Корпоративным клиентам
пользователям системы
«Интернет-банк «FAKTURA.RU»

Уважаемые клиенты!

АО «БАНК ОРЕНБУРГ» обращает Ваше внимание, что для обеспечения безопасной работы в системе интернет-банк необходимо соблюдать рекомендации и требования правил информационной безопасности, с которыми Вы можете ознакомиться ниже:

1. Защитите компьютер, с которого Вы осуществляете работу в системе ДБО.

Приступая к работе с системой ДБО, помните, что компьютер, с которого Вы будете осуществлять дистанционное управление Вашим банковским счётом, должен быть надёжно защищён от несанкционированного доступа и вредоносного программного обеспечения (компьютерных вирусов).

1. Не используйте для работы с системой ДБО чужой компьютер, установленный в общедоступном месте.
2. Установите на вход в Ваш компьютер пароль, даже если кроме Вас этим компьютером никто не пользуется. Количество неудачных попыток ввода пароля должно быть обязательно ограничено.
3. Не пользуйтесь нелицензионным (пиратским) программным обеспечением. Оно зачастую содержит вредоносные компоненты, позволяющие удалённо следить за работой Вашего компьютера, пересылать Вашу ключевую информацию злоумышленнику, а нередко и управлять Вашим компьютером через Интернет.
4. Своевременно обновляйте операционную систему.
5. Обязательно установите антивирусные программы. Обеспечьте их регулярное обновление, желательно в автоматическом режиме.
6. Антивирусное программное обеспечение должно действовать постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, с удалением обнаруженных вредоносных программ.
7. Убедитесь, что на Вашем компьютере отключены средства предоставления удалённого доступа, позволяющие осуществлять удалённый контроль за Вашей работой.
8. У пользователя, осуществляющего повседневную работу в системе «Интернет-банк», должны отсутствовать права администратора операционной системы.
9. Включите аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ. Постоянно просматривайте журнал таких событий и реагируйте на ошибки.
10. Используйте при входе в Интернет сетевые экраны, разрешив доступ только к доверенным ресурсам сети.
11. Запретите в межсетевом экране соединение с сетью «Интернет» по протоколам *ftp, smtp*. Разрешите соединения *smtp* только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
12. При работе в Интернете не соглашайтесь на установку каких-либо дополнительных программ.
13. Осуществляйте загрузку компьютера только с установленного в нём жёсткого диска. Средствами BIOS отключите возможность загрузки с иных внешних устройств. Доступ к BIOS компьютера должен быть закрыт паролем.
14. Не используйте Ваш компьютер с установленной на нём системой ДБО «Интернет-банк» для целей, не связанных с исполнением Ваших должностных обязанностей.

Помните, ***Ваш компьютер – важный инструмент для управления Вашими финансами!***

2. Вход в систему и обмен документами осуществляйте через защищённое соединение.

Вход и обмен документами в Системе «Интернет-банк» осуществляется через Интернет в защищённом режиме с помощью протокола SSL.

1. Проверяйте, действительно ли соединение происходит в защищённом режиме SSL. Убедитесь, что адресная строка в браузере начинается с https://. «S» означает «secure» (защищённый). Если эта буква отсутствует, значит Вы находитесь на незащищённом веб-сайте, и вводить свои данные нельзя.
2. Убедитесь в том, что соединение установлено именно с сайтом системы по адресу: https://faktura.ru/
3. Одним из распространенных способов мошенничества является предложение злоумышленников ввести Ваши логин и пароль на поддельном сайте, адрес которого может отличаться незначительно, например, одной буквой или тире. Если Вы обнаружили подобный сайт, сообщите об этом в Банк. Если Вы не уверены в безопасности Интернет-ресурса, не рискуйте.

3. При использовании мобильной версии интернет-банка рекомендуется:

1. Производить установку приложения Faktura.ru Business только из авторизованного магазина приложений (Google Play и App Store).
2. Установить код доступа на ваше мобильное устройство.
3. Установить и своевременно обновлять лицензионные антивирусные программы на вашем мобильном устройстве.
4. Всегда совершать выход из Приложения Faktura.ru Business с помощью пункта меню ≪Выйти≫ после окончания работы.
5. Не хранить логин и пароль для доступа, а также код доступа в Приложение на своём мобильном устройстве или в общедоступном месте, не записывать его на бумагу.
6. Ни при каких обстоятельствах не сообщать никому (в том числе работникам банка, родственникам и друзьям) логин, пароль и код доступа в Приложение.
7. Никогда не отвечать на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашиваются коды доступа, разовые пароли, персональная конфиденциальная информация.
8. В случае утери мобильного устройства или в случае обнаружения подозрительных действий, совершенных от вашего имени в Сервисе, незамедлительно смените логин и пароль, а также обратитесь в банк.

