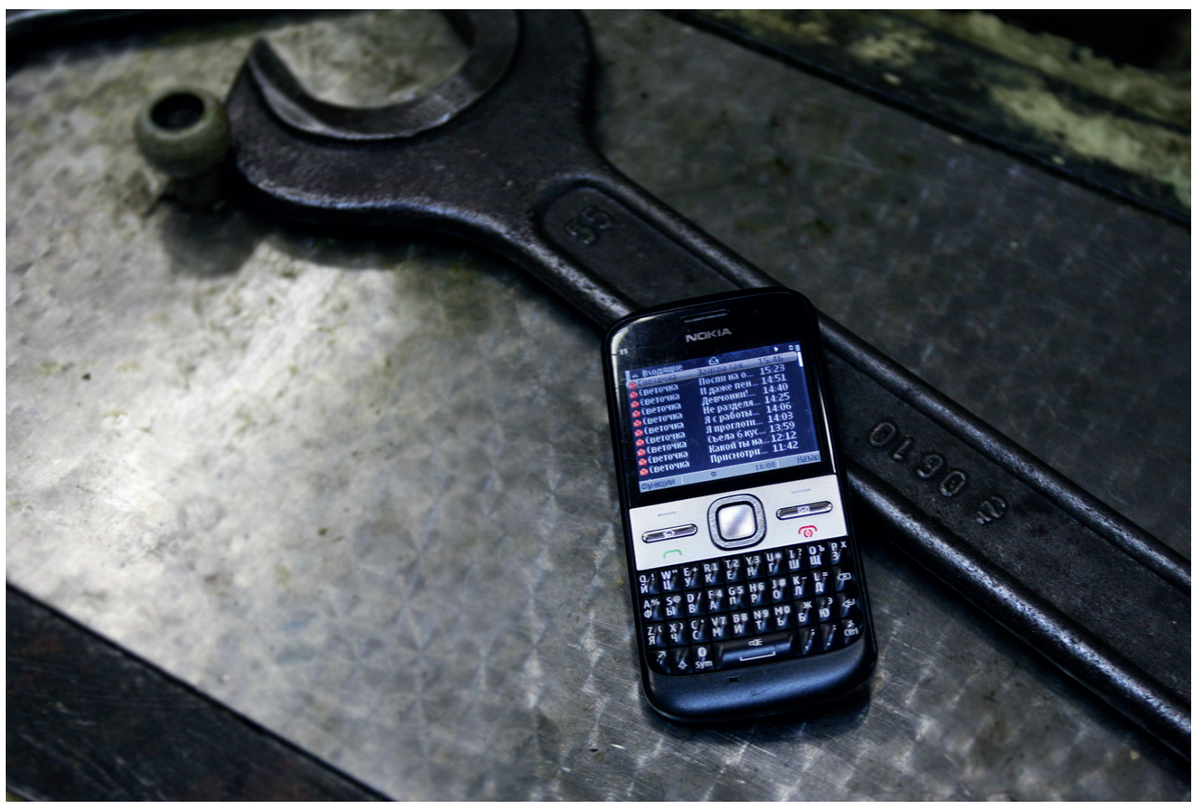
финансы

Причинная версия

технологии

Распространение мобильного интернета, новые мобильные технологии и мобильный банкинг не просто приводят к изменению пользовательских привычек, но уже становятся едва ли не основной причиной в изменениях на банковском рынке. Крупные банки, которые не сумеют адаптироваться к новым запросам потребителя на мобильность, рискуют проиграть новым или менее известным игрокам, которые предложат клиенту качественные, безопасные и удобные услуги мобильного банковского обслуживания.



Смартфоны стали удобными инструментами для мобильного банкинга ФОТО НИКОЛАЯ ЦЫГАНОВА

Согласно отчету британского телеком-регулятора Ofcom, объемы мобильного интернета ежегодно увеличиваются в мире в полтора-два раза. Также, по данным опроса, проведенного J`son & Partners Consulting, 42% российских пользователей мобильного интернета ежедневно выходят в сеть со своего смартфона, которым является почти каждый третий проданный в России телефон, а это более 27 млн мобильных устройств.

