ИНФОРМАЦИЯ ДЛЯ КЛИЕНТОВ
О мерах по обеспечению информационной безопасности и противодействию мошенничества

Уважаемые Клиенты!

ПАО «НИКО-БАНК» информирует Вас о необходимости соблюдения принципов обеспечения информационной безопасности при использовании корпоративных банковских карт и сервисов дистанционного банковского обслуживания в целях предотвращения несанкционированного доступа к Вашим электронным средствам платежа и мошеннических операций по переводу денежных средств.

Информируем Вас, что в настоящее время для хищения денежных средств у граждан, юридических лиц и индивидуальных предпринимателей злоумышленники используют **все более изощренные сценарии обмана с применением современных технологий**, позволяющих выполнять подмену телефонных номеров, аккаунтов социальных сетей и мессенджеров, использовать для убедительности голос, фото и видео с изображением знакомых Вам людей, руководителей, коллег, партнеров, работников Банка, а также связываться с Вами от имени различных финансовых, правоохранительных, налоговых органов, Банка России, сервиса Госуслуг, операторов мобильной связи (якобы с целью продления договора), партнеров по бизнесу и любых других компаний и маркетплейсов.

Обращаем Ваше внимание, **что в последнее время одной из наиболее популярных схем является «Важное сообщение от «руководителя»**, **полученное в мессенджере с поддельного аккаунта, либо с настоящего аккаунта, который был взломан. Злоумышленники могут использовать WhatsApp, Telegram, Viber, VK и т.п.**

Злоумышленник выдает себя за руководителя, связывается с подчиненным через мессенджеры, подготавливая жертву к звонкам или сообщениям от «куратора по безопасности», «полиции», «профильного ведомства» или другого государственного органа. Дальнейшее взаимодействие с такими «кураторами» приводит к переводам денежных средств на счета, принадлежащие мошенникам.

Детально данный сценарий выглядит так:

1. Мошенники создают в мессенджерах поддельные аккаунты: с реальной фотографией и ФИО руководителя (председателя правления, директора компании, главврача больницы, ректора учебного заведения, начальника какого либо подразделения и т.п.) либо непосредственно взламывают мессенджер руководителя. С этого аккаунта пишут сотруднику организации.
2. Фейковый руководитель сообщает, что скоро этому сотруднику должны позвонить из уполномоченного органа по очень важному вопросу. Подчеркивается, что подчиненный должен следовать инструкциям, полученным по телефону, и не сообщать никому об этом разговоре.
3. Подготовленный к будущей беседе с «представителем власти» сотрудник теряет бдительность, и, не желая быть уволенным или наказанным, выполняет все, что ему скажут.
4. Цель таких звонков – заставить жертву перевести деньги, а также собрать сведения, которые будут использовать для дальнейших атак, о других сотрудниках или компании.

Нельзя недооценивать злоумышленников:

С развитием информационных технологий данная схема также совершенствуется мошенниками, которые начинают использовать технологию **Deepfake (**Дипфейк).

Дипфейки представляют собой поддельные изображения, аудио- и видеозаписи, созданные с использованием технологий машинного обучения и искусственного интеллекта. Получается реалистичный, но фальшивый контент, который можно

применять в мошеннических схемах, при распространении дезинформации, нарушении неприкосновенности частной жизни и многом другом.

Данную технологию злоумышленники используют для подделки голосов руководителей компаний или финансовых учреждений и последующего проведения мошеннических операций. Также дипфейки начинают внедрятся мошенниками в схемы социальной инженерии и обмана людей, когда мошенники подделывают голос родственника или друга, коллегу, либо другого знакомого человека, чтобы попросить финансовую помощь или раскрыть конфиденциальную информацию.

Напоминаем!

Схемы мошенников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Такое психологическое воздействие представляет собой методы социальной инженерии.

Даже если собеседник представляется именем знакомого или вышестоящего руководства, не спешите выполнять его требования. Убедитесь, что аккаунт на самом деле принадлежит человеку, которого вы знаете, и не был взломан.

Кем бы ни представлялись звонящие, никогда не переводите деньги по их указаниям. Никто не имеет полномочий требовать этого от вас.

