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

Уважаемые Клиенты!

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

Обращаем Ваше внимание, на высокую значимость мер, необходимых для снижения рисков, связанных с получением несанкционированного доступа к защищаемой информации и хищением денежных средств мошенниками!

Риски получения несанкционированного доступа к защищаемой информации в ДБО:

- Слабые пароли: Использование простых, легко угадываемых паролей или повторное использование одного пароля для разных сервисов.
- Небрежное хранение аутентификационных данных: Запись паролей, пин-кодов, кодов подтверждения на бумаге, в электронных файлах или передача их третьим лицам.
- Утеря устройств: Потеря токенов, SIM-карт, смартфонов или компьютеров, используемых для доступа к ДБО.
- Фишинг: Переход по ссылкам из фишинговых писем или SMS, раскрытие конфиденциальной информации мошенникам, выдающим себя за сотрудников банка, государственных органов и т.д.
- Социальная инженерия: Раскрытие конфиденциальной информации под воздействием психологического давления или манипуляций со стороны мошенников.
- Установка вредоносного ПО: Загрузка и установка программ (приложений) из ненадежных источников, что может привести к заражению устройства вирусами, шпионскими программами (приложениями), банковскими троянами и т.д.
- Уязвимости в программном обеспечении: Отсутствие обновления программного обеспечение на компьютере, мобильном устройстве может быть использовано злоумышленниками для получения доступа к системе.
- Небезопасные каналы связи: Перехват данных при использовании незащищенных каналов связи, например, общественных Wi-Fi сетей.
- Несоблюдение правил безопасности: Игнорирование рекомендаций банка по безопасности, например, использование незащищенных Wi-Fi сетей для доступа к ДБО, отсутствие антивирусного ПО, использование ПО для удаленного доступа и т.д.

Последствия несанкционированного доступа:

- Хищение денежных средств со счетов.
- Оформление кредитов на имя клиента.
- Утечка конфиденциальной информации: персональные данные, банковская тайна.
- Уголовная ответственность для клиента при использовании ДБО и банковских карт в мошеннических схемах, при вовлечении клиента в дропперство.

Меры предотвращения несанкционированного доступа к ДБО и контроля конфигурации устройств:

Для обеспечения безопасности при использовании системы ДБО и предотвращения финансовых потерь, связанных с несанкционированным доступом необходимо выполнение указанных мер по снижению данных рисков.

1. Предотвращение несанкционированного доступа:

- Сложные пароли: Используйте надежные, уникальные пароли для всех учетных записей, связанных с ДБО. Пароли должны быть длинными (не менее 12 символов), содержать буквы разного регистра, цифры и специальные символы. Регулярно меняйте пароли (не реже одного раза в квартал). Избегайте использования легко угадываемых паролей (даты рождения, имена и т.п.).
- Ограничение доступа: Не используйте для работы в ДБО учетные записи Вашего компьютера с правами администратора.
- Антивирусная защита: Установите и регулярно обновляйте антивирусное программное обеспечение на всех устройствах, используемых для доступа к ДБО.
- Фишинг и социальная инженерия: Будьте осторожны с подозрительными электронными письмами, SMS-сообщениями и звонками (особенно в мессенджерах). Никогда не сообщайте свои учетные данные, пароли или коды подтверждения третьим лицам. Банк, а также государственные органы (портал Госуслуг, МФЦ, МВД, Банк России и т.д) не запрашивает эту информацию у клиентов таким образом.
- Защита от нежелательных звонков и сообщений: По возможности используйте специализированные приложения для мобильных устройств, а также услуги операторов связи по защите от нежелательных звонков и SMS-сообщений.
- Безопасные сети: Избегайте использования публичных Wi-Fi сетей для доступа к ДБО.
- Своевременное обновление ПО: Устанавливайте все обновления безопасности для операционной системы, браузера, антивирусного ПО на устройствах, используемых для работы с ДБО.
- Удаленный доступ: Исключите использование ПО для удаленного доступа на устройстве, которое используется для работы с ДБО.