Мобильный банкинг позволяет узнать баланс всех счетов по всем картам и вкладам клиента, найти ближайшие банкоматы и отделения банков на карте, конвертировать валюту, оплачивать товары и услуги, совершать денежные переводы, удаленно открывать срочные вклады и даже использовать автоматические сервисы персонального финансового менеджмента. Мобильная операционная система Android позволяет использовать мобильные виджеты, с помощью которых можно отслеживать на экране смартфона информацию о счете в реальном времени.

Банковские платежные мобильные приложения также могут предоставлять клиенту информацию о товарах и услугах, способную повлиять на решение о покупке прямо в магазине.

Использование новых технологий передачи информации на короткие расстояния, таких как NFC, создает новые возможности для мобильных платежей, поддержка которых в будущем может стать обязательным требованием к банкам, особенно в клиентском сегменте до 35 лет. Исследование PwC показало, что только 5% пользователей смартфонов используют их для оплаты товаров и услуг в платежных терминалах, но более 50% потребителей заинтересованы возможностью использования мобильного телефона в качестве банковской карты.

С помощью NFC-чипа, встроенного в мобильный телефон, появится возможность оплачивать общественный транспорт, товары в магазинах, счета в ресторанах и совершать любые другие привычные платежи, просто поднося телефон к считывающему устройству. Уже сейчас есть возможность оплачивать поездку в аэропорт на аэроэкспрессе, кофе в «Старбаксе» и проезд в метро в Москве и Екатеринбурге с помощью мобильного телефона, получив специальную SIM-карту у оператора сотовой связи.

Рынок NFC-платежей еще незначительно развит в абсолютных значениях, но растет на 70% в год и имеет огромный потенциал к использованию в местах, где скорость обслуживания является основным критерием. Согласно оптимистическому сценарию J`son & Partners Consulting, объем мобильных платежей к 2017 году в России с использованием NFC превысит 50 млрд руб., несмотря на прогноз на 2012 год в 30–150 млн руб.

На данный момент основными сложностями в распространении NFC-систем являются неразвитость инфраструктуры, комиссии операторов сотовой связи и NFC-чипы. Из-за более высоких затрат на технологии и обслуживание NFC многие финансовые институты в США начинают тестирование новых «облачных» технологий хранения и обработки платежной информации, которые не зависят от провайдеров связи, производителей дополнительного оборудования и даже карточных систем. Такие технологии позволяют безопасно хранить клиентские данные «в облаке», отсылая в платежный терминал только токен, используя мобильное приложение на смартфоне с камерой для считывания QR-кода, заменяя технологию NFC.

В свою очередь, привлекательность для банков предложения мобильных банковских услуг обусловлена не только удовлетворением спроса уже имеющихся клиентов и привлечением новых, но и снижением затрат на транзакции и содержание дополнительных офисов из-за снижения количества обслуживаемых в них клиентов.

Причем клиенты, использующие мобильные приложения для проверки баланса, совершения платежей и переводов, поиска отделений и банкоматов и даже для удаленного открытия вкладов, менее склонны к смене банка. На основе таких систем уже сейчас могут быть построены мобильные приложения, связанные с виртуальными платежными кошельками, которые могут пополняться как из других платежных систем, так и с помощью наличных в терминалах, полностью исключая банки и международные карточные платежные системы из цепочки оплаты.

То есть серьезной опасностью для банков и международных платежных систем типа Visa и MasterCard является возможность продвижения в России мобильных платежных систем, не привязанных к банковским картам. Переход процессинга платежей от банков к новым игрокам рынка платежей грозит платежным системам не только потерей прибыли, но и потерей важной статистической информации о клиентском поведении, на основе которой разрабатываются новые продукты и поддерживаются уже имеющиеся.

Наталья Геращенко, Радек Йезбера, PwC

Правила съема

интернет-банкинг

Развитие сферы банковских услуг с использованием удаленных каналов доступа не только облегчило операции по проведению расчетов и переводу денежных средств, но и создало условия для совершения преступлений. Методы работы преступников и противодействия им изучал корреспондент "Ъ–Финансы" Дмитрий Астахов.

