Как защитить себя от мошенничества с банковскими картами

С каждым годом количество пользователей банковских карт неимоверно растёт. И это не удивительно, ведь выплата заработной платы на многих предприятиях осуществляется с помощью именно этой банковской услуги, немалое количество людей хранят и используют свои сбережения, пользуясь маленькой пластиковой карточкой, считая такой вариант более надёжным, удобным и безопасным, чем ношение наличных денег с собой или хранение их дома.

На фоне роста популярности использования банковских карт участились случаи мошенничества, связанные с кражей денег со счётов клиентов. Ничего неподозревающие люди в мгновении ока лишаются крупных денежных сумм после покупки товара или услуги, использования банкомата или оплаты счёта. При этом иногда случаются хищения массового масштаба, когда одновременно у большого количества клиентов одного банка со счетов списываются крупные суммы денег.

Банковская карта – это действительно более удобный и безопасный способ хранения и использования денежных средств, но только при строгом соблюдении мер предосторожности. Многие забывают об этом и не придают значение простым вещам, способным предотвратить плачевные последствия. В последнее время рост массовых хищений со счетов клиентов в первую очередь связан со следующими причинами:

- установкой на смартфоны приложений, позволяющих управлять счётом через мобильный телефон;
- покупкой товаров в интернет - магазинах;
- оплатой счетов через интернет.

На этом, конечно, список не заканчивается и есть множество других причин, по которым происходит рост количества хищений денежных средств с банковских карт. Но главная причина всё-таки остаётся той же – невнимательность и несоблюдение правил безопасности при работе с банковской картой.

Виды мошенничества с банковскими картами

На сегодняшний день существуют десятки способов обмана людей и кражи денег с банковских карт, начиная от банального подглядывания из-за плеча во время использования клиентом банкомата и последующим хищением его карты, заканчивая хакерскими атаками на программное обеспечение пользователя. При этом злоумышленники постоянно придумывают новые способы хищения денежных средств.

Одним из наиболее распространённых на данный момент является способ обмана людей через интернет. Обычно кражи происходят по одной из следующих схем - заражение вирусом-трояном. Операционная система персонального компьютера или мобильного устройства перенаправляет пользователя при входе на официальный сайт банка на поддельную, так называемую фишинговую веб-страницу, которая полностью имитирует внешний вид настоящего сайта (иногда переход на такую страницу может быть произведён без заражения вирусом просто по невнимательности пользователя). Ничего не подозревающий клиент вводит свои персональные данные, тем самым предоставляя мошенникам часть необходимой информации для того, чтобы они смогли войти в личный кабинет жертвы. После этого злоумышленники просят ввести разовый код подтверждения, который выслал банк, а затем перечисляют денежные средства на свои счета. В это время на фишинговой веб-странице появляется надпись, что в системе произошёл сбой и клиенту могут приходить на телефон ошибочные смс-сообщения о переводе с карты денег на другие счета. При этом очень часто жертве поступает звонок с номера, очень похожего на банковский, где некто представляется сотрудником банка и сообщает ту же информацию о сбое в системе и ошибочных сообщениях, уверяя, что всё в порядке, а при необходимости подтверждения каждой операции по переводу денежных средств разовыми паролями, приходящими на телефон от реального банка, просит

вводить их в поле, запрашиваемое страницей. После этого клиенту может прийти смс-сообщение, якобы от банка, об отмене ошибочных операций, но это только для того, чтобы на время усыпить бдительность.

Другие вирусные программы способны встраиваться в операционную систему и браузер и изменять данные при произведении финансовых операций. Клиент, оплачивая коммунальные услуги, погашая кредиты или производя другие оплаты, не замечает, как вирус мгновенно подменяет номера счетов и даже суммы перечислений. При этом эти программы способны изменять данные, отображаемые интернет - банками, поэтому информация о незаконных переводах будет скрыта.

При телефонном обмане злоумышленники, взламывая личный кабинет пользователя на сайте мобильного оператора (кстати, это сделать значительно легче, чем у интернет-банков), используют предоставляемую услугу переадресации смс-сообщений и перенаправляют к себе на номер информацию, получаемую клиентом от банка. Это информация позволяет получить доступ к личному кабинету интернет-банка и опустошить счёт.

При краже либо утери телефона или SIM-карты, к которой была привязана банковская карта, мошенники способны также с легкостью получить доступ к интернет-банку и осуществить перевод денежных средств к себе на счёт. Также имейте ввиду, что, если вы не используете SIM-карту в течение определённого времени, оператор вправе перепродать номер другому абоненту. А если к этому номеру была привязана ваша банковская карточка, то другой владелец сможет получить доступ к вашему счёту. Всегда помните, при утрате мобильного телефона, на который подключена услуга «Мобильный банк» или при смене номера телефона, на который подключена услуга «Мобильный банк», Вам необходимо срочно обратиться в банк с заявлением на отключение услуги «Мобильный банк».

