Информация

о наиболее распространенных видах мошенничеств в сфере информационно-телекоммуникационных технологий и основных мерах предосторожности

ОСНОВНЫЕ СХЕМЫ МОШЕННИЧЕСТВ:

«ВАША КАРТА ЗАБЛОКИРОВАНА»

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходят сообщения следующего характера: «Ваша банковская карта заблокирована. **Инфо по телефону...» «Операции по карте №…….. приостановлены. Подробнее по номеру телефона....».** В сообщениях предлагается бесплатно позвонить на определенный номер для получения подробной информации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Мошенники осуществляют СМС - рассылку на различные номера телефонов и ждут звонка. Когда Вы звоните по указанному телефону, Вам отвечает мошенник, который представляется сотрудником службы безопасности банка и под различными предлогами (разблокировка карты, отмена подозрительных операций по Вашей карте, которых Вы не совершали, возврат денежных средств, похищенных с Вашей карты мошенниками, сбой обслуживания карты и прочее) пытается выяснить у Вас номер карты и пароли доступа, поступающих в СМС оповещениях.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Предупреждаем: никому и ни при каких обстоятельствах не сообщайте реквизиты Вашей карты, ПИН-код, одноразовые пароли доступа, которые приходят на телефон и позволяют войти в мобильный банк, а также цифры, указанные на оборотней стороне Вашей карты (CVC2, CVV2 коды)! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Относитесь к ПИН-коду как к ключу от сейфа с Вашими средствами! Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери! Единственно правильный номер банка указан на оборотней стороне Вашей карты. Для того чтобы убедиться, что Вашим деньгам ничего не угрожает достаточно позвонить в клиентскую службу поддержки банка или обратиться лично в банк.

Внимание! Ни при каких обстоятельствах не сообщайте свои пароли никому, включая сотрудников Банка, не перезванивайте на номер мобильного телефона, указанный в поступившем СМС-сообщении от Банка, не предоставляйте информацию о реквизитах карты (номере карты, сроке ее действия, ПИН-коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС-сообщений, а также сотруднику банка, не проводите через банкомат никакие операции по инструкциям, полученным по телефону.

Специалисты банков никогда не запрашивают у клиентов информацию о паролях из СМС, от интернет-банка и серийный код карты, так как им эти сведения и так известны.

«НОВЫЙ ВИД МОШЕННИЧЕСТВА»

Это мошенничество основано на возможности подменять любой номер телефона при звонке с ip-телефонии. Вам могут позвонить с номера вашего близкого и сообщить, что он попал в беду (или, например, задержан полицией) и начать требовать деньги, для решения вопроса. Могут позвонить с телефона вашего банка и

представившись сотрудником службы безопасности выманить данные Вашей карты, рассказав, например, о взломе вашей карты и попытках несанкционированного списания денежных средств, а потом уже узнать у вас всю нужную информацию.

Пожалуйста запомните, мошенники могут подставить ЛЮБОЙ номер. Если вы видите при входящем звонке номер вашего банка, страховой компании, государственной организации, друга или родственника, это НЕ ОЗНАЧАЕТ, что вам звонит действительно тот, чей это номер. Будьте осторожны!

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и самостоятельно перезвонить на абонентский номер близкого человека. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. В случаи если звонили со стационарного номера телефона банка, для того чтобы убедиться, что Вашим деньгам ничего не угрожает достаточно позвонить в клиентскую службу поддержки банка или обратиться лично в банк.

«УДАЛЕННЫЙ ДОСТУП»

Это когда жертва в телефонном режиме, под руководством мошенников установила приложение и предоставила злоумышленникам удаленный доступ к мобильному устройству, и тем самым дают возможность беспрепятственно завладеть персональной информацией и в последующем похитить деньги со счетов через мобильный банк.

КАК ЭТО ОРГАНИЗОВАНО:

Преступник представляется сотрудником банка и сообщает о выявлении вредоносного программного обеспечения на мобильном устройстве клиента. Сообщает, что для его устранения нужно предоставить доступ к устройству. Жертве необходимо скачать на мобильный телефон программу удаленного доступа — TeamViewer, Anydesk или другую, после установки лжесотрудник банка просит клиента назвать код, отображающийся в приложении. Мошенник вводит этот код в программу на своем устройстве. После того как жертва предоставляет все разрешения, злоумышленник получает полный доступ к персональным данным мобильного устройства в том числе и к личному кабинету мобильного банка, и от лица жертвы осуществляет операции по банковским счетам, в том числе имеет возможность оформления онлайн заявки и в последующем получения кредита.

Поэтому нужно запомнить, что настоящие сотрудники банка никогда не попросят:

- Сообщить им код подтверждения операции.
- Установить программы на мобильный телефон, тем более с функцией удаленного доступа.
- Перевести или через банкомат внести ваши деньги на счета третьих лиц.