По данным управления Центробанка по Пермскому краю, в минувшем году банками региона было эмитировано 2,3 млн платежных карт. На территории Пермского края было совершено 128 млн операций на сумму 330,2 млрд руб. По сравнению с 2011 годом количество сделок увеличилось на 39,2%, а объем — на 34,3%.

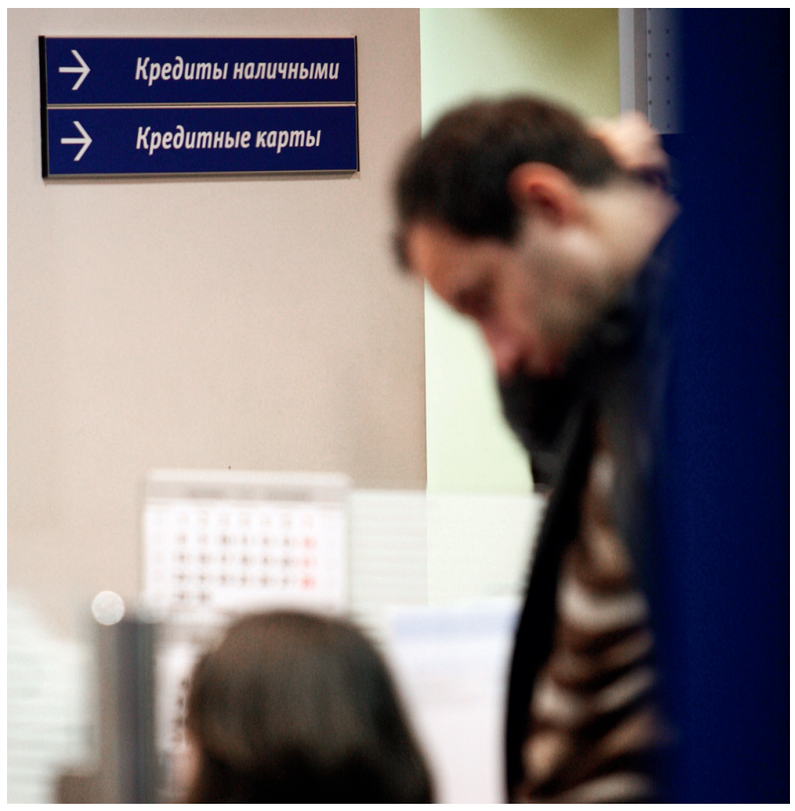
Вместе с ростом объема потребления этих услуг растет и число преступлений, связанных с хищением средств, находящихся на банковских счетах клиентов, с использованием высоких технологий. Потерпевшими от действий злоумышленников в разное время были бывший пермский политик, губернатор Кировской области Никита Белых, футболист пермского «Амкара» Сергей Волков, авиакомпании «Уральские авиалинии» и UTair. По данным отдела «К» ГУ МВД по Пермскому краю, в прошлом году было зафиксировано более 100 преступлений, связанных с кредитными картами. При этом борцы с киберпреступностью отмечают, что их отдел оказывает оперативное сопровождение далеко не по всем уголовным делам. Некоторые из них расследуются в районных отделах МВД, где специалистов этого профиля просто нет.

Наиболее распространенные виды преступлений — хищение средств через получение доступа к персональному компьютеру клиента, а также компрометация (завладение данными) банковских карт. Суммы ущерба от таких преступлений варьируются от нескольких десятков тысяч до миллионов рублей. «Жертвами становятся и физические и юридические лица, каких-то особых предпочтений у злоумышленников нет, в большинстве случаев деньги воруют у тех пользователей, чей компьютер заражен вирусом, с помощью которого можно получить доступ к данным счета», — пояснил один из сотрудников отдела «К».

Полицейские отмечают, что, как и программное обеспечение, вредоносные программы постоянно совершенствуются и развиваются. Стопроцентную защиту не может обеспечить ни одна система. При этом часто инфицирование компьютера происходит по вине самих потерпевших, которые пренебрегают мерами по обеспечению безопасности передаваемой информации.

«Самым популярным способом мошенничества является выманивание у пользователя личной информации, необходимой для проведения операций с его счетами», — рассказывает управляющая РОО «Пермский» ВТБ 24 Светлана Щеголева. По ее словам, чаще всего используется ссылка на поддельную страницу банка, на которой клиента просят ввести его конфиденциальные данные — логин и пароль для входа в интернет-банк, реквизиты банковской карты. Также данные пытаются получить с помощью SMS и других видов рассылок.