Не поддавайтесь панике. Злоумышленники 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 пытаются вывести человека из спокойного состояния и отключить у него логическое мышление, запугивая, торопя, запрещая кому-либо рассказывать о разговоре и оказывая давление на жертву или, напротив, стараясь заинтересовать и обрадовать внезапной выгодой. Возьмите паузу, сообщите о подозрительных звонках в банк по официальному номеру или обратитесь в офис. Позвоните на мобильный телефон своему руководителю и обсудите с ним ситуацию.

Также обращаем Ваше внимание на активное использование злоумышленниками различных способов получения доступа к аккаунтам портала Госуслуг. Сценарии обмана могут быть самые разные, но цель их одна – узнать код из СМС, направленный на Ваш номер телефона и получить доступ к учетной записи в личном кабинете портала Госуслуг. Основные распространенные сценарии, используя которые мошенники связаться с Вами:

- под видом сотрудника портала Госуслуг;
- звонок оператора связи для продления действия договора на обслуживание;
- от имени социального фонда по вопросам получения субсидий, социальных выплат, перерасчета пенсии или срока трудового стажа;
- от имени медицинских учреждений;
- электронные сообщения от налоговых органов по вопросам получения налоговых вычетов, либо срочного предоставления налоговых деклараций.
- от имени правоохранительных органов или Банка России и т.д.

Особого внимания заслуживает вариант **«Вам создан сертификат электронной подписи на портале «Госуслуги»**. И предлагаются варианты его скачивания и активации: либо пройти по ссылке и подтвердить, либо пройти по ссылке и отказаться. А также одним из вариантов является необходимость сообщить код из СМС для активации и скачивания сертификата. В связи с тем, что электронная подпись начинает активно использоваться в разных сферах жизни, необходимо понимать и помнить, что на Госуслугах действительно может быть информация о выпущенных сертификатах электронной подписи, которая передается туда Удостоверяющими центрами их выпустившими, но **скачивание их с портала невозможно и активация их не требуется.**

Любой диалог со злоумышленником, который изначально может не иметь подозрительных признаков, очень грамотно и профессионально построен, и даже может

состоять из нескольких этапов для создания доверия к звонившему, будет сведен к тому, что Вас попросят выполнить определенные действия, в необходимости которых злоумышленник будет настаивать. В итоге, как правило, все сводится к получению кода из СМС сообщения, либо переводу денежных средств.

Помните!

Переходя по ссылкам и диктуя коды из СМС неизвестным, Вы открываете преступникам доступ к использованию Вашей учетной записи и персональных данных на портале Госуслуг. С помощью них злоумышленники могут от Вашего имени подавать заявки на кредиты в финансовые учреждения, совершать сделки с недвижимостью, а также использовать весь набор возможностей, предоставленных данным сервисом.

Чтобы не стать жертвой мошенников необходимо помнить и соблюдать следующие основные плавила:

- Не переходите по ссылкам в сообщениях от «Госуслуг» с информацией, которую вы не запрашивали.
- Будьте внимательны к адресу отправителя и тексту сообщений, которые Вам приходят.
- Не сообщайте никому коды из СМС, кем бы Вам ни представлялись звонившие.
- Официальные рассылки от Госуслуг никогда не содержат запросов кодов подтверждения, банковских реквизитов и т.п. Они носят, как правило, информационный характер.
- Контролируйте Ваш личный кабинет на портале Госуслуг и соблюдайте правила безопасности, чтобы защитить свой профиль.

В предпраздничные и праздничные дни опасность стать жертвой мошенников особенно высока!

Чтобы избежать этого, просим Вас быть бдительными, а также соблюдать следующие **основные рекомендации безопасности** при использовании системы ДБО **на компьютере и мобильном устройстве**.

Рекомендации по обеспечению информационной безопасности при использовании системы ДБО на компьютере.

Для обеспечения информационной безопасности при использовании системы дистанционного банковского обслуживания и сведению рисков мошенничества и, как следствие, финансовые потери к минимуму, необходимо быть предельно внимательными и следовать рекомендациям приведенным ниже.

Особенное внимание безопасности необходимо уделить тем клиентам с так называемым «домашним» компьютером, где выход в Интернет наиболее часто осуществляется без межсетевого экрана защиты и антивирусного программного обеспечения.

