Финансы

Охотники за кодами. Ловушка для доверчивых

С развитием технологий растут и «технологии» мошенничества

Дмитрий Рухмалёв

Чаще всего для обмана потенциальной жертвы преступники используют либо sms-сообщения, либо звонки по телефону. По данным управления МВД по Магнитогорску, только за 11 месяцев текущего года было зарегистрировано более 830 фактов мошенничества и более 290 краж с банковских счетов.

Способов обмана с каждым днём становится всё больше. Один из распространённых – мошенник звонит на телефон и представляется оператором мобильной связи, сотрудником банка и сообщает об ошибочно подключенной услуге, для отключения которой нужно сообщить код активации, который во время разговора приходит на телефон. На самом деле, используя данный код, мошенник сможет списать с вашей карты деньги или получить доступ к системе интернет-банка. Ещё один распространённый вариант – поступает звонок с информацией: вашу карту взломали, для сохранности средств нужно немедленно сделать перевод на «безопасный» счёт, иначе вы всего лишитесь. Или приходит сообщение о блокировке карты с требованием перезвонить по указанному номеру телефона.

Мошенники могут представляться не только сотрудниками банков, но и различных государственных учреждений, в том числе социальной защиты, Пенсионного фонда, и под предлогом необходимости начисления денежных средств выманивают персональные данные владельца карты. Часто жертвами мошенников становятся продавцы, размещающие информацию о продаже товаров в открытом доступе. Позвонив по объявлению, мошенники узнают всю информацию о карте продавца для якобы «оплаты» на карту – на самом же деле используют эти сведения для кражи средств. Есть и такой вариант обмана – с поддельного номера приходит сообщение о том, что на ваш счёт была зачислена крупная сумма. Тут же раздаётся звонок – мол, деньги перевели по ошибке, верните на такой-то номер. Не спешите «возвращать» средства – для начала проверьте, а было ли поступление.

Мошенники активно пользуются приёмами психологического давления, подделывают даже сигналы автоответчика и системы ожидания ответа оператора, чтобы потенциальные жертвы поверили, что звонок поступил из официальной организации. Они могут скрывать номера телефонов, подделывая их под реальные номера банков

О правилах безопасности, которые необходимо соблюдать, чтобы не попасться на уловки злоумышленников и не стать жертвой телефонных мошенников, мы попросили рассказать **старшего вице-президент Банка «КУБ» (АО) Александра Лазуткина:**

– Как ни печально, в последнее время всё чаще случаются ситуации, когда держатели карт становятся жертвами мошенников. И какими бы надёжными ни были современные системы безопасности банков и платёжных систем, всё же многое зависит от действий самих пользователей карт.

Александр Лазуткин

– Александр Анатольевич, есть какие-то правила безопасного использования банковских карт? Что прежде всего нужно соблюдать, чтобы не попасться мошенникам?

– Основное правило – никогда и никому не сообщайте реквизиты своей банковской карты – это конфиденциальные персональные сведения, которые следует хранить в тайне. К ним относятся: PIN-код, код CVV2/CVC2, код 3D-Secure, логин или пароль от интернет-банкинга.

Расшифрую термины: PIN-код – это персональный номер, который позволяет получать доступ к своему карточному счёту через дистанционные устройства (например, банкомат). Код CVV2 или CVC2 – код безопасности карты платёжной системы Visa или Mastercard. Эти коды размещены на оборотной стороне карты (после последних четырёх цифр номера карты). Технология 3D-Secure предполагает однократную регистрацию карты на сайте банка и подтверждение каждой покупки в сети Интернет заданным вами кодом.

Будьте бдительны, предоставляя информацию о карте для совершения перевода или платежа. Помните, что для совершения перевода достаточно сообщить только номер карты или счёта. При оплате покупок в Интернете потребуется номер карты, срок её действия, имя владельца и CVV2/CVC2–код, код 3D-Secure. Если покупка совершается с чужого компьютера, после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились. В остальных случаях перечисленную информацию следует хранить в тайне.

– Эти сведения никогда не будет запрашивать даже реальный сотрудник банка?

– Банк ни при каких условиях не вправе требовать от вас код или пароль идентификации. Сотрудникам банка эти данные не нужны, а вот мошенникам они откроют доступ к вашим сбережениям.

– А что же делать, если поступил звонок или sms от представителя банка, например, о несанкционированном списании средств с карты?

– В первую очередь, убедитесь, что это звонок с официального банковского номера. Он всегда указан на оборотной стороне карты или на официальном сайте банка. Если же вам поступил звонок с официального номера и есть подозрение, что вы разговариваете с мошенником, необходимо уточнить контактные данные сотрудника, немедленно положить трубку, вручную набрать номер банка и озвучить специалисту контакт-центра свою ситуацию. Напомним, что обратиться по телефону контакт-центра Кредит Урал Банка +7 (3519) 248 933 можно круглосуточно по всем вопросам, связанным с использованием и обслуживанием карты.

Также никогда не переходите по неизвестным ссылкам из sms-сообщений и не перезванивайте по сомнительным номерам. Даже если ссылка в сообщении кажется вам надёжной, а телефон знакомым, лучше не полениться и сверить адрес с доменным именем официального сайта организации, а номер проверить в официальных источниках. Банки осуществляют sms-рассылку с определённых номеров. Кредит Урал Банк направляет sms-сообщения только с номера CREDITURAL.