Бывают случаи, когда на номер, к которому привязана пластиковая карта, поступает смс-сообщение с информацией о блокировке карты и просьбой перезвонить по телефону, для уточнения информации. Доверчивые люди перезванивают по указанному номеру, на другом конце представляются сотрудником банка и говорят, что для разблокировки необходимо назвать данные банковской карты, кодовое слово и другую информацию. После это злоумышленники используют полученные сведения для кражи денежных средств. Настоятельно рекомендуем:

- не перезванивать на мобильный номер, указанный в полученном сообщении, и не отправляйте SMS, обратитесь к специалисту Банка и покажите ему SMS,

- не называть реквизиты пластиковой карты (PIN-код, номер карты, срок действия, код защиты). Сотрудники банка могут запросить только 4 последние цифры карты, кодовое слово, указанное при открытии счета банковской карты в заявлении.

- помните, что сотрудники банка не просят клиентов вставить карту в банкомат и провести какую-либо операцию по переводу денежных средств на счета, не принадлежащие клиенту, в том числе перевод в счет оплаты услуг мобильной связи.

Самый простой способ кражи денег с помощью банкомата, когда мошенник подглядывает вводимый PIN-код, а затем производит кражу пластиковой карты. При проведении операции с вводом PIN-кода ВСЕГДА прикрывайте клавиатуру, например, свободной рукой, чтобы не было возможности увидеть Ваш PIN-код или записать его на видеокамеру. Храните PIN-код отдельно от Вашей карты, не пишите его другим лицам, не вводите PIN-код при работе в сети Интернет. Во время съема денежных средств в банкомате не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. В таких случаях нужно обратиться к сотрудникам банка или позвонить по телефонам, указанным на устройстве или на обратной стороне банковской карты.

В другой схеме воры используют небольшой кусок фотоплёнки, который складывается пополам, а края загибаются под прямым углом. Это приспособление

вставляют в банкомат в отверстие для приёма карты, таким образом, что нижняя часть плёнки позволяет карте пройти внутрь и провести финансовую операцию, но не даёт ей выйти обратно. В это время к владельцу карты подходит один или несколько человек, которые советуют немедленно обратиться в сервис. Пока жертва отвлечена, злоумышленники используют карту, заранее подглядев вводимый PIN –код.

При утрате карты либо при малейшем подозрении о том, что посторонним лицам удалось узнать ваши персональные данные, немедленно звоните в банк и блокируйте карту.

ИТАК, для того чтобы обезопасить себя от уловок мошенников, в первую очередь относитесь к своей пластиковой карте также, как и к наличным деньгам, всегда держите её подальше от чужих глаз. Не оставляйте её без присмотра, ведь злоумышленникам достаточно нескольких секунд, чтобы скопировать с карты всю необходимую информацию. Не передавайте банковскую карту третьим лицам, включая родных и близких. Также не стоит записывать ПИН-код от карты в записную книжку или на любую бумажку и уж тем более хранить её рядом с картой. Пользуйтесь только проверенным банкоматом, расположение которого указывается в официальной информации. При малейшем подозрении лучше позвонить в банк и уточнить, не является ли тот или иной аппарат поддельным. Также удостоверьтесь, что к банкомату не подключено какое-либо устройство, которое может передавать персональные данные третьим лицам, и всегда при вводе ПИН-кода прикрывайте цифры от посторонних людей. При возникновении проблем во время работы с банкоматом (например, застряла карта) не слушайте советов подходящих к вам людей, никуда не отходите и совершите звонок в банк для решения возникшей ситуации. Никогда не совершайте покупки в сомнительном интернет-магазине, обязательно посмотрите отзывы об этом ресурсе на других сайтах, свяжитесь с продавцом и задайте интересующие вопросы. Установите антивирусы на свои гаджеты, никогда не скачивайте и не устанавливайте сомнительные программы. Игнорируйте спам, приходящий к вам на телефон или электронный почтовый ящик, не переходите по сомнительным ссылкам и никогда не перезванивайте по указанным номерам телефона. Всегда имейте при себе номер банка для связи в подозрительных ситуациях.

Для того чтобы обезопасить свои сбережения от уловок злоумышленников, учитывая происходящие события, вовсе не нужно избавляться от пластиковой карты и хранить деньги «по старинке». Необходимо просто быть осведомлённым в способах мошенничества и всегда соблюдать правила предосторожности.