

ПАМЯТКА КЛИЕНТА

о возможных угрозах хищения денежных средств с использованием Системы «iBank 2» и способах защиты

Сегодня хакерские атаки на счета клиентов - физических лиц, мошенничество с использованием вирусных программ – это не миф, а реальная угроза. При этом кража средств зачастую происходит из-за недостаточного внимания и конфиденциальности данных со стороны самих клиентов.

Хищение средств со счетов возможно при получении злоумышленниками доступа к логину и паролям. Для исключения несанкционированного доступа в Систему «iBank 2» ООО МИБ «ДАЛЕНА» проводит комплекс мероприятий для повышения Вашей информационной и финансовой безопасности.

Убедительно просим Вас ознакомиться с «Памяткой о возможных угрозах хищения денежных средств с использованием Системы «iBank 2» и способах защиты» и настоятельно рекомендуем придерживаться правил, указанных в ней. Они позволят защитить Ваши счета и информацию от взлома.

- ✓ **Не ставьте «пустые» или простые пароли**, например, 123456, qwerty – и периодически меняйте их. Рекомендуемая частота смены паролей -1 раз в месяц.
- ✓ **Используйте разные пароли для разных систем (вход в windows, вход в Систему «iBank 2», электронная почта).**
- ✓ **Рекомендуется соблюдать следующие требования при создании пароля:**
 - использовать числа (0-9);
 - использовать Заглавные буквы
 - использовать строчные буквы
 - использовать специальные символы (@,#,\$,%и т.д.).
- ✓ **Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.** Если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление паролей, срочно сообщите об этом в Службу технической поддержки клиентов Банка.
- ✓ **Ни при каких условиях не сообщайте Ваш Пароль никому**, включая сотрудников Банка.
- ✓ **Проверяйте, что соединение с Системой «iBank 2» происходит в защищенном режиме SSL <https://dalенabank.ru/>**, удостоверьтесь, что сертификат SSL соединения действителен (идентификационные данные сертификаты подтверждены).
- ✓ **Прежде чем пройти авторизацию**, убедитесь, что Вы находитесь на главной странице

Интернет-Банка. Он всегда доступен по адресу - https://dbo.dalenabank.ru/web_banking/

- ✓ **Подтверждение Ваших финансовых операций осуществляется посредством SMS.** Обязательно ознакомьтесь с информацией во входящих сообщениях, сверьте ее с проводимой операцией.
- ✓ **Помните, что Банк никогда не просит подтверждать отмену операции при помощи SMS.**
- ✓ **Ни в коем случае не храните Ваш Пароль** на носителях информации, включая компьютер и телефон.
- ✓ **После окончания работы в Системе «iBank 2»** обязательно завершайте сеанс, используя кнопку "Выход".
- ✓ **При возможности не пользуйтесь Интернет-Банком** в общедоступных местах, таких как интернет-кафе. При необходимости использования, смените Пароль с Вашего персонального компьютера или телефона, как только появится возможность.
- ✓ **Установите и обновляйте антивирус на Вашем компьютере, телефоне.** Действие вирусных программ может быть направлено на запоминание и передачу конфиденциальной информации злоумышленникам.
- ✓ **Используйте программное обеспечение из проверенных и надежных источников,** выполняйте регулярные обновления.
- ✓ **При возникновении подозрений, что Ваш Пароль стал известен посторонним,** незамедлительно смените Пароль или заблокируйте доступ в Систему «iBank2» самостоятельно или путем обращения в Банк.
- ✓ **При возникновении подозрений, что кто-то посторонний имеет доступ к Вашим счетам в Системе «iBank2»,** незамедлительно заблокируйте доступ в Систему «iBank2» самостоятельно или путем обращения в Банк и примите меры по смене Логина и Пароля.