По всем вопросам обслуживания нужно обращаться только в банк, выдавший вам карту.

– Как Кредит Урал Банк защищает своих клиентов от мошенников?

– Мы со своей стороны делаем всё, чтобы проведение банковских операций было не только удобным, но и максимально безопасным. В системе дистанционного обслуживания «КУБ-Direct» действует четырёхфакторная аутентификация пользователя, мы используем современные технологии и постоянно совершенствуемся с учётом актуальных рисков и угроз. Но, несмотря на высокую степень защиты и уровень безопасности используемых систем, настоятельно рекомендуем клиентам соблюдать основные правила информационной безопасности: хранить в тайне платёжные реквизиты своей банковской карты, не выкладывать в сети Интернет данные карты и не выполнять никаких действий с картой, предлагаемых по телефону. Помните, безопасность ваших денежных средств – всегда в ваших руках!

Мария Митлина

Мошенничество

Очки вместо видеокамеры

Пресс-служба УМВД России по Магнитогорску сообщает о недавних случаях мошенничества с использованием сети Интернет.

В одном из преступлений пострадал 39-летний магнитогорец. Обратившись в дежурную часть отдела полиции «Правобережный», мужчина пояснил, что на одном из сайтов прочёл сообщение о 50-процентной скидке в рамках акции «Чёрная пятница», в том числе на видеокамеры для подводных съёмок. Пообщавшись с продавцом, он сделал заказ и вскоре в почтовом отделении получил посылку. Оплатив, открыл, но вместо видеокамеры в ящике лежали виртуальные очки и фонарик.

Он оказался не единственной жертвой мошенников, среди потерпевших ещё пять магнитогорцев. Двадцатипятилетняя жительница города перевела на банковский счёт мошенников 14 тысяч рублей. Она не стала перезванивать своей подруге, которая якобы просила занять деньги. Вскоре выяснилось, что интернет-страничку подруги взломали, финансовая помощь ей не требовалась и денежные средства она не получала.

Пятнадцать тысяч рублей за колёса, которые так и не поступили адресату, заплатил 35-летний магнитогорец. А 40-летняя женщина, решив сделать подарок сыну, заказала через Интернет сотовый телефон. Получив товар в почтовом отделении, заплатила восемь тысяч рублей, но вместо гаджета в коробке оказался обычный кнопочный телефон.

На уловку жуликов попался и 58-летний магнитогорец: поверил сообщению, что ему полагается «кэшбэк» в размере 11 тысяч рублей. Женский голос убедил его продиктовать конфиденциальную информацию о банковской карте, и пока в телефонной трубке играла музыка, у него с банковского счёта похитили 57 тысяч рублей.

Ещё один сценарий обмана позволил провести 39-летнюю женщину. Потерпевшей поступила информация, что на неё оформлен кредит: чтобы его закрыть, необходимо установить программу удалённого доступа. Женщина выполнила указания мошенников, в результате лишилась 13 тысяч рублей.

Пресс-служба УМВД предупреждает: мошенники не применяют новых методов обмана, а пользуются доверчивостью горожан. Чтобы не стать жертвой, следует проверять информацию, заказывать вещи на проверенных сайтах и не при каких обстоятельствах не называть секретные данные банковских карт.

Законодательство

Коллекторов ограничат в правах

Официальные посредники между кредитором и должником окончательно потеряют доступ к долгам за жилищно-коммунальные услуги.

Об этом газете «Известия» рассказал глава комитета Госдумы по финансовому рынку Анатолий Аксаков. По его словам, в начале следующего года будет разработан соответствующий законопроект.

С лета 2019 года коллекторов лишили права покупать задолженности граждан по коммунальным платежам, однако, отмечает издание, взыскатели обходят запрет благодаря агентскому договору, без переуступки прав требования и с фиксированным процентом с возвращённых денег.

12 ноября стало известно, что задолженность россиян по платежам за ЖКУ достигла 1,3 триллиона рублей. Особенно остро проблема стоит в Северо-Кавказском федеральном округе, в частности, в Дагестане.

Ранее замминистра строительства и ЖКХ Максим Егоров объяснил задолженность россиян за ЖКУ финансовой безграмотностью. По его мнению, у граждан отсутствует культура потребления ресурсов.

Криминал

Иномарку вернули хозяину

В дежурную часть отдела полиции «Орджоникидзевский» обратился 37-летний магнитогорец. Мужчина заявил о похищении иномарки, которая была припаркована рядом с домом. Причинённый ущерб составил более миллиона рублей.

Сотрудники уголовного розыска УМВД России совместно с сотрудниками уголовного розыска ОП «Орджоникидзевский» задержали подозреваемых в совершении кражи: троих жителей Орска и Челябинска 1971, 1977, 1964 годов рождения. Мужчины не имеют постоянного места работы, ранее все они привлекались к уголовной ответственности.

Отделом по расследованию преступлений на территории, обслуживаемой ОП «Орджоникидзевский», возбуждено уголовное дело по признакам состава преступления, предусмотренного частью 4 статьи 158 УК РФ – кража. Максимальное наказание статьи предусматривает лишение свободы на срок до десяти лет. Подозреваемым избрана мера пресечения в виде заключения под стражу. Похищенная иномарка изъята.