Рекомендации

по соблюдению требований информационной безопасности
при работе Клиентов по системе Интернет-Клиент-Банк

Для снижения рисков, возникающих при дистанционном банковском обслуживании, в том числе с применением интернет-технологий, КБ «Альтернатива» (ООО) настоятельно рекомендует Вам выполнить следующие требования:

1. Общие требования безопасности при работе в интернете:

1.1. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.

1.2. Своевременно обновлять операционную систему из доверенных источников или встроенными средствами ОС (установка патчей, критических обновлений).

1.3. В системе работать под правами пользователя. Не использовать права администратора без явной необходимости.

1.4. Антивирусное ПО должно быть запущено постоянно, с момента загрузки компьютера и до его выключения. Обновление базы данных антивирусного ПО должно производиться ежедневно!

1.5. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов и вредоносного ПО. Обнаруженное вредоносное ПО должно быть незамедлительно удалено.

1.6. При выходе в Интернет следует использовать сетевые экраны. Блокировка всплывающих окон браузера Интернет должна быть включена. Рекомендуется разрешать доступ только к доверенным ресурсам.

1.7. При работе в интернете не соглашаться на установку каких-либо дополнительных программ, в том числе надстроек поисковых сайтов.

1.8. При работе программ обмена мгновенными сообщениями, принимать сообщения только от известных отправителей, не принимать и не передавать посредством таких сервисов файлы.

1.9. Не переходить по ссылкам, полученным от неизвестных или сомнительных источников, Не запускать на компьютере, использующемся для работы в системе «Банк-Клиент» постороннее по.

2. Общие требования настройки персонального компьютера при работе в интернете:

2.1. На компьютере следует включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, Администратор должен периодически просматривать журнал и реагировать на ошибки.

2.2. Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (ПО).

2.3. Контролировать работоспособность антивирусного ПО ежедневно, выполнять полную проверку ПК не реже одного раза в неделю.

2.4. При выходе в Интернет использовать сетевые экраны, разрешив доступ только к доверенным ресурсам.

2.5. Запретить в сетевом экране исходящее соединение с сетью Интернет по всем протоколам, за исключением HTTP и HTTPS, Разрешить SMTP-соединения только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики. Входящие соединения должны быть полностью запрещены.

2.6. При выявлении прикладных программ неизвестного назначения удалить неизвестное ПО.

3. Требования к персональному компьютеру, используемому при работе в системе Интернет-Клиент-банк:

3.1. Доступ к компьютеру с установленной Системой Интернет Клиент-Банка должен быть только у ограниченного круга лиц, в том числе через информационно-вычислительную сеть.
3.2. На компьютере должно быть установлено только лицензионное программное обеспечение, помните - использование нелицензионного ПО это не только правонарушение, но и огромная брешь в Вашей системе безопасности, которой могут воспользоваться мошенники.
3.3. Не рекомендуется устанавливать на компьютер средства удаленного доступа.
3.4. Должен быть установлен и обновлен антивирус.
3.5. Должен быть настроен межсетевой экран.
3.6. Пароли учетных записей, обладающих правами администратора, должны быть сложными.
3.7. Учетная запись «Гость» должна быть выключена.
3.8. Не должно быть учетных записей с пустыми паролями или паролями по умолчанию.
3.9. Должны быть установлены все обновления безопасности к установленной операционной системе.
3.10. Версия браузера, при использовании Internet Explorer, рекомендуется не ниже 9.0.
3.11. Для того чтобы защитить ваши денежные средства, настоятельно рекомендуем производить регулярный контроль состояния счета путем просмотра выписки.
3.12. Перед отправкой распоряжений в Банк необходимо проверить их количество и суммы, на предмет наличия нелегитимных. В случае обнаружения незамедлительно сообщить в Банк.

4. Также просим Вас незамедлительно обращаться в банк при возникновении следующих ситуаций:

4.1. Утерян или украден USB токен с ключами Интернет-Клиент-банка, утеряны пароли.
4.2. На компьютере, используемом для работы в системе Интернет-Клиент-банк обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
4.3. Имеется подозрение на проникновение в систему посторонних лиц, в выписке обнаружены несанкционированные вами расходные операции.
4.4. При посещении системы Интернет-Клиент-банк имеются существенные изменения внешнего вида системы без уведомления об обновлении со стороны банка.
4.5. У Вас не работает система Интернет-Клиент-банк по неизвестным причинам.
4.6. Недопустимо оставлять компьютер с активной Системой «Клиент-Банк» без присмотра, также недопустимо оставлять включенными в компьютер USB токены вне работы в системе Интернет-Клиент-Банк.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошенничества.

Сотрудники Банка готовы оказать помощь по вопросам соблюдения требований безопасности при работе в сети Интернет и использования системы Интернет-Клиент-банк