ИКБанк
Инвестиционный Кооперативный Банк
420043 г. Казань, ул. Вишневского 24, тел.: 8 (843) 231 72 73; факс: 8 (843) 238 07 56, www.icbru.ru
ИНН 1653005038

Рекомендации по снижению рисков повторного осуществления переводов денежных средств без добровольного согласия

В целях снижения рисков повторного осуществления перевода денежных средств без согласия клиента, АО «ИК Банк» рекомендует:

1. При открытии сайт Интернет-Банка, прежде чем начать работать, убедитесь, что адрес сайта в адресной строке браузера указан верно: https://online.icbru.ru/.

Обращаем внимание: адрес должен начинаться с «https://»!

В браузере должен быть виден значок «Замочка». Наличие этого значка подтверждает наличие многоступенчатой системы безопасности с протоколом защищенной передачи данных (TLS - Transport Layer Security). Нажав на изображение замочка, вы можете посмотреть сертификат Интернет-Банка и убедиться, что данный сайт, на котором вы находитесь, действительно является Интернет-Банком «ИК Банк».

2. Не сообщайте свои личные данные, такие как ФИО, паспортные данные, логины, пароли, коды доступа, SMS-коды, одноразовые пароли, реквизиты банковских карт, ПИН-код, цифры с обратной стороны карты (CVV/CVC-код), посторонним людям во время телефонного разговора, по электронной почте или другим способом, в том числе если они представляются сотрудниками правоохранительных органов, операторами сотовой связи, работниками банков, работниками Центрального банка, Госуслуг и т.д;

Не проводите никакие действия по указанию или по рекомендациям посторонних лиц, не сообщайте им результаты своих действий в ДБО/Мобильном банке/на Госуслугах и т.д.

Если Вам говорят, что сбережения в опасности и их немедленно необходимо перевести на безопасный счет или просят передать личные данные, незамедлительно прекращайте общение.

В случае сомнений, положите трубку и перезвоните в нужную организацию по официальному номеру телефона сами. При необходимости, обратитесь в отделение Банка, либо позвоните по номеру на обратной стороне карты и убедитесь, что с вашими деньгами все в порядке

3. При создании паролей придерживайтесь следующих правил:

- Пароли от разных систем должны отличаться между собой;
- Пароль должен быть не меньше 8 символов;

● Не используйте простые, легко угадываемые комбинации букв и цифр, символов или личных данных (123, qwerty, дата рождения, девичья фамилия, логин от почты и т.д.).

● В пароле должны быть буквы в верхнем (прописные) и нижнем (строчные) регистре;

● Обязательно используете специальные символы при создании пароля (@, #, $, &, *, % и т.п.);

● Используйте сложные парольные фразы, так будет проще запомнить вам и сложнее вычислить киберпреступникам. Сложная парольная фраза – это набор из несвязанных логически между собой слов, которые вы берете, как буквенную часть в Ваш пароль. Дополнительно к нему добавляете цифры и специальные символы. Парольную фразу из четырех или более произвольных слов с комбинацией из дополнительных символов взламывать будут несколько веков, а «qwerty123» - миллисекунду.

● Меняйте пароль раз в месяц, измените пароль на другой, если у вас возникли подозрения, что кто-то его узнал;

4. Используйте только лицензионное программное обеспечение или свободно распространяемое программное обеспечение с официальных сайтов (операционные системы, офисные пакеты и пр.).

5. Обеспечьте автоматическое обновление системного и прикладного программного обеспечения.

6. Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз.

Необходимо на постоянной основе регулярно, например, ежемесячно, проводить полную проверку электронного устройства, на котором производиться переводы денежных средств, на наличие вредоносного программного обеспечения.

7. Применять на рабочем месте лицензионные персональные межсетевые экраны, антишпионское программное обеспечение и т.п.

Не рекомендуется работать в Интернет-Банке с подозрительных компьютеров (например, на компьютере, на котором не установлены антивирус и межсетевое устройство защиты) и с компьютеров, которые находятся в публичных местах (например, интернет-кафе, компьютерный клуб).

8. Исключить обслуживание компьютеров, используемых для работы с Системой ДБО, случайными сотрудниками технической поддержки.

9. При обслуживании компьютера сотрудниками технической поддержки обеспечивать контроль за выполняемыми ими действиями.

10. Никогда не передавать ключи электронной подписи сотрудникам технической поддержки для проверки работы системы ДБО, проверки настроек взаимодействия с банком

и т.п. При необходимости таких проверок владелец ключа электронной подписи лично должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентской части системы ДБО, и лично ввести пароль.

11. Будьте внимательны при получении писем или смс-сообщений якобы от имени Банка. Основные признаки, того, что сообщение отправлено мошенниками:

● ссылка, указанная в сообщении, не содержит названия Банка, либо содержит его в искаженном виде;

● запрашиваемые в сообщении действия требуют Вашего срочного ответа или принятия немедленного действия (ваш счет будет заблокирован);

● в сообщении требуется предоставить, обновить или подтвердить Ваш логин и пароль к системам дистанционного банковского обслуживания (в случае использования их Клиентами);

● содержит информацию, что на Ваш счет поступили денежные средства, которых Вы не ожидали.

12. Не высылайте по электронной почте идентификационные данные Интернет-Банка;

13. Не отвечайте на электронные письма с запросом о ваших идентификационных данных (код пользователя, пароль, код доступа, данные паспорта) или другой личной информации, которые посылаются как бы от имени банка. Банк НИКОГДА не запрашивает такую информацию по почте, электронной почте или телефону;

14. Закончив работать в Интернет-Банке, всегда нажимайте кнопку «Выход» в правом верхнем углу страницы, чтобы выйти из Интернет-Банка;

15. Контролируйте состояние своего счета и остатки на счете;

16. Не проводите никакие действия по указанию или по рекомендациям посторонних лиц, не сообщайте им результаты своих действий в ДБО/Мобильном банке/на Госуслугах и т.д. Если Вам говорят, что сбережения в опасности и их немедленно необходимо перевести на безопасный счет или просят передать личные данные, **незамедлительно прекращайте общение.**

В случае обнаружения сайтов, доменных имен и стилей оформления, сходных с именами и оформлением страницы сервиса ДБО Банка (https://online.icbru.ru/), а также при отсутствии возможности подключения к сервису ДБО Банка, при возникновении подозрений на несанкционированную работу в сервисе ДБО или на наличие на АРМах, задействованных в работе сервиса ДБО Банка по номеру телефону: (843) 231-72-17.