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

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

«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.

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.

Полиция Адыгеи
01.мвд.рф
Facebook
Одноклассники
Twitter
ВКонтакте
YouTube
Telegram
mvd01rus

МВД по Республике Адыгея предупреждает!!!

ОБМАН В ИНТЕРНЕТЕ

ВНИМАНИЕ: МОШЕННИКИ!

➡ ЗАПОМНИТЕ САМИ и РАССКАЖИТЕ БЛИЗКИМ!

ФИНАНСОВЫЕ ПИРАМИДЫ

Мошенники маскируют финансовые пирамиды под инвестиционные компании или коммерческие организации, с высокой доходностью. Помните, что вложив деньги в сомнительную компанию, вы соглашаетесь с условиями оферты и можете потерять свои деньги.

ВЗЛОМ СТРАНИЦЫ В СОЦИАЛЬНЫХ СЕТЯХ

Мошенники путем взлома получают доступ к странице ваших родственников или друзей в соцсетях. От их имени просят пополнить счет телефона, занять деньги либо выясняют реквизиты вашей карты. Это - ОБМАН!

Не сообщайте реквизиты банковских карт чужим людям!

САЙТ-ДВОЙНИК

(заказ билетов, путевок, товаров через Интернет)

Мошенники используют сайт организации, адрес которого и оформление страницы почти идентичны официальному сайту (например авиакомпании или туристического агентства). Не торопитесь, обратите внимание на дату создания, почитайте отзывы и не осуществляйте сделки через непроверенные сайты. Не переводите деньги на электронные кошельки и неопределенные счета.

КУПЛЯ-ПРОДАЖА ТОВАРОВ В ИНТЕРНЕТЕ

Вам сообщают, что готовы купить (продать) товар по объявлению, размещенному на сайте Авито, Юла, Авто.ру и др. Для осуществления сделки (с целью внесения предоплаты или оплаты полностью) просят сообщить реквизиты банковской карты, ПИН-код, пароль из СМС-сообщения. Будьте внимательны, если у вас приобретают имущество без предварительного просмотра или продают по заниженной цене, возможно – это ОБМАН!

Возможны иные способы и виды мошенничества. **БУДЬТЕ БДИТЕЛЬНЫ!!!**

Полиция Адыгеи: 02 (102/112 - с мобильного)