СКРЫТЫЕ УГРОЗЫ

ОБРАТНАЯ СТОРОНА РОСТА БАНКОВСКОГО РИТЕЙЛА — УЧАЩЕНИЯ СЛУЧАЕВ ФИНАНСОВОГО МОШЕННИЧЕСТВА, ЖЕРТВАМИ КОТОРОГО СТАНОВЯТСЯ КРЕДИТОРЫ И ИХ ЗАЕМЩИКИ. ПРАКТИЧЕСКИ КАЖДЫЙ ЧЕЛОВЕК, БУДЬ ОН ПЕНСИОНЕРОМ ИЛИ СТУДЕНТОМ, МОЖЕТ В ЛЮБОЙ МОМЕНТ ОКАЗАТЬСЯ ЖЕРТВОЙ МОШЕННИКОВ, ВЗЯВШИХ НА ЕГО ИМЯ КРЕДИТЫ. ТАКАЯ СИТУАЦИЯ ЧРЕВАТА В ОСНОВНОМ ПОТЕРЕЙ ВРЕМЕНИ И УХУДШЕНИЕМ КРЕДИТНОЙ ИСТОРИИ. ОДНАКО ТОТ ФАКТ, ЧТО КРЕДИТ БРАЛ ДРУГОЙ ЧЕЛОВЕК, ЧАЩЕ ВСЕГО ДОКАЗАТЬ МОЖНО. ДРУГИМИ СЛОВАМИ, ДЕНЕЖНЫЕ ПОТЕРИ ПОНЕСЕТ ПРЕЖДЕ ВСЕГО САМ БАНК. АЛЕКСЕЙ ДОЛЯ

ПСЕВДОКРЕДИТ Опасной угрозой является взятие кредитов на чужое имя. Ситуация становится особенно неприятной, если мошенники взяли кредит на ваше имя, и все свои претензии банк предъявляет вам.

Если говорить о России, то речь, конечно, не идет о крупных кредитах, типа ипотечного. Довольно редко такое случается и с автомобильным кредитом. Однако потребительский кредит в сумме до 500–600 тыс. руб. очень часто выдают без изощренных проверок, что в конечном итоге приводит к мошенничеству. Посмотрим, как это происходит.

Чтобы получить кредит, гражданин должен представить в банк ряд документов. Если сумма небольшая, то достаточно и только паспорта. Если на кону деньги побольше, то банк может попросить справку о зарплате, проверить кредитную историю и запросить какие-нибудь дополнительные документы.

Наиболее распространенная схема мошенничества предполагает, что у преступника есть практически все персональные сведения жертвы: паспортные данные, адрес регистрации, а также другая информация, если она потребуется. Используя одни только эти сведения, можно получить потребительский кредит прямо в магазине и накупить бытовой техники, правда, банковский служащий, оформляющий кредит, должен быть с преступником заодно. Ведь у мошенника нет оригинального паспорта с фотографией, поэтому идентифицировать покупателя невозможно.

Далеко не у всех мошенников есть такие подельники-инсайдеры, поэтому на практике используются и другие, более изощренные методы. Можно, например, подделать военный билет или паспорт, просто вклеив в него другую фотографию. Банковский служащий сделает ксерокс с документа и почти наверняка не сможет отличить оригинал от фальшивки. Или мошенник подыскивает жертву, внешне на него похожую, и крадет у нее паспорт.

Несколько сложнее получить кредит на серьезную сумму, скажем, в районе 500 тыс. руб. В этом случае банк может проверить кредитную историю заемщика, но и мошенник может воспользоваться одной из продающихся сегодня на черном рынке баз данных.

Например, в августе прошлого года в продажу поступила база данных заемщиков, бравших кредиты на приобретение товаров в торговых сетях. Размер базы был просто огромен — более 700 тыс. записей. Каждая запись базы содержала ФИО заемщика, его адрес, название торговой сети, где была совершена покупка в кредит, сумма покупки, размер первоначального взноса, размер кредита, срок кредита, размер ежемесячного платежа, объем просрочки и сумма санкций. За всю базу, которая содержит более 700 тыс. записей, продавцы запросили 90 тыс. руб., что не идет ни в какое сравнение с рыночной стоимостью кредитных историй — одна такая история в кредитном бюро стоит около $0,4.

Все тем же летом 2006 года в свободной продаже ходила база частных клиентов банка «Первое ОВК» (ныне поглощен Росбанком), получавших кредиты в 2002–2003 годах. Ее можно было купить всего за 900 руб. В ней были указаны заемщики, номера их домашних или мобильных телефонов, а в ряде случаев — паспортные данные и домашние адреса. То есть все, что необходимо для получения розничного кредита.