«РОДСТВЕННИК В БЕДЕ»

КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует перечислить на счет либо привезти в оговоренное место и передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный телефонных разговор вплоть до получения денег.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Следует понимать: если незнакомый человек звонит Вам и требует взятку – это мошенник. Если вы разговариваете, якобы, с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда. Обращаем ваше внимание на то, что требование взятки является преступлением.

«КУПЛЯ-ПРОДАЖА ТОВАРОВ В ИНТЕРНЕТЕ»

Очень большое распространение в последнее время приобрел такой вид мошенничества как обман покупателя или продавца, при совершении сделок через различные интернет – сайты. При совершении данного вида мошенничества могут быть использованы различные социальные сети, группы и интернет-магазины, основной целью преступника является получение информации о карте, для завладения Вашими деньгами.

КАК ЭТО ОРГАНИЗОВАНО:

Вы размещаете объявление на каком-либо сайте о продаже товара. Вам поступает звонок от якобы покупателя, который сообщает о готовности купить товар. При этом под различными предлогами, например, для зачисления задатка или полной стоимости товара, выясняет у Вас номер карты и CVC-код, расположенный на оборотной стороне банковской карты, срок его действия, либо просит сообщить пароли и коды доступа, полученные в СМС – сообщении, что даст преступнику возможность получить доступ к Вашим счетам.

Другой пример: Вы вступаете с продавцом в переписку или звоните по телефону, желая купить интересуемый товар. Преступник в ходе беседы сообщает, что для отправки товара Вам необходимо оплатить его полную (частичную) стоимость. После перечисления денежных средств на абонентские номера, банковские карты, либо электронные счета, преступники скрываются, не выполняя свои обязательства.

КАК ПОСТУПИТЬ В ТАКОЙ СИТУАЦИИ:

Оплачивайте товар только после того как Вы его получили на почте или через курьерскую службу. Никогда не сообщайте реквизиты карты, ПИН-код и пароли доступа из СМС – сообщений.

Вы должны знать, что покупатель, который готов оплатить товар, даже не увидев его, является мошенником. Не соглашайтесь оплачивать товары и услуги путем безналичного расчета даже через якобы официальные интернет-сайты.

«ВЗЛОМ СТРАНИЦЫ В СОЦИАЛЬНОЙ СЕТИ»

Еще один распространенный вид мошенничества, на который попадается, как правило, молодое поколение.

КАК ЭТО ОРГАНИЗОВАНО:

Преступник путем взлома получает доступ к странице Ваших знакомых, родственников или друзей в социальной сети (ВКонтакте, Одноклассники и т.д.). От имени друга, родственника или знакомого Вам приходит сообщение с просьбой

занять деньги в долг, либо под различными предлогами выясняют реквизиты Вашей карты, пароли и коды из СМС-сообщений. После того как Вы сообщили преступникам реквизиты своей карты и пароли они получает доступ к Вашим счетам.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Следует связаться со знакомыми или родственниками по телефону и выяснить действительно ли им нужна помощь. Ни в коем случае не сообщайте реквизиты Вашей банковской карты.

«ВРЕДОНОСНАЯ ПРОГРАММА (ВИРУС)»

В данном случае преступники используют вредоносную программу, как способ завладения Вашими деньгами. Данная программа устанавливается на телефон при получении СМС или ММС сообщений с различными ссылками, а также при входе на различные сайты в интернете. Особо следует обратить внимание на то, что подобные сообщения могут приходить от знакомых, родственников, которые записаны в Вашей телефонной книге, а также в сообщениях может быть указано Ваше имя или другие персональные данные.

КАК ЭТО ОРГАНИЗОВАНО:

На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». Или другой пример «Алексей, привет! Выложила наши фотографии здесь…., посмотри». При переходе по указанному адресу на телефон скачивается вирус. Либо заражение может произойти при посещении различных сайтов в интернете.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУЦИИ:

Следует установить на телефоне антивирусное программное обеспечение, не следует открывать сообщения с вложениями, перезванивать на номер, указанный в полученном сообщении.

«ОШИБОЧНЫЙ ПЕРЕВОД»

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS-сообщение о поступлении средств на счет. Сразу после этого поступает звонок от мошенников, которые излагают легенду, что они по ошибке перевели деньги и просят их вернуть.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Мошенники пытаются таким образом завладеть Вашими деньгами. Естественно никакой ошибки не было. Денег Вам не присылали.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Советуем Вам не поддаваться на обман. Если Вас просят перевести, якобы, ошибочно переведённую сумму, напомните, что для этого используется чек.

«СМС-ПРОСЬБА О ПОМОЩИ»

СМС-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» и т.д.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Следует запомнить, что на СМС с незнакомых номеров реагировать нельзя, это могут быть мошенники.

