Памятка: как минимизировать риски денежных переводов без согласия клиента

Вместе с РОССИЕЙ
БАНК РОССИЯ

Уважаемый клиент, будьте внимательны: в последнее время участились случаи переводов денежных средств без добровольного согласия клиента. Это подтверждает статистика на сайте ЦБ РФ.

Для кражи средств со счетов мошенники используют методы социальной инженерии — представляются сотрудниками Банка и пытаются получить данные для проведения банковских операций: коды доступа, коды СМС-подтверждений и прочую конфиденциальную информацию.

Что повышает риски

- Посещение с рабочего компьютера соцсетей, почтовых клиентов и прочих незащищённых сайтов в интернете
- Отсутствие антивируса либо его нерегулярное обновление на компьютере для работы с Банком
- Использование неактуальных версий ПО
- Утеря носителей ключей электронной подписи или несанкционированное копирование данных
- Нерегулярная проверка входящих электронных документов из Банка, несвоевременное получение важной информации
- Передача данных для совершения операции третьим лицам, в том числе под воздействием методов социальной инженерии

Какие правила нужно соблюдать

- Не сообщайте никому свою персональную информацию, включая логины и пароли, данные технических устройств
- Не сообщайте никому коды доступа и коды для проведения операций
- Сразу обращайтесь в Банк для обновления контактной информации, если она изменилась
- Не обходите и не изменяйте установленное производителем защитное ПО при использовании системы ДБО
- Пользуйтесь только лицензионными антивирусами, работающими автоматически, и регулярно их обновляйте
- Не загружайте и не устанавливайте ПО из недостоверных источников
- Не используйте публичные беспроводные сети Wi-Fi для переводов денежных средств
- Используйте сложные пароли, избегайте легко угадываемых комбинаций букв и цифр, а также паролей для доступа к другим ресурсам
- Ограничьте прямой и удалённый доступ к компьютеру для работы с ДБО и не оставляйте его без присмотра
- Не переходите по ссылкам из почтовых сообщений и СМС из недостоверных источников; проверяйте ссылки: в адресной строке браузера безопасный адрес начинается с https и имеет пиктограмму закрытого замка
- Будьте внимательны при получении писем и СМС от имени Банка; основной признак мошеннического сообщения — ссылка, которая не содержит адреса Банка abr.ru, либо содержит искажённый адрес
- Проверяйте подлинность сообщений от Банка, будьте внимательны, если сообщение требует срочного ответа или немедленных действий, такие сообщения часто рассылают мошенники
- Не сообщайте по телефону конфиденциальную информацию — ключи, пароли и прочие сведения, даже если это «звонок из банка», специалисты Банка никогда не запрашивают по телефону конфиденциальные данные
- Обеспечьте своевременное поступление информации от Банка — регулярно проверяйте входящие документы в системе ДБО
- Не посещайте сомнительные сайты и не вводите на них свои данные, чтобы не допустить заражения компьютера или смартфона вредоносным ПО для кражи денежных средств
- Убедитесь, что для работы с ДБО подключились к официальному сайту Банка по безопасному протоколу — вначале https, затем корректный адрес интернет-банка
- Доверяйте обслуживание компьютеров для работы с системой ДБО только проверенным специалистам технической поддержки
- Никогда не передавайте свои ключи электронной подписи сотрудникам технической поддержки для проверки работы системы ДБО
- Если заметили, что Клиент-банк ведёт себя необычно или изменился его интерфейс, срочно позвоните в Банк: 8 (812) 335-65-25 или 8 (495) 276-02-85