Уважаемые клиенты!

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.

С уважением, администрация ПАО "НИКО-БАНК".