КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ЗДРАВООХРАНЕНИЯ
“НОРИЛЬСКАЯ МЕЖРАЙОННАЯ БОЛЬНИЦА № 1”

ПАМЯТКА

Как не стать жертвой мошенников

Мошенники специально оказывают психологическое воздействие на человека таким образом, чтобы он раскрыл личные или финансовые данные, перевел им деньги или даже взял кредит для последующей передачи средств в чужие руки. Они могут неоднократно звонить жертве, в том числе используя технологию подмены телефонных номеров, направлять электронные письма и сообщения со ссылкой на поддельные (фишинговые) сайты как финансовых организаций, так и любых других компаний и маркетплейсов. Злоумышленники всячески пытаются вывести человека из спокойного состояния и отключить у него логическое мышление. Для этого они могут запугивать, торопить и оказывать давление или, напротив, стараться заинтересовать и обрадовать внезапной выгодой. Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Такое психологическое воздействие представляет собой методы социальной инженерии.

Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

Если с неизвестного номера звонит сотрудник Центробанка, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

Не совершайте каких-либо действий по счету, если вам звонят из Центробанка с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

По возможности установите антивирус на все устройства и обновляйте его.
Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос,

получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Сотрудники Банка России, а также государственных и правоохранительных органов никогда не звонят через мессенджеры. Так поступают мошенники, которые представляются в том числе сотрудниками Банка России. Иногда злоумышленники направляют в мессенджер или на электронную почту поддельное удостоверение с логотипом и печатью Банка России. Такие документы иногда содержат имена реальных сотрудников, сведения о которых мошенники могут получить на сайте регулятора или каким-либо другим способом. Высылая фальшивое удостоверение, они рассчитывают добиться доверия, чтобы потом обманом выманить у человека деньги или оформить на него кредит.
Если вам позвонили якобы «работники» Банка России или правоохранительных органов и разговор касается ваших финансов, положите трубку. Никому и никогда не переводите деньги и не сообщайте свои личные и финансовые данные по просьбе незнакомого абонента, кем бы он ни представлялся.

СИТУАЦИИ:

Мне позвонили из полиции и сообщили, что мои персональные данные были скомпрометированы, а деньги могут быть похищены, и предлагают перевести их на специальный счет в Центробанке. Что делать?

Это наиболее распространенная мошенническая схема. Не существует «специальных», «безопасных», «защищенных» или каких-то других счетов, на которые граждане должны переводить деньги в адрес Центрального банка. Злоумышленники упоминают якобы специальный счет в Центробанке, чтобы усыпить бдительность человека. На самом деле счет, реквизиты которого называют мошенники, принадлежит им. Не совершайте никаких действий по своему счету, положите трубку.
Если у вас остались какие-то сомнения, самостоятельно позвоните в банк по номеру телефона, который указан на оборотной стороне карты или на официальном сайте банка

Что делать, если кто-то по ошибке зачислил на мой счет деньги?

Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем вам звонит человек, который по ошибке зачислил деньги, и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, прежде чем переводить кому-то деньги, если поступление все-таки было, обратитесь в свой банк и сообщите об этом. Банк должен сам вернуть ошибочно зачисленные деньги.
Что делать, если приходит сообщение о необходимости подтвердить покупку, которую я не совершал?

Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас данные, чтобы списать с вашего счета средства или подписать вас на ненужный платный сервис. Если вам придет сообщение о необходимости подтвердить покупку — игнорируйте его.

Что делать, если мне звонят из МВД, ФСБ или других правоохранительных органов и просят данные карты или перевести деньги?

Если вам звонят из банка, полиции или другой организации и просят совершить финансовые операции по счету (перевод, зачисление, в т.ч. на «безопасный» счет и т.д.), немедленно прекратите разговор. Если есть сомнения — позвоните в свой банк и узнайте, все ли в порядке с деньгами.
Зачастую при звонке злоумышленники представляются не только «службой безопасности банка», но и «сотрудниками МВД» или других правоохранительных органов, используют разнообразные приемы, сообщают, например, о якобы проводимых в данный момент мероприятиях по поимке преступников. Будьте бдительны и не выполняйте требования позвонившего. Настоящие сотрудники правоохранительных органов или банка никогда не будут запрашивать у вас данные карты или просить перевести деньги.

Какую именно информацию о своей банковской карте ни в коем случае нельзя сообщать посторонним людям?

Если кто-либо запрашивает у вас номер карты, срок действия, код проверки подлинности карты (три цифры на обратной стороне — CVV или CVC), ПИН-код, а также код из СМС для подтверждения платежей и переводов — это мошенник. Ни в коем случае не сообщайте эти данные в разговоре с незнакомым человеком.
Вы можете указывать номер карты, срок действия, код проверки подлинности карты (CVV или CVC), а также код подтверждения транзакции из СМС только при совершении покупок на проверенных и надежных сайтах — в строке браузера должен быть указан значок замочка
Никогда и никому не сообщайте информацию о ПИН-коде: ее не знает и не должен знать даже банк, в котором вы обслуживаетесь.

На чем играют мошенники, чтобы выманить у вас нужную им информацию?

Есть основные признаки того, что с вами разговаривает мошенник: собеседник активно использует ваше чувство страха (ваша карта заблокирована, вы можете потерять деньги, данные украдены и т.д.), собеседник давит на жажду наживы (пройдите опрос и получите вознаграждение, получите компенсацию, выплату, очень выгодные условия по кредиту или вкладу и т.д.). При этом от вас требуют срочно принять решение и совершить некоторые действия: сообщить персональные данные, проделать какие-то манипуляции с банковской картой. В противном случае вам угрожают потерей денег или возможности получить их.
Имейте в виду: даже если банк действительно зафиксировал попытку несанкционированной операции с вашего счета, он имеет право приостановить эту операцию на срок до двух суток, поэтому настоящий представитель кредитной организации не будет торопить вас принимать решение. Также вас всегда должны настораживать предложения получить легкие деньги, очень выгодные условия по кредитам или депозитам.

Если стали жертвой мошенников – звоните по телефонам: 102 или 112.

Помните, что лучше предупредить правонарушение, чем в результате незнания или доверия оказаться пострадавшим от преступления, потерять денежные средства. Раскрыть преступления данной категории весьма сложно, в связи с тем, что мошенники зачастую работают удаленно (при помощи информационно-коммуникационных средств), впоследствии отключают телефоны, убирают адреса и т.д.).