4. Соблюдайте меры по предотвращению несанкционированного доступа к ключу электронной подписи и парольной информации.

Безопасность работы в системе ДБО «Интернет-банк» строится на уникальности и конфиденциальности Вашего ключа электронной подписи (далее – ЭП) и персональной парольной информации. Её невозможно подделать, но, к сожалению, можно украсть. Применяйте все возможные меры для предотвращения потери, раскрытия, искажения и несанкционированного использования ключа ЭП и парольной информации. Несоблюдение этого требования является основной причиной утери денежных средств при работе с системами ДБО.

1. Не оставляйте внешний носитель с ключами ЭП постоянно подключенным к компьютеру. Используйте ключ ЭП только во время работы Системы «Интернет-банк».
2. Храните ключевой носитель в недоступном для посторонних лиц месте.
3. Если для проведения технического обслуживания, установки программного обеспечения на компьютере, используемом для работы с системой ДБО, Вы приглашаете технических специалистов, тем более сторонних, всегда контролируйте их действия. Не позволяйте им что-либо делать с Вашим компьютером, если Вы подключены к системе ДБО, а в компьютере находится ключевой носитель.
4. Никому не сообщайте логин и пароли, используемые в системе ДБО.
5. Не отвечайте на подозрительные письма, сообщения или телефонные звонки с просьбой прислать секретный ключ, сообщить PIN-код, пароль и другие конфиденциальные данные. **Банк НИКОГДА не запрашивает у клиентов конфиденциальную информацию!**

5. Выполняйте требования к формированию паролей.

Парольная защита является одним из важных способов по предотвращению несанкционированного доступа к системе ДБО на Вашем компьютере. Степень надёжности такой защиты в первую очередь зависит от того насколько Вы правильно формируете свои пароли.

1. Регулярно, не менее одного раза в месяц, производите смену паролей доступа к Вашему компьютеру и к установленной на нём системе ДБО.
2. Пароли должны иметь длину не менее 8 символов. Среди них должны быть сочетания букв и цифр из разных наборов символов.
3. Никогда не используйте в качестве паролей свои персональные данные (дата рождения, номер паспорта и т. д.), а также данные Ваших близких людей (дата рождения, имя дочери и т. д.).
4. Не используйте в качестве паролей простые и логически закономерные комбинации («1234», «11111», «qwerty» и т. д.).
5. Не назначайте пароль, используемый Вами до этого в других системах и сервисах.

6. Обязательно производите плановую, а в некоторых случаях и внеплановую смену паролей.

Кроме плановой смены паролей производите обязательную внеплановую смену паролей в следующих случаях:

- смена ответственных лиц, имеющих право доступа к системе ДБО (при увольнении, переводе на другой участок работы и т. д.);
- обнаружение фактов доступа неуполномоченных лиц к ключевой информации (а также при подозрении о таком доступе, в том числе и удалённом доступе по сети).

7. Используйте дополнительные меры обеспечения безопасности.

Настройте сервис SMS-уведомлений и/или E-mail уведомлений об отправке и исполнении Ваших документов, а также обо всех Ваших входах в систему «Интернет-банк».

ВАЖНО!

В случаях если:

- Вы заподозрили, а тем более Вам стало известно о компрометации ключей ЭП (утере, факте передачи ключа ЭП третьи лицам и т. д.),
- во время работы с ДБО Вы обнаружили чьё-то постороннее воздействие на Ваш компьютер, например, самопроизвольное перемещение мыши, набор каких-либо команд или какие-нибудь другие несанкционированные Вами действия, а также в случае появления при работе в системе ДБО нестандартных запросов, дополнительных страниц или дополнительных данных,
- в «Журнале сеансов работы» Вы обнаружили факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время);
- в выписке обнаружены несанкционированные Вами расходные операции либо Вы получили уведомление об операции, которую не совершали,

незамедлительно отключите смарт-ключ (если он подключен) от компьютера, обратитесь в Банк по телефону (3532) 343-191, а также предоставьте в Банк письменное заявление о приостановлении доступа в систему ДБО с описанием обстоятельств произошедшего.

Являясь клиентом Банка, своевременно предоставляйте достоверную информацию для связи с Вами.

Соблюдение вышеперечисленных правил позволит Вам существенно снизить риски, связанные с использованием системы «Интернет-банк», и предотвратить несанкционированный доступ к Вашим денежным средствам.