

ПАМЯТКА О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМ КОШЕЛЬКОМ

Уважаемый Клиент!

ООО «Вайлдберриз Банк» обращает Ваше внимание на необходимость соблюдать принципы обеспечения информационной безопасности с целью исключения случаев несанкционированного доступа к Вашему электронному кошельку и осуществления переводов электронных денежных средств неуполномоченными лицами.

Рекомендации для безопасной работы с электронным кошельком:

1. При работе с электронным кошельком используйте компьютер/мобильное устройство, на котором установлено только лицензионное программное обеспечение, дистрибутивы которого получены из надежных источников.
2. Установите на компьютер/мобильное устройство лицензионное антивирусное программное обеспечение, обеспечьте автоматическое обновление антивирусных баз.
3. Не допускайте посторонних к Вашему электронному кошельку, мобильному устройству, компьютеру.
4. Никому не сообщайте пароли (в т.ч. и одноразовые) для доступа к электронному кошельку.
5. Никому не сообщайте полный номер Вашего электронного кошелька.
6. Не используйте функцию запоминания паролей и автоматической авторизации в платежных интернет – сервисах.
7. Не храните логины и пароли для доступа к электронному кошельку на жестком диске компьютера. Если у Вас есть необходимость хранить эти данные именно в цифровом формате, сохраняйте их на внешних носителях: картах памяти, "флешках" и т.п.
8. Используйте режим «Инкогнито» (приватный) при совершении покупок через Интернет. Удаляйте информацию о платежах с помощью очистки буфера файлов и файлов сохранения данных.
9. Совершайте покупки в Интернете только на проверенных сайтах. Внимательно проверяйте адресную строку браузера, она должна начинаться с https://*****.
10. При завершении работы с электронным кошельком – выйдите из приложения с помощью специальной кнопки, просто закрыть приложение – недостаточно.
11. Проверяйте реквизиты переводов и платежей, которые приходят в сообщениях от Банка.
12. Незамедлительно уведомляйте Банк, если электронный кошелек «взломан», скомпрометирован или с него без Вашего согласия списаны электронные денежные средства.
13. Если Вы потеряли мобильное устройство с СИМ-картой телефона, свяжитесь с Банком для блокировки электронного кошелька и оператором сотовой связи для блокировки СИМ-карты.
14. Не реагируйте на звонки/сообщения якобы от банка, если предлагается установить дополнительное программное обеспечение, изменить настройки, перерегистрироваться, повторно ввести данные, перезвонить на незнакомый номер, сообщить Ваши реквизиты для доступа к электронному кошельку, сказать платежный пароль, перевести электронные денежные средства и т.п.