Начальник управления безопасности информационных систем Уральского банка реконструкции и развития (УБРиР) Александр Падерин также отмечает, что с каждым годом методы преступников становятся все более изощренными, но при этом случаи, когда попытки мошенников увенчались бы успехом, в УБРиР единичны. По словам господина Падерина, пик попыток несанкционированного доступа приходится на осень и зиму, наиболее спокойное в этом отношении время — весна. «Очень важно понимать, что для мошенников всегда слабым звеном является клиент, именно его рабочее место, а не сервер банка, подвергается атаке злоумышленников», — пояснил Александр Падерин.



В прошлом году в Прикамье зафиксировано более 100 преступлений, связанных с кредитными картами ФОТО АЛЕКСАНДРА ВАЙНШТЕЙНА

В качестве элементарных мер обеспечения безопасности интернет-банкинга в отделе «К» предлагают использовать только лицензионное ПО, а также антивирусные программы и поддерживать их постоянное обновление. «Идеальный вариант — это когда для дистанционного банковского обслуживания используется специальный компьютер, который не привлекается для выполнения каких-то других задач», — говорят в отделе «К».

Полицейские отмечают, что банковские организации активно сотрудничают с правоохранительными органами в борьбе с киберпреступниками. «Если преступление все же произошло, то от действий злоумышленников страдает не только счет клиента, но и имидж банка, восстановление которого зачастую зависит от результатов расследования и изобличения лица, совершившего преступление», — считает сотрудник отдела «К».

Средства обеспечения безопасности банковского счета — один из наиболее быстро развивающихся видов услуг, предлагаемый банками. «ВТБ 24 применяет различные средства и методы защиты информации, начиная с паролей и заканчивая многоуровневыми системами безопасности на основе современных криптографических протоколов и алгоритмов, реализующих шифрование и работу с электронными цифровыми подписями (ЭЦП), — говорит Светлана Щеголева, — все зависит от выбранной услуги или продукта».

По словам Александра Падерина, максимальный предлагаемый банком пакет услуг включает в себя возможность использования OTP-токена для формирования одноразовых паролей с целью подтверждения платежей, USB-токен для неизвлекаемого хранения ключей электронной подписи, а также антивирусное программное обеспечение с годовым правом пользования. Господин Падерин отмечает, что каждый клиент, счет которого подвергался попытке несанкционированного доступа, приобретает дополнительные средства защиты.

Менее распространенный способ — хищение средств с помощью несанкционированного доступа к банкоматам. Собеседники "Ъ–Финансы" отмечают, что таким образом совершить преступление гораздо сложнее, так как за их безопасность отвечают банковские структуры. Так, по словам Светланы Щеголевой, в ВТБ 24 существует внутренний регламент по установке банкоматов. Большая часть из них располагается в офисах банка, в крупных торговых сетях. «При этом соблюдено требование отсутствия зеркальных поверхностей и потолков, обеспечена «зона безопасности» для клиента, устройства обеспечены камерами видеонаблюдения, банкоматы и их содержимое застрахованы», — рассказывает госпожа Щеголева. В рабочее время банкоматы регулярно осматривают сотрудники кредитной организации, а в выходные и праздничные дни банкоматная сеть охраняется техническими средствами охраны, силами специализированных охранных предприятий и МВД России.

По ее данным, наиболее распространенным способом хищения является использование скиммеров — устройств, считывающих данные с магнитной полосы платежной карты. Данные карты, в том числе и пин-код, передаются злоумышленнику, который изготавливает дубликат и получает возможность снять наличные со счета потерпевшего.

Эксперты в области ГТ-безопасности отмечают, что в качестве средства защиты от скримминга банки предлагают чиповые карты, которые исключают передачу пин-кода по каналам связи и снижают риск получения данных мошенниками. «Проблема в том, что с чипом работать могут не все банкоматы. Быстро произвести модернизацию всей банкоматной сети у кредитных организаций нет ни возможности, ни особого желания», — отметил собеседник "Ъ–Финансы".