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 (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 с целью совершения переводов 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 доступа: 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.
- 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.
- Установка вредоносного ПО: Загрузка и установка программ из ненадежных источников, что может привести к заражению устройства вирусами, шпионскими программами, 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.

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: Разграничьте права доступа сотрудников к ДБО в соответствии с их должностными обязанностями. Минимизируйте количество сотрудников с полными правами доступа. Не используйте для работы в ДБО учетные записи Вашего компьютера с правами администратора.

• Контроль IP-адресов: По возможности настройте ограничение доступа к ДБО по IP-адресам, разрешая вход только с доверенных адресов.

• Антивирусная защита: Установите и регулярно обновляйте антивирусное программное обеспечение на всех устройствах, используемых для доступа к ДБО.

• Фишинг: Будьте осторожны с подозрительными электронными письмами, SMS-сообщениями и звонками. Никогда не сообщайте свои учетные данные, пароли или коды подтверждения третьим лицам. Банк никогда не будет запрашивать эту информацию у вас таким образом.

• Безопасные сети: Избегайте использования публичных Wi-Fi сетей для доступа к ДБО.

• Обучение персонала: Регулярно проводите обучение сотрудников по вопросам информационной безопасности и безопасной работы с ДБО.

• Своевременное обновление ПО: Устанавливайте все обновления безопасности для операционной системы, браузера и других программ, 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 всех устройств, используемых для доступа к ДБО.

• Контроль программного обеспечения: Устанавливайте только лицензионное и проверенное программное обеспечение. Контролируйте появление на устройстве новых программ, которые Вы не устанавливали.

• Защита от вредоносного ПО: Регулярно проверяйте устройства на наличие вредоносных программ.

• 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 надежное антивирусное программное обеспечение:

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

• Регулярно обновляйте антивирусные базы.

• Настройте автоматическое сканирование системы.

• Периодически проводите полное сканирование системы.

• Настройка

2. Будьте бдительны с электронными письмами и мессенджерами:

• 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:

• 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.

5. Обновляйте операционную систему и программное обеспечение:

• Устанавливайте все обновления безопасности для операционной системы и других программ.

• 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.

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.

<u>Последствия несанкционированного доступа:</u>

• Финансовые потери: Хищение денежных средств со счетов.

• Утечка конфиденциальной информации: Потеря данных о клиентах, финансовых операциях и другой защищаемой информации.

• Репутационный ущерб.

• Юридические последствия: Возможные судебные разбирательства и штрафы.

Выполнение данных мер по снижению рисков несанкционированного доступа, а также рекомендаций по обеспечению информационной безопасности при использовании системы ДБО на компьютере и мобильном устройстве размещенных на сайте Банка, поможет защитить ваши финансы и обеспечить безопасную работу с системой ДБО.