ПАМЯТКА
информация о видах и способах мошенничеств и иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Как не стать жертвой «мобильного» мошенничества

Злоумышленники могут обратиться к Вам:

- под видом сотрудников полиции, о нарушении их близкими родственниками законов, с целью передачи Вами денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившийся ситуации.

Не продолжайте разговор, не позволяйте себя убедить.

Вам звонит мошенник! Обратитесь в полицию!

- о блокировке банковской карты путем рассылки SMS-сообщений, а так же о переводе денежных средств за покупку товара по объявлению и последующего информирования о необходимости дальнейшего введения ряда команд.

Вам звонит мошенник. Не предоставляйте злоумышленникам сведения о Вашей карте. Обратитесь в банк, обслуживающий Вашу банковскую карту, в банке Вам помогут решить Вашу проблему.

- о сообщении Вам, якобы из поликлиники или больнице, что у Вас или у Ваших родственников обнаружили страшный диагноз и чтобы вылечить болезнь необходимо перевести деньги за лекарства.

Прервите разговор. Вам звонит мошенник. Медицинское учреждение принимает денежные средства после заключения соответствующего договора в письменном виде, при Вашем личном присутствии. Свяжитесь с Вашим родственником, позвоните в больницу.

Не сообщайте информацию по вашей банковской карте и не переводите денежные средства мошенникам.

Обратитесь в полицию!

- о получении СМС-сообщений с неизвестных номеров о выигранном призе, с просьбой положить деньги на телефон, или вернуть деньги, так как они были переведены ошибочно.

Это обман! Не отвечайте на сообщение, не присылайте информацию по карте и не переводите денежных средств.

1.

Никому нельзя сообщать реквизиты своей банковской карты, в том числе сотруднику банка, об этом всегда информируют банк при получении пароля к карте, в последствии необходимо лично обратиться в ближайшее отделение банка, с целью выяснения возникших проблем с банковской картой.

2.

Различные компенсации выплачиваются гражданам только при их личном письменном обращении, никаких процентов за выплату компенсации платить не надо.

Это мошенник!

3.

Настоящий врач никогда не будет звонить вам по телефону и сообщать о страшном диагнозе или просить перевести деньги за лекарства.

4.

В случае получения СЬС- сообщений с неизвестных номеров, помните это мошенники! Человек не может выиграть приз не участвуя в лотереях, родственники не будут высылать СМС-сообщения с неизвестных номеров.

Это мошенники!

Как не стать жертвой мошенничества, используя сеть Интернет.

Злоумышленник, с целью хищения ваших денежных средств, размещает в сети Интернет объявление о продаже какого-либо объекта (телефон, машина, квартира) по заниженной цене и оставляет свои контактные данные. После того, как Вы собираетесь приобрести товар, связываетесь с мошенником, он сообщает, что для покупки необходимо внести предоплату (на расчетный счет, счет, яндекс-деньги, вебмани и т.д.).

Наиболее часто встречающимися площадками для размещения подобных объявлений являются сайты социальных сетей «В контакте», «Одноклассники», «Instagram», также такими сайтами могут выступать ресурсы бесплатных объявлений «Авито», «Юля» и «auto.ru». Злоумышленник объясняет внесение предоплаты тем, что живет в другом регионе и отравить товар сразу после того, как удостовериться в уплате за товар. Злоумышленник может выслать копию паспорта (поддельную).

Также, распространенным способом мошенничества в сети Интернет, является создание сайтов интернет-магазинов. Злоумышленник по электронной почте высылает договор, который заполняете заказчик, после чего просит внести предоплату за товар. Встречается создание сайтов-клонов на которых искажены реквизиты получателя. Различие может заключатся только в доменном имени (например: оригинальный сайт «tech-point.ru» и двойник «tex-point.ru»).

Интернет-магазины с хорошей репутацией работают без предоплаты, товар на дом привозит курьер, только после осмотра и проверки товара продавец платить деньги;

прежде чем заказать товар в Интернете, почитайте отзывы на разных сайтах о данном Интернет-магазине или виртуальном продавце, как правило, вы сразу обнаружите отрицательные отзывы либо их отсутствие о выбранном Вами Интерне-магазине (следует сделать вывод о коротком периоде его существования);

внимательно читайте названия Интернет-магазина, пробуйте зайти на его сайт с других сайтов, тем самым Вы сразу обнаружите сайты-клоны;

избегайте покупки товара по предоплате;

если цена товара гораздо ниже цены как в обычных розничных магазинах, так и в других Интернет-магазинах, либор на рынке в целом (например, при продаже автомашины по заниженной стоимости), задумайтесь!;

запрос покупателем, якобы для перечисления предоплаты, либо оплаты за товар информации не только о шестнадцатизначном номере карты (требуется исключительно только он), срок ее действия, данных владельца и трехзначном коде проверки подлинности карты, расположенном на оборотной стороне на полосе для подписи держателя карты также является одной из схем действия мошенников. Не сообщайте при покупке товара сведений о Вашей банковской карте.

