• безопасность

Кардинг, скимминг и др.

В банковской сфере пышным цветом расцветает киберпреступность

Татьяна Власенко

Рост безналичных расчётов на рынке товаров и услуг сопровождается негативом, который снижает доверие юридических и физических лиц к электронной финансовой деятельности банков. Учащаются случаи взлома информационных систем, в результате чего злоумышленники получают доступ к банковским картам клиентов и их реквизитам.

По словам начальника отдела управления безопасности и защиты информации ГУ Банка России по Пермскому краю Станислава Попова, наиболее распространёнными нарушениями являются изготовление дубликатов платёжных карт и вещевой кардинг.

Классическая преступная схема представляет собой изготовление дубликатов кредитных или расчётных (в том числе выпущенных в рамках зарплатных проектов) карт, которые в дальнейшем перепродаются для обналичивания денежных средств или перевода денег на счета мобильных телефонов, зарегистрированных на вымышленных лиц.

Вещевой кардинг связан с приобретением различных товаров в интернет-магазинах с помощью полученных преступным путём банковских реквизитов. Прежде так называемые кардеры преимущественно имели дело с иностранными банками и их клиентами, но в последнее время переключились на российский рынок банковских услуг.

Преступники действуют и на территории Пермского края. Это хорошо организованные межрегиональные группы, которые распределяют между собой роли, поэтому обнаружить их и привлечь к ответственности достаточно сложно.

Среди них есть спецы, которые занимаются только взломом и получением информации о банковской карте. Полученная ими информация передаётся лицам, содержащим подобие интернет-магазина, который перепродаёт банковские реквизиты производителю поддельных пластиковых карт. Тот, в свою очередь, распространяет подделки, продавая или передавая их последнему звену цепочки — «дрогу». «Дрог» — это физическое лицо, которое организует непосредственно съём денег в банкоматах. Он обладает наименьшим объёмом информации, часто его используют «втёмную».

Общение между участниками преступной группы происходит через различные интернет-сервисы: Сеть пестрит объявлениями о «простом и доступном» заработке. И это провоцирует значительный рост таких преступлений.

Станислав Попов, начальник отдела управления безопасности и защиты информации ГУ Банка России по Пермскому краю:

— Организаторы такого бизнеса — люди образованные — как с технической, так и с юридической стороны. Они зачастую имеют несколько высших образований, знакомы в том числе с криптографией, что значительно затрудняет их поиск.

На территории края действует несколько устойчивых преступных групп, которые занимаются кардерской деятельностью. Они пропагандируют лёгкий заработок, якобы не грозящий наказанием, ведут свою деятельность с помощью SIM-карт, зарегистрированных на подставных лиц, что зачастую приводит розыск злоумышленников в тупик.

Ещё один вид преступлений — мошенничество с платёжными картами посредством скимминга (перехват информации с магнитной полосы платёжных карт с использованием специального устройства — скиммера, устанавливаемого на банкомат). Скиммер накладывается непосредственно на картридер, куда ничего не подозревающая жертва вставляет свою карту. Преступники снимают данные и в любой момент могут опустошить банковский счёт клиента или изготовить поддельную копию карты.

Существуют даже специальные панели, которые накладываются на всю поверхность банкомата, где считываются одновременно и PIN-код, и номер банковской карты. При этом скиммеры свободно продаются в интернете и стоят порядка $200. Некоторые продавцы за определённую плату предлагают даже обучить изготовлению скиммеров.

Специалисты по банковской безопасности рекомендуют: прежде чем воспользоваться банкоматом, стоит внимательно его осмотреть. На нём не должно быть выступающих частей, особенно отличающихся по цвету. Возле банкомата не должно быть подставок с буклетами, следует обратить внимание и на людей, находящихся поблизости.

«Многие банки начали вести видеонаблюдение за банкоматами, использовать специальную сенсорную сигнализацию, устанавливать антискримминговые накладки, устраивать плановые проверки банкоматов на предмет установки таких устройств», — поясняет Станислав Попов методы борьбы с преступниками.

По данным специалистов антивирусных компаний, в последнее время наблюдается расцвет интернет-мошенничества. Такие действия подпадают под статью Уголовного кодекса РФ «Создание и использование, распространение вредоносного программного обеспечения».

Станислав Попов:

— Для противодействия разработчики защитного программного обеспечения пытаются совершенствовать свои продукты. Правоохранительные органы взялись за эту разновидность киберпреступности, которая, развиваясь, приобретает новые формы.

Самое популярное средство у мошенников — так называемые банковские «трояны». Они ориентированы на получение неавторизованного доступа злоумышленников к счетам физических лиц посредством системы дистанционного банковского обслуживания, которая набирает обороты.

