МУНИЦИПАЛЬНЫЙ КАМЧАТПРОФИТБАНК

Рекомендации по снижению рисков перевода денежных средств без согласия клиента

1. Не сообщайте посторонним лицам свою персональную информацию (ФИО, реквизиты электронного средства платежа - банковской карты и/или Интернет банка (далее - ЭСП): логин, пароль, номер карты, счета, паспорта и т.д. Сотрудник Банка имеет право уточнять у клиента подобную информацию только в случае, если клиент самостоятельно обратился в Банк.

2. Помните: полиция, Центральный Банк Российской Федерации, Федеральная служба безопасности, Следственный комитет, Социальный фонд России, службы безопасности банков никогда не решают важные вопросы по телефону. Если диалог Вам кажется сомнительным, закончите вызов и перезвоните по официальному номеру, указанному на официальном сайте государственного учреждения или Банка. Если родственник/знакомый связался с Вами с незнакомого номера и просит о помощи, свяжитесь персонально с ним по известным Вам номерам. Главное — не паникуйте и не совершайте никаких действий по указке звонящего.

3. В случае утери смартфона/ мобильного телефона незамедлительно заблокируйте SIM-карту у оператора сотовой связи.

4. В случае изменения номера телефона обратитесь в Банк для замены телефонного номера, по которому осуществляется доступ к сервисам Банка. Помните, что старый номер сотовый оператор может передать другому абоненту в случае, если он неактивен некоторое время.

5. Если у Вас неожиданно перестала работать SIM-карта – незамедлительно обратитесь к оператору сотовой связи для выяснения причин, так как это может быть одним из признаков, совершаемых в отношении Вас третьими лицами мошеннических действий.

6. Для перевода денежных средств используйте защищенные электронные устройства (компьютер, электронный планшет, смартфон, мобильный телефон, далее – ЭУ) не пытайтесь обходить установленные производителем ЭУ программные средства защиты. Не перепрошивайте свое ЭУ программным обеспечением сторонних лиц, не являющихся производителями устройства, т.к. это может сделать Ваше устройство уязвимым к заражению вредоносным программным обеспечением (далее - ВПО).

7. Не работайте на ЭУ и не осуществляйте переводы денежных средств через публичные беспроводные сети (free Wi-Fi), незащищенные беспроводные сети. Специальные приложения применяют механизмы защиты своих данных при передаче, а так как публичные беспроводные сети сравнительно труднее контролировать, то у злоумышленников появляется больше возможностей для попыток обхода защитных механизмов. Используйте для работы подключение к сети Интернет через оператора мобильной связи или через доверенную защищенную беспроводную сеть.

8. При создании паролей придерживайтесь следующих правил:

- Не используйте в качестве пароля простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в другие системы.

- Пароль должен быть не менее 8 символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, год рождения, номер телефона и т.п.).

9. Храните код доступа в тайне и предпринимайте необходимые меры предосторожности для предотвращения его несанкционированного использования. Не записывайте код доступа там, где доступ к нему могут получить посторонние лица (включая незаблокированное ЭУ).

10. Не сообщайте код доступа, SMS-коды, необходимые для проведения операций, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карты (CVV/CVC-код) посторонним лицам, сотрудникам Банка, банка-эмитента карты по телефону, электронной почте или иным способом. При возникновении подозрения, что такие данные стали известны третьему лицу, сообщите об этом по контактным телефонам, указанным на официальном сайте Банка.

11. Не оставляйте ЭУ без присмотра. Ограничьте доступ посторонних лиц к компьютеру, с которого осуществляется переводы денежных средств. Установите пароль на доступ к ЭУ и/или на доступ к SMS-сообщениям. Это затруднит доступ злоумышленникам к ЭУ в случае его утраты.

12. Применяйте на ЭУ лицензионные средства антивирусной защиты, работающие в автоматическом режиме, и регулярно в рекомендуемые разработчиками сроки проводите их обновление.

13. Не допускайте отключения или несвоевременное обновление антивирусных средств, установленных на ЭУ. В случае обнаружения на ЭУ нештатного отключения антивирусных средств – не работайте на ЭУ и не осуществляйте переводы денежных средств до устранения причины нештатного отключения.

14. Проверяйте ЭУ на наличие ВПО перед началом работы, а также после доступа к Вашему ЭУ сотрудников технической поддержки различных организаций или любых других частных мастеров, выполнивших работу по установке, обновлению и поддержке различных программ.

15. На постоянной основе, например, ежемесячно, проводите полную проверку ЭУ, на котором производиться переводы денежных средств, на наличие ВПО.

16. Не рекомендуется передавать ЭУ для использования третьим лицам, в том числе родственникам, т.к. на оставленном без присмотра ЭУ может быть совершён ряд действий, направленных на получение доступа к персональным данным, ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платёжной карты (CVV/CVC-код) и иные данные. Например, злоумышленник может установить ВПО, настроить переадресацию SMS сообщений на другое устройство и т.п.

17. Не рекомендуется переходить по ссылкам, приходящим в почтовых сообщениях, SMS и MMS-сообщениях из недостоверных источников, в том числе на известные сайты, а также загружать и устанавливать на ЭУ программное обеспечение из недостоверных источников.

18. 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.

19. При обращении от имени Банка по телефону, электронной почте, через SMS сообщения лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах не сообщайте данную информацию. Банк никогда не запрашивает у клиентов персональные данные.

20. Регулярно контролируйте состояние своих счетов и незамедлительно информируйте Банк обо всех подозрительных или несанкционированных операциях в соответствии с Договором. При установке порядка регулярного контроля рекомендуем принимать в расчёт, что переводы денежных средств, в отношение которых наступила безотзывность перевода денежных средств, не могут быть приостановлены.

21. В случае неожиданного выхода из строя устройства, либо пропадания на нём программного обеспечения, прекратите на устройстве работу, отключите его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно свяжитесь с Банком для блокировки, запросите выписку по счету непосредственно в Банке. При обнаружении несанкционированных платежных операций напишите заявление в Банк, а также обратитесь с соответствующим заявлением в правоохранительные органы. Не восстанавливайте работоспособность поврежденного устройства до проведения технической экспертизы.

22. Если у Вас есть предположения о раскрытии пароля доступа, Ваших персональных данных, позволяющих совершить неправомерные действия с их использованием, немедленно обратитесь в Банк и следуйте указаниям сотрудника Банка.

23. Не отправляйте переводы по любым причинам от имени других лиц. В случае возврата перевода инициатором возврата и получателем средств будет являться лицо, от имени которого отправлен перевод. Недобросовестный отправитель может воспользоваться возможностью возврата и получить необоснованное обогащение.