2. Контроль конфигурации устройств:

- Инвентаризация устройств: Учет и контроль всех устройств, используемых для доступа к ДБО.
- Контроль программного обеспечения: Устанавливайте только лицензионное и проверенное программное обеспечение. Контролируйте появление на устройстве новых программ (приложений), которые Вы не устанавливали. Контролируйте разрешения, которые предоставлены приложениям на Вашем устройстве, особенно приложениям, к которым нет доверия.
- Защита от вредоносного ПО: Регулярно проверяйте антивирусным ПО устройства на наличие вредоносных программ (приложений).
- Резервное копирование: Регулярно создавайте резервные копии важных данных.

3. Взаимодействие с банком:

- Своевременное информирование: Незамедлительно сообщайте банку о любых подозрительных активностях в ДБО, утере устройств или компрометации учетных данных в целях своевременной блокировки доступа в ДБО.

Меры по защите информации от воздействия вредоносного кода:

1. Используйте антивирусное программное обеспечение:

• Установите антивирусное ПО на свои устройства (компьютеры, ноутбуки, смартфоны, планшеты).

• Регулярно обновляйте антивирусные базы.

• Настройте автоматическое сканирование системы.

• Периодически проводите полное сканирование системы.

2. Будьте бдительны с электронной почтой, мессенджерами и SMS:

• Не открывайте письма и вложения от неизвестных отправителей.

• Не переходите по ссылкам из подозрительных писем или сообщений.

• Критически анализируйте подозрительные признаки письма или сообщения.

3. Защитите свой браузер при использовании ДБО на компьютере:

• Регулярно обновляйте свой браузер до последней версии.

• Используйте блокировщики рекламы и всплывающих окон.

• Включайте в браузерах расширения установленных антивирусных систем.

4. Будьте осторожны при загрузке файлов:

• Скачивайте файлы только с проверенных и надежных источников.

• Обращайте внимание на расширение файлов (избегайте .exe, .scr, .bat и других потенциально опасных или неизвестных Вам расширений).

• Сканируйте загруженные файлы антивирусным ПО перед открытием.

• Высокую опасность представляют файлы и ссылки, полученные в мессенджерах от неизвестных отправителей, или отправителей, представляющихся работниками банков либо государственных органов.

5. Обновляйте операционную систему и программное обеспечение:

• Устанавливайте все обновления безопасности для операционной системы и других программ (приложений) на компьютерах и мобильных устройствах, используемых для доступа к ДБО.

• Используйте только лицензионное программное обеспечение.

6. Используйте надежные пароли:

• Создавайте сложные и уникальные пароли для всех своих учетных записей.

• Используйте менеджер паролей для хранения и генерации паролей.

• Не используйте один и тот же пароль для разных сервисов.

7. Будьте осторожны с публичными Wi-Fi сетями:

• Избегайте использования общественных Wi-Fi сетей для проведения финансовых операций и передачи важной информации.

8. Регулярно создавайте резервные копии важных данных:

• Создавайте резервные копии важных файлов и документов на внешнем носителе или в облачном хранилище. Это поможет восстановить данные в случае заражения устройства вредоносным кодом.

9. Обучайтесь основам кибербезопасности:

• Повышайте свою осведомленность о методах защиты от вредоносного кода.

• Ознакомьтесь с рекомендациями банка по безопасности.

10. Сообщайте о подозрительной активности:

• Если вы заметили подозрительную активность на своем устройстве или в своем банковском счете, немедленно сообщите об этом в банк для блокировки доступа в ДБО.

Следование этим рекомендациям поможет вам защитить свою информацию от воздействия вредоносного кода и предотвратить финансовые потери.

Выполнение данных мер по предотвращению несанкционированного доступа, контролю конфигурации устройства, защите от вредоносного кода при использовании системы ДБО на компьютере и мобильном устройстве, поможет защитить ваши финансы и обеспечить безопасную работу с системой ДБО и банковскими картами.