Памятка по информационной безопасности пользователю системы Интернет-Банк

Уважаемые Клиенты!

В целях предотвращения несанкционированного доступа к Вашим счетам со стороны злоумышленников рекомендуем Вам соблюдать **следующие меры предосторожности** при использовании системы Интернет-Банк:

1. В качестве места хранения ключевой информации используйте только смарт-карту. Использование в качестве хранилища ключевой информации реестра или жесткого диска компьютера резко увеличивает риск ее компрометации.

2. Смарт-карта должна быть подключена к компьютеру только во время сеанса работы с системой Интернет-Банк. В остальное время смарт-карта должна храниться в сейфе или иных местах хранения, доступ к которым ограничен для посторонних лиц.

3. Рекомендуется оформлять право второй подписи, например, на главного бухгалтера предприятия. В этом случае для совершения операций с Вашим счетом через систему Интернет-Банк потребуется наличие двух подписей под электронным платежным документом, что снижает риск неправомерных операций.

4. Используйте лицензионное программное обеспечение (операционная система, офисные приложения и др.), полученное из проверенных и надежных источников, своевременно устанавливайте все обновления программного обеспечения, повышающие безопасность.

5. Установите лицензионную антивирусную программу и регулярно обновляйте антивирусные базы данных. Проводите периодическое сканирование компьютера на наличие вирусов. Обратите внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Вашем пароле или ключевой информации.

6. Не используйте взломанные операционные системы и программное обеспечение, во избежание активации злоумышленниками вложенных в данное программное обеспечение вредоносных кодов или программ.

7. Используйте межсетевые экраны (firewall), разрешив доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений. Используйте рекомендуемые настройки безопасности для вашего браузера.

8. На компьютере, используемом для работы с Интернет-Банком не рекомендуется работать под учетной записью, обладающей правами администратора.

9. Отключите на компьютере, с которого ведется работа в системе Интернет-Банк, гостевые учетные записи и возможность дистанционного управления.

10. На компьютере, используемом для работы в системе Интернет-Банк, не должно быть учетных записей (пользователей) с пустыми паролями.

11. Пароли должны удовлетворять следующим требованиям сложности:

- длина пароля должна быть не менее 6 символов;

- пароль должен содержать прописные и строчные буквы (a-z, A-Z), цифры, специальные символы (например !*$%^*()_+|~-=\`{}[]:";'?./).

12. Не храните пароли в открытом виде, исключите доступ к Вашему паролю посторонних лиц. Периодически, не реже чем раз в 3 месяца меняйте пароль на учетную запись под которой производятся платежные операции.

13. Не открывайте файлы и не переходите по ссылкам, полученным от неизвестных отправителей. Не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.

14. При входе в Систему необходимо убедиться, что в адресной строке web-браузера отображается именно адрес, начинающийся с **https://www.crocusbank.ru**. В случае, если

отображаемый адрес отличается от указанного, следует отказаться от дальнейших действий и незамедлительно обратиться в Банк.

15. Убедитесь в том, что соединение установлено в защищенном режиме, т.е. адресная строка в браузере начинается с https://. При этом в строке состояния или адресной строке браузера должен быть виден значок закрытого замка.

16. Включите систему фильтрации ложных web-узлов (антифишинг) в браузере; если браузер не имеет такой системы, обновите его.

17. Если при входе в систему Вы заметили какие-либо несоответствия стандартным запросам или вам позвонили от имени Банка с предложением попытаться войти в систему еще раз, ввести или сообщить пароль, не вводите и не сообщайте никаких данных. Незамедлительно обратитесь в Банк по телефону: +7(495) 228-12-44.

18. Не используйте функцию автозаполнения в установках браузера. Это предотвратит использование данных(имя пользователя, пароль и т.д.) сторонними лицами.

19. После окончания работы в системе всегда используйте кнопку «Выход».

20. Контролируйте состояние счѐта путем просмотра выписки.

21. Обращайте внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в систему, а также в специальном разделе «Безопасность -> Журнал сеансов работы»).

22. Рекомендуется использовать SMS-информирование о проведенных операциях по счетам.

23. В случаях компрометации или подозрения на компрометацию ключевой информации необходимо немедленно обратиться в Банк для блокировки и замены ключей.

24. Если у Вас возникли подозрения о компрометации пароля, Вам необходимо самостоятельно сменить его или заблокировать доступ в интернет-банк с помощью обращения в Банк.

25. Следует осуществлять информационное взаимодействие с Банком только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.

Просим Вас незамедлительно обращаться в Банк при возникновении следующих ситуаций:

- В выписке обнаружены несанкционированные Вами расходные операции.
- Утерян или похищен носитель ключевой информации.
- У Вас не работает система Интернет-Банк по неизвестным причинам.

Телефон службы поддержки клиентов: +7(495) 228-12-44

Помните, что соблюдение указанных правил и своевременное обращение в Банк при угрозе компрометации Ваших ключей помогут существенно снизить угрозу мошенничества с Вашими счетами посредством системы Интернет-Банк.