АЛЕКСАНДР МИРИДОНОВ

ЕСЛИ В ВЕЛИКОБРИТАНИИ СРЕДНЯЯ СТОИМОСТЬ НОМЕРА ФАЛЬШИВОЙ КРЕДИТКИ СОСТАВЛЯЕТ $10 (£5), ТО В КИТАЕ И ИНДИИ ОНА ПАДАЕТ ДО $1. РОССИЯ ЗАСТРЯЛА ГДЕ-ТО ПОСЕРЕДИНЕ

ПСЕВДОБАНК Фишинг подразумевает, что преступники рассылают по электронной почте фальшивое сообщение от лица банка, в котором призывают получателя зайти на веб-сайт и осуществить какие-нибудь операции со своим счетом. Ловушка состоит в том, что пользователи заходят не на сайт банка, а на поддельную страницу, которая полностью копирует элементы оформления оригинала. Только вот реквизиты для доступа к счету (например, пароль или номер карточки) отправляются прямиком на компьютер преступникам, которые потом смогут продать их своих заокеанским подельникам, изготовить фальшивую пластиковую карточку или просто перевести деньги вкладчика на свой счет через интернет.

Еще пару лет назад в нашей стране фишинг представлял угрозу лишь теоретически. Действительно, пусть боятся американцы и европейцы, а у россиян не так много кредитных карт, слабо развита система интернет-банкинга, да и достучаться до клиентов какого-то конкретного банка по электронной почте — проблема.

Между тем, уже в этом году два российских банка и одна платежная система подверглись атаке фишинга. Причем один из банков пострадал дважды. Это Альфа-банк, чьи клиенты стали объектом фишинга в марте и в сентябре. До этого весной пострадал Райффайзенбанк, а чуть позже пришла очередь платежной системы «Яндекс.Деньги».

В случае с Альфа-банком мошенники действовали по классической схеме. Пользователи электронной почты получили небольшое письмо с адреса ibank@alfabank.ru. В сообщении, в частности, утверждалось, что «в целях обеспечения безопасности денежных средств Вашей организации» необходимо получить некий «электронный ключ». А чтобы сделать это, гражданам предлагалось перейти по расположенной ниже ссылке и указать логин и пароль для входа в систему интернет-банкинга Альфа-банка.

Надо ли говорить, что ссылка вела не на корпоративный сайт банка, а на поддельный ресурс, который контролировали мошенники. После того как наивный пользователь вводил запрашиваемые данные, они мгновенно попадали в руки злоумышленников, которые использовали их для перевода денег с электронных счетов.

Вместе с тем, сегодня очень маловероятно, что конкретный клиент конкретного банка станет жертвой фишинга. Дело в том, что одновременно должны совпасть три обстоятельства. Во-первых, у человека должен быть открыт счет в банке. Во-вторых, для этого счета должна быть подключена услуга интернет-банкинга. В-третьих, именно этому клиенту банка нужно прислать фишинговое письмо от лица его конкретного банка. Чтобы повысить свои шансы, фишеры обычно рассылают миллионы и десятки миллионов сообщений от лица самых популярных банков. Они словно рыбаки закидывают удочку и ждут, поймается ли кто. Если из миллиона хоть несколько человек оставят свой логин и пароль, то затея уже оправдалась.

Однако в России подобная схема не работает. У нас попросту нет такого количества популярных гигантских банков, у которых десятки миллионов клиентов. Исключением является, быть может, Сбербанк, но своей огромной клиентской базой он обязан пенсионерам, которым интернет-банкинг точно никогда не понадобится.

Так на что же тогда делают ставку фишеры? В первую очередь на адресные атаки. Сейчас российские преступники только пристреливаются, но уже в самое ближайшее время последуют по стопам своих трансатлантических коллег и начнут рассылать сообщения только самой что ни на есть целевой аудитории.

Другими словами, фишеры должны знать, кто конкретно подключил к своему счету услугу интернет-банкинга, в каком это было банке и какой электронный адрес у этого человека. Получить всю эту информацию можно только через инсайдеров, т. е. сотрудников банка, которые сольют мошенникам все нужные сведения за деньги. Такие организованные преступные группы уже не раз разоблачали в США и Европе, причем все указывает на то, что в ближайшие два года этих преступников начнут ловить и в России.

Как защититься от адресной фишинговой атаки? С точки зрения банка все ясно. Надо лишь следить за своим персоналом и не давать ему красть конфиденциальную информацию. А с точки зрения клиента все еще проще. При получении письма от банка надо просто позвонить в этот банк, взяв номер телефона с официального сайта или из надежного источника (банковского договора, пластиковой карточки и т.д.). В подавляющем большинстве случаев клиент услышит по телефону, что банк никакой рассылки не осуществлял и реквизиты для доступа к счету ему, естественно, не нужны.