Как не стать жертвой мошенничества с банковскими картами!

При использовании услуги «Мобильный банк»:

В случае потреи мобильного телефона с подключенной услугой «мобильный банк» или мобильным приложением «Сбербанк Онлайн» следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в Контактный центр Банка для блокировки услуги «Мобильный банк» и/или «Сбербанк Онлайн».

При смене номера телефона, на который подключена услуга «Мобильный банк», необходимо обратиться в любой филиал (внутреннее структурное подразделение), с целью отключения услуги «мобильный банк» от старого номера и подключения на новый.

Не следует оставлять свой телефон без присмотра, что исключить несанкционированное использование мобильных банковских услуг другими лицами.

Не подключайте к услуге «Мобильный банк» абонентские номера, которые Вам не принадлежат, по просьбе третьих лиц, даже если к Вам обратились от имени сотрудников Банка.

При пользовании банковскими картами:

С целью избежать несанкционированных действий с использованием карты, необходимо требовать проведения операций с ней только в Вашем присутствии, никогда не позволять уносить третьим лицам карту из поля Вашего зрения.

В случае обращения какого-либо лица лично, по телефону, в сети «Интернет», через социальные сети или другим способом, которое под различными предлогами пытается узнать полные данные о Вашей банковской карте: шестнадцатизначном номере, сроке действия, данных владельца, трехзначном коде проверки подлинности карты и т.д. (паролях или другой персональной информации), будьте осторожны – это явные признаки противоправной деятельности. При любых сомнениях рекомендуется прекратить общение и обратиться в банк по телефону, указанному на обратной стороне банковской карты.

Не следует прислушиваться к советам третьих лиц, а также отказаться от их помощи при проведении операций. В случае необходимости, обращаться к сотрудникам филиала банка или позвонить по телефонам, указанным на устройстве или обратной стороне карте.

Во избежание использования карты другим лицом, следует хранить ПИН-код отдельно от карты, не писать ПИН-код на карте, не сообщать ПИН-код другим лицам (в том числе родственникам)

Не переходите по ссылкам и не устанавливайте приложения/обновления, пришедшие по SMS/MMS/электронной почте/мессенджерам (Вайбер, ВацАп и др.), в том числе от имени Банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.

НЕ ВЕРЬТЕ ПОДОБНЫМ СООБЩЕНИЯМ, НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ, НЕ ОТВЕЧАЙТЕ НА СООБЩЕНИЯ.

Сообщения, которые присылают мошенники!

Если вы потеряли карту или подозреваете, что она украдена, незамедлительно произведите ее блокировку.

Заблокировать банковскую карту можно разными способами:

По телефону горячей линии

Универсальный способ. Номер для экстренной связи всегда указан на официальном сайте банка. Лучше заранее сохранить номер горячей линии банка в мобильном телефоне, чтобы не разыскивать его в экстренном случае. Оператор службы поддержки попросит назвать паспортные данные, кодовое слово или СМС-код, который пришлет Вам на телефон. После этого он заблокирует карту.

Через мобильное приложение.

Самый быстрый способ, если у Вас есть доступ к Интренету, приложение уже установлено на Вашем телефоне и в нем есть опция по блокировке карте.

В интернет-банке.

Удобно, если у Вас подключен интернет-банкинг и рядом есть компьютер, планшет или смартфон с доступом в интернет. В личном кабинете на сайте банка обычно есть опция «Заблокировать карту». Свое решение надо будет подтвердить кодом из СМС, которое банк вышлет на ваш номер.

По СМС.

Некоторые банки используют систему СМС-команд. На короткий номер банка надо отправить кодовое слово (например, «Блокировка»). В ответ Вы получите код, который надо снова отправить на номер банка, что подтвердить действие. Но лучше заранее уточнить, предлагает ли Ваш банк такую услугу и какие кодовые слова нужно использовать.

В отделении банка.

Если Вы находитесь рядом с офисом банка или потеряли телефон вместе с картой, пишите заявление о блокировке карты в отделении. Но для этого понадобится паспорт.

Сразу после блокировки карты вы можете оставить заявку на выпуск новой. Если будете действовать быстро, у Вас есть большой шанс вернуть

похищенное. Вы можете опротестовать операцию по карте, которую совершили мошенники. Но сделать это нужно не позднее следующего дня после того, как получите от банка уведомление об операции. Чтобы не дать шанса мошенникам украсть Ваши деньги, внимательно отслеживайте все операции по картам. Банк обязан уведомлять Вас обо всех платежах – в Вашем договоре прописано, каким способом он должен это делать.

Лучше всего подключить СМС-оповещения.

Отследить операции по карте Вы можете можете через мобильное приложение или онлайн-банк. Всегда можно получить выписку по счету в отделении банка и иногда через банкомат. Если у Вас украли карту, имеет смысл перепроверить все последние платежи.