КРОНА-БАНК
Основан в 1993 году

Памятка по информационной безопасности пользователю системы Клиент Windows

Уважаемые Клиенты!

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

1. В качестве места хранения ключевой информации используйте только электронные ключ Rutoken. Использование в качестве хранилища ключевой информации реестра или жесткого диска компьютера резко увеличивает риск ее компрометации.
2. Электронный ключ Rutoken должен быть подключен к компьютеру только во время сеанса работы с системой Клиент Windows. В остальное время Rutoken должен 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 Клиент Windows 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.
8. Не рекомендуется работать с системой Клиент Windows под учетной записью, обладающей правами администратора.
9. Отключите на компьютере, с которого ведется работа в системе Клиент Windows, гостевые учетные записи и возможность дистанционного управления.
10. На компьютере, используемом для работы в системе Клиент Windows, не должно быть учетных записей (пользователей) с пустыми паролями.
11. Покидая рабочее место, необходимо блокировать компьютер (Alt+Ctrl+Del -> Блокировать компьютер или сочетание клавиш Win+L). В случае необходимости использования компьютера несколькими пользователями, необходимо установить пароль на Клиент Windows с помощью встроенных в него средств.
12. Не оставляйте без присмотра работников сторонних организаций, которые производят сервисные работы на компьютере с установленной системой Клиент Windows.

13. 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 !*$%^*()_+|~-=\`{}[]:";'?./).
14. 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.
15. Не открывайте файлы и не переходите по ссылкам, полученным от неизвестных отправителей. Не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.
16. Контролируйте состояние счёта путем просмотра выписки.
17. Рекомендуется использовать SMS-информирование о проведенных операциях по счетам.
18. В случаях компрометации или подозрения на компрометацию ключевой информации необходимо немедленно обратиться в Банк для блокировки и замены ключей.
19. Если у Вас возникли подозрения о компрометации пароля, Вам необходимо самостоятельно сменить его или заблокировать доступ к счетам из Клиент Windows, обратившись в Банк.
20. 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 или компьютер, на котором была установлена система Клиент Windows.
- У Вас не работает система Клиент Windows по неизвестным причинам.

Телефоны службы поддержки клиентов:
+7 (3952) 48-40-77

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