ПСЕВДОКАРТА Нет, пожалуй, более быстрого способа расстаться с деньгами чем через пластиковые карты. Зная номер карты, имя ее владельца, срок действия карты и так называемый CVV-код (последние три или четыре цифры, написанные на обратной стороне карты), можно делать покупки в любых интернет-магазинах. Имея на руках значительно меньшую информацию, скажем, только номер карты и имя владельца, можно изготовить поддельную пластиковую карту и снять деньги в любом банкомате.

Чтобы получить данные о чужой кредитке, мошенники иногда используют фишинг, но намного чаще «кредитная» информация крадется напрямую из баз данных компаний, обрабатывающих транзакции банковских карт. Примерами таких компаний могут быть банки, крупнейшие розничные сети или государственные организации. Для кражи «кредитных» данных мошенники подкупают сотрудников этих компаний, используют различные вредоносные программы (вирусы) или крадут технику физически (например, ноутбуки или жесткие диски).

Однако профессиональные мошенники редко занимаются «обналичкой», предпочитая продавать номера и имена владельцев чужих кредиток на черном рынке. Сегодня в сети существует огромное количество сайтов, предлагающих «кредитную» информацию по весьма приемлемым низким ценам. Так, ресурс http://mccrack.narod.ru/ предлагает 10 «кредитных» записей всего за $3,5, которые можно заплатить в платежной системе WebMoney (WMZ).

Некоторые мошенники идут еще дальше и вместо информации продают сами пластиковые карты, конечно, поддельные. Их можно обналичить в любом ближайшем банкомате. Согласно сведениям на сайте http://kredit-kard.biz/, стоимость одной такой карты составляет $100–200 долларов (в зависимости от объемов покупки). На сайте имеется раздел «Ответы на вопросы», в котором утверждается, что среднее количество денег, которые можно снять с одной карты, колеблется в интервале от $1500 до $2500.

Конечно, в первую очередь приходит мысль, что этот сайт создали скорее спецслужбы, чем настоящие преступники. Однако анализ веб-сайтов не только в России, но и за границей показывает, что в любой стране мира и на любом языке существуют черные рынки номеров кредитных карт. Причем если в Великобритании средняя стоимость номера кредитки составляет $10 (£5), то в Китае и Индии она падает до $1. Россия, как видно, застряла где-то посередине.

Защититься от кардинга очень сложно. Здесь нет столь же простых рецептов, как и с фишингом. Однако эксперты советуют просто не хранить большую сумму денег на том счете, к которому прилагается пластиковая карта. В этом случае клиент просто ограничит объем потерь на случай мошенничества. Тем более что лишь редкие банки в этом случае возвращают деньги пострадавшим клиентам. ■

РАСПРОСТРАНЕННАЯ СХЕМА МОШЕННИЧЕСТВА ПРЕДПОЛАГАЕТ, ЧТО У ПРЕСТУПНИКА ЕСТЬ ВСЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЖЕРТВЫ, С ПОМОЩЬЮ КОТОРЫХ МОЖНО ПОЛУЧИТЬ ПОТРЕБИТЕЛЬСКИЙ КРЕДИТ, ПРАВДА, БАНКОВСКИЙ СЛУЖАЩИЙ, ОФОРМЛЯЮЩИЙ КРЕДИТ, ДОЛЖЕН БЫТЬ С ПРЕСТУПНИКОМ ЗАОДНО

ЗАКОН О КРЕДИТНОЙ КАРТЕ

Разросшиеся масштабы кредитования и финансовых операций с помощью кредитных карт к 70-м годам XX века потребовали более внимательного отношения со стороны властей США. Возникало много вопросов: каких правил придерживаться для исправления ошибок, происходящих по вине компьютерных систем, кто должен их устанавливать; что делать для защиты клиентов от несовершенных операций; как определить ответственность клиента и обязанности эмитента при утере карты; по каким критериям оценивать возможности доступа разных клиентов к кредиту; что делать для обеспечения или ограничения доступа к кредитным историям миллионов владельцев карт. Федеральная комиссия по торговле в 1970 году приняла решение запретить рассылку по почте не затребованных клиентом карт. В 1972 году регулятором индустрии карт стала Федеральная резервная система. В последующие годы был принят закон, обеспечивающий защиту владельцев карт от несанкционированного использования счетов и информации по картам. Было также запрещено использовать расовую принадлежность, пол, вероисповедание, национальное происхождение или семейное положение в качестве критерия для разрешения или отказа в кредите. Современные финансисты в один голос признают операции по картам самой значительной банковской услугой прошлого века. Ни один из банковских продуктов не смог завоевать столько приверженцев по всему миру, как пластиковая карта. В настоящее время пластиковые карты разных типов используют миллиарды людей, ежегодный мировой оборот превышает $3 трлн. Платежные системы VISA и MasterCard до сих пор доминируют в мире финансовых операций, осуществляемых посредством кредитных карт, а American Express лидирует в области туризма и развлечений.

ЕКАТЕРИНА ДУДАРЕВА