- Рекомендуется осуществлять работу в системе Дистанционного банковского обслуживания (ДБО) с использованием отдельной учетной записи в операционной системе компьютера, защищенной сложным паролем, известным только Вам. При возможности рекомендуется осуществлять доступ в ДБО с выделенного компьютера, используемого исключительно для работы с ДБО. Права пользователя в операционной системе компьютера должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в ДБО. По возможности исключите посещение с данного компьютера сайтов сомнительного содержания и любых других потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов полученных из недостоверных источников;
- Соблюдайте правила безопасности при работе с ключевыми носителями:

- Необходимо сохранять в тайне закрытый (секретный) ключ электронной подписи. Не оставлять ключи в компьютере или на столе, если Вы покидаете свое рабочее место. По окончании работы ключи убирать в сейф, либо в шкаф, запираемый на замок. Не оставляйте без присмотра компьютер с активной ДБО;

- Уделите вопросу хранения ключей ДБО должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк;

- Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске компьютера;

- Постарайтесь внедрить использование для отправки документов двух подписей (2-х ключей);

- При компрометации или подозрения на компрометацию секретных ключей или компьютера, увольнения ответственного сотрудника или ИТ специалиста Вашей компании, который имел доступ к компьютеру или к секретным ключам, а также при истечении срока действия ключа с периодичностью, установленной договором на ДБО и правилами работы в системе незамедлительно сообщите в Банк для блокировки ключей и генерации новых.

- Рекомендуется избегать работы в ДБО с «недоверенных» компьютеров (в Интернет-кафе или другие общедоступные компьютеры, а так же «чужие» компьютеры временно используемые вами и т.п.). Крайне не желательно использование для работы в ДБО публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.);
- Соблюдайте правила безопасности при использовании паролей:

- Для работы в ДБО необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

пароль должен иметь длину от 8 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков ! # $ % & ( ) * + - . / : ; < = > ? [\ .

пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.)

пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера вашей банковской карты и т.п.)

пароль не должен содержать словарных слов (*passw0rd, football,* shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей – Cthutq).

пароль не должен совпадать с предыдущими паролями и не должен совпадать с именем входа.

пароль не должен быть копией или комбинаций паролей используемых Вами в других системах (операционная система компьютера, электронная почта, развлекательный ресурсы в Интернет и т.п.);

- Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и работникам Банка, вводите пароль только при работе в ДБО. Работник Банка не имеет права запрашивать у Вас пароль, даже если вы самостоятельно обратились в Банк. Вводите пароль только в ДБО, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль;

- Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять пароль на компьютере, мобильном устройстве, а так же на иных электронных носителях, доступ к которым могут получить третьи лица. Необходимо периодическое изменение пароля входа в систему. Во избежание раскрытия пароля входа в систему третьими лицами, рекомендуется изменять пароль один раз в три месяца.

- Рекомендуется постоянное использование системы антивирусного программного обеспечения (NOD32, AVP Kaspersky, Symantec AntiVirus и т.п.) на Ваших компьютерах. Необходимо использовать лицензионные программные продукты последних версий и постоянно обновлять антивирусные базы данных программных продуктов. Обновление антивирусных баз рекомендуется проводить в автоматическом режиме по мере их выпуска организацией-разработчиком. Необходимо обеспечить регулярные периодические проверки по поиску вирусов на автоматизированных рабочих местах используемых для ДБО.
- При поломке компьютера, с которого осуществляется работа по системе дистанционного банковского обслуживания, немедленно звоните в Банк и просите блокировать операции по системе;
- Остерегайтесь мошенничества:

- Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по СМС или email с просьбой предоставить, подтвердить или уточнить Вашу личную информацию (пароли, логины, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли и другие личные данные). Не отвечайте на такие сообщения;

- При получении подозрительного сообщения якобы от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении (даже если адрес похож на адрес сайта Банка). В сообщениях Банка никогда не будет просьбы зайти в ДБО по указанной в сообщении ссылке;

