Рекомендации по обеспечению информационной безопасности
при работе в системе ДБО Faktura.ru

Уважаемый Клиент!

Безопасность работы в системе Faktura.ru обеспечена комплексом организационных и логических мер, направленных на предотвращение мошенничества и разглашения конфиденциальной информации.

Со стороны клиента безопасность работы в системе обеспечивается выполнением следующих рекомендаций:

Общие рекомендации по обеспечению безопасности при работе в Интернет

При работе в Интернет рекомендуем Вам соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах.

1. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
2. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
3. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
4. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
5. Ограничить список IP-адресов, с которых будет разрешена работа в системе ДБО Faktura.ru, направив в банк письмо с перечнем разрешенных IP-адресов. Наиболее предпочтительно использовать при работе статические IP-адреса, что позволяет задействовать встроенный в систему механизм IP-фильтрации в полной мере.
6. Установить и своевременно обновлять на компьютере антивирусное ПО (NOD32, AVP Kaspersky, Symantec AntiVirus и т.д.).
7. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
8. При выходе в Интернет использовать сетевые экраны (Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам Сети.
9. Запретить в межсетевом экране соединение с интернет по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
10. Не давать разрешения неизвестным программам выходить в интернет.
11. При работе в интернет не соглашаться на установку каких-либо дополнительных программ.
12. Осуществлять информационное взаимодействие с Банком и другими кредитными организациями только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные WEB-порталы/сайты, обычная и электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в Банке или других кредитных организациях.

Рекомендации по обеспечению безопасности при работе в системе ДБО Faktura.ru

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей финансовых интернет-систем файлов с секретными ключами ЭП и пароли, вводимые с клавиатуры. Трояны распространяются через e-mail, по каналам ICQ, Skype, через принадлежащие преступникам сайты.

Зафиксированы случаи заражения компьютеров и среди пользователей системы Faktura.ru. При этом злоумышленники похищают ключ ЭП и пароль к нему, что позволяет совершать операции от имени клиента.

Обращаем Ваше внимание на то, что хранение закрытого ключа ЭП на жёстком диске недопустимо.

Для того чтобы защитить Ваши средства, настоятельно рекомендуем использовать на компьютере, с которого осуществляется работа с системой Faktura.ru, следующий комплекс дополнительных мер безопасности:

- Подключить дополнительные средства защиты: **разовые SMS-пароли**, которые будут приходить на указанный Вами номер мобильного телефона. Пароль необходимо вводить для подтверждения входа в систему Интернет-банк и платежей, относимых системой контроля Faktura.ru к категории потенциально рисковых.
- Настроить сервис **«SMS-уведомления об отправке платежных документов в банк»** в разделе «Безопасность». Дополнительно можно настроить **E-mail-уведомления** об отправке и исполнении документов, а также обо всех входах в Интернет-банк.
- Контролировать состояние счёта (путем просмотра выписки).
- Обращать внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в систему, а также в специальном разделе «Безопасность -> Журнал сеансов работы»).
- Подключайте носитель ключевой информации (токен, flash-карта, смарт-карта) только на время работы с системой ДБО Faktura.ru по окончании сеанса носитель с ключом необходимо извлечь.

ПРОСИМ ВАС НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В БАНК ПРИ ВОЗНИКНОВЕНИИ СЛЕДУЮЩИХ СИТУАЦИЙ:

1. На компьютере, используемом для работы в интернет-банке, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
2. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
3. В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS или e-mail-уведомление об операции, которую не совершали.
4. Вы получили SMS или e-mail-уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

Рекомендуем Вам хранить файлы секретного ключа ЭП не на традиционных носителях (flash-карта, дискета и т.п.), а на специализированной смарт-карте с USB-считывателем. На сегодняшний день использование таких носителей — самая радикальная мера противодействия хищениям вредоносными программами (троянами) секретных ключей ЭП.

Рекомендации по выбору пароля

Не делайте простые и легкие пароли (111111,12345,abcdefg,qwerty и т.п.). Не выбирайте в качестве пароля дату рождения, номер телефона и другие данные, которые легко узнать. Пароль должен быть не короче 8-ми символов. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@ # $ & * % и т.п.). Пароли должны быть незапоминающимися. При выборе между Password и Jfhru195ki1@_) отдайте предпочтение второму. Любой пароль со смысловой нагрузкой небезопасен.

Не передавайте пароли третьим лицам и не записывайте пароли на носители ключевой информации (токены, flash-карты, смарт-карты).