Рекомендации по информационной безопасности при работе с Системой дистанционного банковского обслуживания «Крокус-Банк Онлайн»

При первом входе в Интернет-банк Клиент обязан изменить Пароль доступа, сформированный банком, на Пароль, который будет использоваться в дальнейшем. Рекомендации по выбору Клиентом Пароля указаны в Общих рекомендациях по безопасности.

Обязательно используйте пароль со степенью надежности «Надежный»

При проведении всех видов банковских операций необходимо подтвердить операцию вводом одноразового пароля из SMS-сообщения.

Общие рекомендации по безопасности

1. *Не сообщайте логин, пароль доступа к Системе ДБО, а также реквизиты счетов/банковских карт другим лицам.*
2. *Не передавайте никому, не оставляйте без присмотра Ваши электронные устройства (смартфоны, телефоны и т.д.), на которые приходят одноразовые пароли.*
3. *Не передавайте никому, не оставляйте в легкодоступных местах Вашу платежную карту и ее фотографию/*
4. *ПРЕЖДЕ чем вводить свои логин и пароль для входа в Интернет-банк:*
   - *внимательно проверьте адрес интернет-банка, введенный в адресную строку, вплоть до каждого знака;*
   - *проверьте, что соединение со страницей Интернет-банка действительно происходит по защищенному протоколу SSL (Secure Sockets Layer). Об этом свидетельствует наличие пиктограммы закрытого замка на панели браузера*  .
5. *Обратите внимание, что мошенниками могут быть созданы сайты, визуально напоминающие банковский сайт, специально для незаконного получения Вашей персональной информации.*
6. *ПИН-код, код CVV (на обратной стороне карты), логин и пароль к системе дистанционного банковского обслуживания – это Ваша конфиденциальная информация. Не сообщайте их никому, включая сотрудников Банка.*
7. *Не сохраняйте и не храните Ваши ПИН-код, код CVV (на обратной стороне карты), логин и пароль к системе дистанционного банковского обслуживания на мобильных устройствах, флешках или на любых других, не предназначенных для секретного (зашифрованного) хранения носителях информации.*
8. *Ограничьте доступ посторонних лиц к Вашим электронным устройствам, с помощью которых осуществляется работа с системой ИПБ-онлайн.*
9. *Не используйте устройства третьих лиц для подключения к системам для совершения финансовых операций.*
10. *Избегайте осуществления входа в Систему в местах, где услуги Интернета являются общедоступными, например, Интернет-кафе. Если же пришлось осуществить операцию с компьютера общего пользования, ОБЯЗАТЕЛЬНО после этого измените Ваш пароль на личном компьютере. Это имеет большое значение, так как существует риск перехвата Ваших конфиденциальных данных при помощи специальных программ, встроенных в компьютер общего доступа, без Вашего ведома.*
11. *Ограничьте информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Старайтесь не использовать компьютер, с которого Вы осуществляете переводы денежных средств, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.*

12. *Используйте для работы в Интернет-банке компьютер, на котором установлено современное антивирусное программное обеспечение, и следите за регулярным обновлением его баз данных и за тем, чтобы обновления системного и прикладного ПО устанавливались своевременно, даже если включено автоматическое обновление.*
13. *Не устанавливайте программы, скачанные из недоверенных источников. Для мобильных устройств настоятельно рекомендуем использовать только официальные магазины Google Play и App Store.*
14. *Не переходите по ссылкам на неизвестные источники.*
15. *Регулярно контролируйте состояние Вашего счёта.*
16. *Регулярно меняйте пароль для входа в Интернет-банк.*
17. *При необходимости передать кому-либо (продать) Ваше электронное устройство (флеш-накопитель, смартфон, планшет, компьютер и т.д.) убедитесь, что вся Ваша конфиденциальная информация, а также платежные приложения надежно удалены с устройства.*
18. *Если Вы потеряли мобильный телефон, на который приходят SMS с разовым паролем, немедленно заблокируйте вашу SIM-карту или доступ в Интернет-банк, обратившись в Банк по телефону: +7 (495) 228-12-44.*
19. *Помните, что Банк не направляет своим клиентам ни электронные письма, ни SMS-сообщения с просьбой уточнить их персональные данные.*
20. *Рекомендации по составлению пароля:*
    - *Пароль должен содержать не менее 8 символов;*
    - *Включать буквы верхнего и нижнего регистра;*
    - *Пароль не должен содержать идущие подряд символы — например, 123456789 или qwerty.*