«САЙТ-ДВОЙНИК»

КАК ЭТО ОРГАНИЗОВАНО:

Преступник создает (использует) сайт, адрес которого и внешнее оформление страницы идентичны официальному сайту, например, сайту банка. Далее происходит рассылка сообщений потенциальным жертвам. Если Вы осуществите вход на «сайт-двойник», то он предложит Вам, ввести свои данные для входа в «личный кабинет» банка (логин и пароль), которыми и могут воспользоваться злоумышленники для получения доступа к Вашим счетам. Другой пример: преступник создает сайт-двойник, отличающийся от оригинального сайта реквизитами. Вы, желая совершить покупку на данном сайте через интернет, оплачиваете стоимость товара, либо вносите предоплату, после чего преступник удаляет сайт, а указанные телефоны становятся недоступными.

КАК ПОСТУПИТЬ В ТАКОЙ СИТУАЦИИ:

Главная цель мошенников – это логины и пароли, а также данные банковских карт. Следует запомнить, что ни один серьезный интернет-сервис никогда не рассылает письма с просьбами о вводе логина, пароля и личных данных своим клиентам. Следует обращать внимание на уведомления Вашего браузера, если имеется предупреждение о переадресации на сторонний ресурс, не следует его игнорировать!

«КОМПЕНСАЦИЯ ЗА НЕКАЧЕСТВЕННЫЙ ТОВАР, УСЛУГУ»

Жертвами данного вида мошенничества, как правило, являются пожилые люди, пенсионеры. В данной схеме, как правило, действует преступная группа, участники которой могут представляться сотрудниками государственных банков и ведомств (Центрального Банка РФ, Следственного комитета, Прокуратуры). Преступник осуществляет телефонный звонок на номер потерпевшего и сообщает, что ему положена компенсация за ранее приобретенные некачественные товары, так называемые БАДы, либо оказанные услуги, при этом для получения компенсации необходимо заплатить определенную сумму (комиссию, налог, пошлину, оплата доставки, разблокировка ячейки для зачисления компенсации и прочее).

Другой пример мошенничества: преступник осуществляет звонок потерпевшему и, представляясь сотрудником правоохранительных органов, сообщает, что счета компании, в которой ранее потерпевший покупал продукцию арестованы и заморожены и ему положена компенсация, для получения которой необходимо заплатить определенную сумму денег. После того как потерпевший перечисляет необходимую сумму денег, преступники продолжают звонить ему и под различными предлогами просят деньги необходимые для выплаты компенсации.

ПОЛИЦИЯ ПРИЗЫВАЕТ не переводить деньги на сомнительные счета по просьбе незнакомцев. Помните, если взамен обещанной компенсации вас просят заплатить некоторую сумму в качестве налога, комиссии или оплатить прочие услуги, то вас пытаются обмануть. Незамедлительно обращайтесь в правоохранительные органы и сообщите о данном факте.

«БРОКЕРСКИЕ КОНТОРЫ»

Для того, чтобы не потерять свои деньги при выборе брокерской компании необходимо обращать внимание на следующие признаки, которые характеризуют компанию-мошенника: обещание высоких процентов, отсутствие регистрации, обещание стабильной прибыли новичкам- трейдерам.

Перед тем, как доверить свой капитал, внимательно изучите не только интернет-ресурсы, но и официальную информацию о брокере и его регламент.

ВАЖНО! Помните, что инвестирование, предлагаемое на условиях брокерской компании, всегда является высоко рискованным даже при наличии безупречной репутации брокерской компании.

«КРИК О ПОМОЩИ»

Один из самых циничных способов хищения денежных средств, является выкладываемая в социальных сетях душераздирающих историй о борьбе с болезнью малолетних детей за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на указанные реквизиты.

Мы не призываем отказывать в помощи всем, кто просит! Но! Прежде чем переводить свои деньги, проверьте - имеются ли контактные данные для связи с родителями (родственниками, опекунами) ребёнка. Позвоните им, найдите их в соцсетях, пообщайтесь и убедитесь в честности намерений.

Указанный список не является исчерпывающим, так как возможны иные способы и виды мошенничеств, а также их изменение или комбинирование. Во всех случаях обращения с мобильными устройствами, банковскими картами и компьютерами необходимо соблюдать меры предосторожности, которые помогут обезопасить себя и своих близких от мошенников.

Вы получили электронное сообщение о том, что вы выиграли приз и вас просят перевести деньги для получения его получения?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по привлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах?

НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности продавца.

Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.

Вы хотите приобрести авиабилеты, туристические путевки, через Интернет?

НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов.

Закажите билеты и туристические путевки через сайты авиакомпании или агентства, положительно зарекомендовавших себя на рынке. Не переводите деньги на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании или туристического агентства.

Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

НИКОГДА не переходите по ссылке, указанной в сообщении.

Помните, что, перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

Общаетесь в интернете и имеете аккаунты в соцсетях?

НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.

БУДЬТЕ БДИТЕЛЬНЫ – НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Помните! Если Вы или Ваши близкие стали жертвами мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в ближайший отдел полиции.