Уважаемые клиенты!

Кибермошенники обманывают людей в Интернете или по телефону. У них множество легенд и способов обмануть человека, которые всегда сводятся к одному: у человека пытаются выманить данные карты, пароли или коды из СМС, либо провоцируют самостоятельно перевести деньги. Поэтому важно помнить: никогда не сообщайте данные своей карты, пароли из СМС, не переводите деньги на счет по просьбе неизвестного абонента, кем бы он не представлялся. Также никогда не вводите эти данные на сайтах, на которые вы перешли по ссылке из письма или СМС, а еще лучше вообще не переходите на сайты по ссылкам из подозрительных писем.

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 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.

За период пандемии участились случаи финансового мошенничества. Принципиальные схемы обмана клиентов банка не изменились, но изменились способы воспроизведения этих схем. Просим ознакомиться с самыми распространёнными схемами обмана в банковской сфере:

1. Самая распространённая схема обмана, так называемый, звонок «Сотрудника службы безопасности банка». В этом звонке злоумышленники будут просить вас предоставить доступ к вашему устройству с личным кабинетом, передать сведения о банковских картах и (или) счетах, просить перевести ваши средства для их защиты от хищения на другой счёт по реквизитам, которые он вам предоставит, установить дополнительное программное обеспечение

Защититься от таких действий можно завершением звонка сразу же после вопросов о ваших персональных данных, реквизитах карт и счетов, паролях из СМС, кодовых словах, последних совершённых операциях.

2. Вторая схема обмана – вирус в фишинговом письме на электронной почте. Такие письма, зачастую, будут присланы с почтового адреса идентичного официальной почте организации с прикреплённым во вложениях файлом, содержащим вирус, или будут прикреплены ссылки на сторонние сайты.

Для защиты от таких писем:

- внимательно сверяйте официальный адрес Банка и тот, с которого пришло сообщение;

- проверяйте вложения в письме антивирусными программами и утилитами;

- не переходите по ссылкам с доменами, отличными от официального ресурса.

3. Третья схема подразумевает подмену реквизитов реального контрагента на реквизиты мошенника. В этом случае мошенник взламывает электронную почту сотрудника компании-контрагента и отправляет счёт со своими реквизитами на оплату. Могут быть пометки о срочности проведения платежа. Такие сообщения могут быть присланы с максимально похожей на оригинальные адреса электронной почты. Она может отличаться на один или несколько символов от официального почтового адреса. Пример:

– Оригинальная почта – bank@domen.ru, подменная почта – banc@domen.ru.

– Также могут использоваться другие почтовые сервисы: bank@email.com.

Для защиты от данной схемы требуется сверять официальную почту организации и почту отправителя письма. Также рекомендуем обращать внимание на дату регистрации компании. С большей вероятностью она будет зарегистрирована за несколько месяцев назад.

Если есть сомнения в данных контрагента, то свяжитесь с партнёром по телефонной связи и уточните данные по реквизитам.

Дополнительно рекомендуем сделать двухфакторную авторизацию для входа в почту и установить оповещения о входе в ваш аккаунт с других устройств.

4. Создание компании-клона существующей длительный срок на рынке крупной компании.

Мошенники регистрируют организацию с идентичным оригинальной названием, полностью копируют её сайт и корпоративный стиль, все каталоги товаров и услуг, но, с большей вероятностью, цены на их услуги или товары будут ниже, чем в целом по рынку. Далее они действуют от лица этой компании, связываясь с потенциальными клиентами и предоставляя им договоры и счета на оплату с реквизитами, принадлежащими мошенникам.

Чтобы избежать потери средств в данном случае:

– будьте внимательны при взаимодействии с контрагентом, которого нашли самостоятельно или он сам связался с вами;

– проверяйте реквизиты указанной компании на принадлежность ей;

– через поисковую строку проверьте адрес сайта организации, указанный в договоре или письме на наличие негативных отзывов.

– проверьте сайт организации на whois-сервисах. Если регион работы компании будет отличным от региона регистрации сайта, будут несовпадения дат регистрации и создания сайта (к примеру: компания зарегистрирована в 2004 году, сайт в 2021), то это сигнал о том, что вы связались с мошенниками.

Свяжитесь с крупной компанией, за которую выдаёт себя ваш контрагент, если даже по одному из пунктов компания не прошла проверку, и уточните, были ли вам отправлены счета на оплату от лица их организации.

5. Ошибка зачисления денежной суммы.

Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит человек, который по ошибке зачислил вам средства, 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 поступившие по ошибке деньги.

6. Сообщение с подтверждением покупки.

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.

7. Звонок с правоохранительных органов (МВД, ФСБ или др.).

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.

8. Письмо от Банка России, в котором говорится, что на моё имя открыт крупный денежный счёт в иностранном банке, и что я должен оплатить теперь комиссию за её получение. Что это?

Банк России по своей инициативе не направляет гражданам письма, не звонит и не рассылает сообщения. При получении электронных писем о поступлении на ваше имя крупной денежной суммы в иностранном банке или организации, происхождение которой вам неизвестно и/или вызывает сомнения, а также с предложением оплатить комиссию/налог/страховку и т.д. для её получения, настоятельно рекомендуем *не отвечать на такие сообщения и ни в коем случае не переводить деньги, т.к. это распространенный вид мошенничества.*

Также мошенники могут от имени Банка России звонить, рассылать смс/сообщения в мессенджерах с предложением получить компенсацию за купленные ранее лекарственные средства (медицинские приборы, БАДы).

Чтобы не стать жертвами злоумышленников, будьте бдительны, всегда проверяйте информацию на достоверность и не поддавайтесь на провокации.

Во всех случаях, вызывающих подозрение, немедленно обращайтесь в правоохранительные органы!

С уважением, администрация ПАО "НИКО-БАНК".