Но есть и просто мошенничество. Пользователи банковских карт могут получить сообщение якобы от службы безопасности кредитной организации, где для повышения безопасности карты и во избежание блокирования клиенту предлагается вставить её в любой банкомат, набрать PIN-код и позвонить с мобильного телефона по указанному в SMS-сообщении номеру. Затем выполнить ряд действий, которые будет диктовать оператор. Это будет набор цифр определённой последовательности. После завершения этих манипуляций человек, как правило, обнаруживает, что деньги с карты уже переведены на другие банковские счета. И это далеко не все схемы мошенничества.

• скимминг

Схема: вы совершаете любую операцию в банкомате и, ничего не подозревая, уходите по своим делам. В то время как мошенники с помощью скиммера считали всю информацию о вашей карте и в любой момент сделают её дубликат и обнулят ваш банковский счёт.

Откуда мошенники узнают PIN-код?

Варианты:

- самый элементарный способ — человек, стоящий за вами в очереди, просто подсмотрит пин-код из-за вашей спины;
- мошенники могут распылить на клавиатуру специальный спрей, на котором будут чётко видны нажатые вами клавиши;
- мошенники могут установить накладную клавиатуру, которая почти ничем не отличается от самой клавиатуры банкомата;
- установка на банкомат микрокамеры, вы её не заметите, потому что она будет спрятана за пачкой рекламных буклетов.

С 1 января 2014 года вступают в силу основные положения ст. 9 «Порядок использования электронных средств платежа» федерального закона №161. В соответствии с этим документом, банки будут обязаны уведомлять клиента о совершении каждой операции с использованием его электронного средства платежа (например, телефонной связи, SMS-сообщений, электронной почты и т. п.).

В случае утраты карты и её использования без согласия клиента он обязан направить соответствующее уведомление кредитной организации незамедлительно после обнаружения пропажи. Клиент тоже должен быть заинтересован в доведении информации о факте мошенничества, это в его интересах: только в этом случае оператор по переводу денежных средств будет обязан возместить клиенту сумму указанной операции. И уже потом банк будет разбираться, в результате чьих злоумышленных действий были похищены деньги.

«Новый компаньон»

В СЕМЬЕ НЕ БЕЗ ИНФЛЯЦИИ

По словам заместителя министра экономического развития Андрея Клепача, инфляция в России в июле 2013 г. составит около 1%, что на 0,2% меньше, чем в прошлом году. Он объяснил это тем, что в июле «было снесено повышение тарифов (естественных монополий)». Что изменилось за прошедшую неделю? Рис, сливочное масло и сыры стали дороже на 0,3-0,4%. Одновременно цены на яйца снизились на 0,5%, на баранину, соль и гречневую крупу — на 0,1-0,2%. Цены на бензин не изменились, а на дизельное топливо даже снизились на 0,1%. Тарифы на электроэнергию выросли на 1,4%, на отдельные виды коммунальных услуг — на 0,7-1,5%. По данным Федеральной службы государственной статистики (Росстат), инфляция в стране в июне 2013 г. составила 0,4%, а за период с начала года — 3,5%. В годовом выражении инфляция в июне 2013 г. составила 6,9%. Согласно же официальному прогнозу Министерства экономического развития, по росту потребительских цен в России в 2013 г. инфляция составляет 5-6%.*

Высокая инфляция — главный враг наших сбережений. Не потерять и приумножить поможет **вексельная сберегательная программа «НАСЛЕДИЕ»**. Это один из гибких и удобных инструментов защиты сбережений и приумножения средств. Размер процентного дохода зависит от суммы векселя и срока вексельного инвестирования. С июня 2013 года можно получать начисленные проценты по векселям ежеквартально**. Вам не нужно ждать даты предъявления векселя к платежу, чтобы получить свой доход. Забрать начисленные проценты вы можете через три месяца после вложения средств! Услуга доступна для новых клиентов ИФК***. Вы можете самостоятельно выбирать, когда получить свой доход****. Получить более подробную информацию можно в офисе **ООО «Сберегательная компания «Наследие»** по адресу: ул. Куйбышева, д. 50А, офис 502А, по телефонам: **(342) 204-04-79, 8-922-354-04-79** или позвонив в Единый федеральный центр обслуживания клиентов по номеру **8-800-333-14-06** (звонок бесплатный), а также на сайте www.gkifk.ru.

* *по материалам РБК, interfax, gov.ru*
** *под кварталом понимается трёхмесячный период с даты выдачи векселя*
*** *при условии подписания соглашения о выплате начисленных процентов по векселю*
**** *условия и порядок определяются подписанным соглашением о выплате начисленных процентов по векселю*