- При работе с ДБО обратите внимание на страницу входа и интерфейс, если вы заметите любые отличия, не заявленные ранее Банком, или возникнут иные причины для возникновения подозрений в том, что сайт поддельный, необходимо незамедлительно прекратить работу и обратиться в Банк по телефону техподдержки (никогда не связывайтесь по телефону указанному на подозрительной странице);

- Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в ДБО;

- Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в ДБО. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности ДБО вследствие проведения каких-либо регламентных работ. Если вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону техподдержки (никогда не связывайтесь с Банком по телефону указанному в подозрительном сообщении);

- Обращайте внимание на появление подозрительной активности на Вашем компьютере, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность зайти на сайт ДБО, при том, что другие Интернет-сайты у Вас загружаются, а так же на невозможность войти в ДБО по причине несовпадения логина и пароля, при том, что они корректны. Обращайте внимание на «зависания» ДБО, при нормальной работе других Интернет сайтов. Данные факты могут свидетельствовать о заражении Вашего компьютера вредоносными программами. Избегайте работы в ДБО с зараженных компьютеров, если на зараженном компьютере уже осуществлялась работа в ДБО, то незамедлительно заблокируйте Вашу учетную запись в ДБО. Вы можете сделать это, связавшись с Банком по телефону техподдержки.

• При эксплуатации средств защиты информации необходимо соблюдать рекомендации по обеспечению безопасности средств защиты информации.

• Нарушение правил безопасности при работе с системой «Интернет-Клиент» – зона ответственности Клиента. При нарушении правил безопасности и несоблюдении рекомендаций от Банка, Клиент берет на себя риски, связанные с безопасностью осуществляемых финансовых операций в системе «Интернет-Клиент».

• В случае подозрения или обнаружения несанкционированного доступа в систему ДБО необходимо незамедлительно позвонить в Банк, чтобы приостановить работу Вашей системы по следующим телефонам:

- с 9:00–18:00 пн.-чт., с 09:00-17:00 пт., за исключением выходных и праздничных дней согласно законодательства РФ по телефону 8 (3532) 34-90-90 – Служба технической поддержки;

- с 9:00–18:00 пн.-чт., с 09:00-17:00 пт., за исключением выходных и праздничных дней согласно законодательства РФ по телефону 8 (3532) 34-90-89 - Отдел по работе с юридическими лицами УКБ.

Рекомендации по обеспечению информационной безопасности при использовании системы ДБО на мобильном устройстве.

1. Для доступа к мобильному устройству установите пароль и настройте автоматическую блокировку устройства.
2. Загружайте и устанавливайте программное обеспечение только из проверенных и надежных источников – Google Play или App Store.
3. Производите своевременное обновление операционной системы и используемых программ (браузера и иных прикладных программ).
4. Установите на свое мобильное устройство лицензионное антивирусное программное обеспечение и обеспечьте регулярное обновление антивирусных баз.
5. Регулярно производите полную антивирусную проверку мобильного устройства.
6. Для работы с системами Банка используйте защищенные мобильные устройства – не пытайтесь обходить установленные производителем защитные механизмы. Не перепрошивайте свое мобильное устройство прошивками сторонних лиц, не являющихся производителями устройства, т.к. это может сделать устройство уязвимым к заражению вредоносным кодом.
7. Используйте защищенные точки доступа к Wi-Fi-сети, а также отключайте Wi-Fi и Bluetooth, если в данный момент они не используются.
8. Не храните на мобильном устройстве конфиденциальную информацию о Вашем логине и пароле для доступа к системе ДБО. Если такая необходимость все же есть, не храните информацию в явном виде.
9. Удаляйте конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек.
10. В случае изменения номера телефона мобильного телефона для работы в системах Банка, обратитесь в Банк для изменения доступа со старого номера на новый номер телефона. Необходимо помнить, что старый номер мобильный оператор может передать другому абоненту в случае, если он неактивен некоторое время.
11. Ни при каких условиях не сообщайте информацию о Вашем логине, пароле, одноразовых паролях и иных сведениях, используемых для авторизации в системе ДБО никому, включая сотрудников Банка.
12. При возникновении подозрений, что Ваши данные для доступа (логин или пароль) к системе ДБО стали известны посторонним и/или в случае утери мобильного устройства незамедлительно обратитесь в Банк для их блокировки.