Уважаемые клиенты, напоминаем вам, что для работы в Системе Банк-Клиент следует соблюдать простые правила безопасности:

Правила выбора пароля:

1. Устанавливайте свой пароль самостоятельно, без участия третьих лиц.
2. Пароль должен содержать не менее 6 различных символов. Чем сложнее будет пароль, тем труднее его будет подобрать.
3. Обязательно смените пароль в том случае, если он стал известен третьему лицу.
4. Не используйте в качестве пароля:
- последовательности символов состоящие из одних цифр (в том числе даты, номера телефонов и т.п.);
- последовательности повторяющихся букв или цифр;
- подряд идущие в раскладке клавиатуры или в алфавите символы;
- имена и фамилии.

Не сообщайте третьим лицам пароль для входа в Систему Банк-Клиент

Не храните данные для входа в систему на компьютере.

Не оставляйте эту информацию в доступных местах, например, в виде записки на рабочем столе или наклейки на мониторе. Подобную информацию рекомендуется хранить исключительно в надежном месте, например, в сейфе.

Регулярно обновляйте антивирус и операционную систему

Используйте только лицензионную антивирусную программу!

Рекомендуем использовать решения от ведущих компаний в данной сфере, например:
Антивирус Касперского
Eset NOD32
Dr.web
Norton AntiVirus

Приобретайте программное обеспечение только в специализированных магазинах или с официальных сайтов производителей! Ни в коем случае не качайте сомнительные антивирусы из интернета, которые сами по себе могут содержать вредоносные файлы!

Позвольте антивирусу и операционной системе обновляться в автоматическом режиме. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов. Проверяйте антивирусом сменные носители (USB-flash, USB-hdd и прочее) перед началом использования.

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Если у вас есть подозрение, что ваш логин и пароль украдены, как можно быстрее смените ваш пароль в Системе Банк-Клиент или через телефонный центр «НБ Траст»(ОАО).

Если настройками вашего компьютера занимается ответственный сотрудник (системный администратор), следует показать ему данное сообщение.

Установите пароль для входа в операционную систему

Для более безопасной работы, следует установить пароль для входа в операционную систему.

Не используйте в качестве пароля номер телефона, фамилию владельца и т.д. Постарайтесь, чтобы пароль нельзя было угадать, добавьте цифры, заглавные буквы. Не забывайте регулярно менять пароль и держать его в тайне. Доступ к учетной записи, с которой осуществляется работа в Системе Банк-Клиент, должен быть строго ограничен! Компьютер, с которого осуществляется подготовка и отправка Электронных документов в Банк, необходимо выделить в отдельную доверенную зону, исключив его из общей локальной сети организации.

На компьютере не должны запускаться программы, полученные из непроверенных источников (особую опасность могут представлять программы, полученные по электронной почте или через Интернет).

Рекомендуется выделить отдельный компьютер и использовать его только для работы в Системе Банк-Клиент под учетной записью локального пользователя с минимальным набором прав, необходимых для функционирования системы.

Если настройками вашего компьютера занимается ответственный сотрудник (системный администратор), следует показать ему данное сообщение.

Не оставляйте электронную подпись в компьютере после окончания работы в Системе Банк-Клиент

Категорически не рекомендуется хранить электронную подпись (ЭП) на жестких дисках вашего компьютера!

Храните ЭП на съемных носителях (например, на флешке).

Извлекайте носители с ЭП из компьютера каждый раз после завершения работы в Системе Банк-Клиент.

Храните носители с ЭП в надёжном месте, например, в сейфе.

Не посещайте сомнительные сайты

Чтобы минимизировать вероятность заражения компьютера вирусами, постарайтесь использовать только проверенные сайты, необходимые для работы.

Не официальные новостные сервисы, развлекательные порталы, социальные сети, и прочие сайты, могут содержать вирусы. Даже разовый переход из поисковой системы по ссылке на сомнительный сайт может стать причиной заражения!

Никогда не соглашайтесь на установку каких-либо дополнительных программ с

неизвестных Вам сайтов!

Не открывайте письма от неизвестных отправителей

При работе с электронной почтой не доверяйте письмам от неизвестных отправителей, они могут содержать в себе вирусы!

Не переходите по ссылкам, приведенным в таких письмах. Не открывайте приложенные файлы.

Письма от НБ «Траст» приходят только с адресов домена @trust.ru

Настоятельно рекомендуется все файлы, пришедшие по электронной почте, в отдельном порядке проверять антивирусом перед открытием

Обращайте внимание!

Мошенники проводят массовые email-рассылки, маскируясь под бренд банка, целями которых может быть:

- заманивание получателей сообщений на сайты-ловушки, на которых под различными предлогами мошенники попытаются получить персональные данные (идентификатор и пароль для входа в Систему Банк-Клиент, криптографические ключи и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц.
- принуждение под различными предлогами получателей писем на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла.

Используйте только официальные контактные данные для связи с банком

Актуальную контактную информацию вы всегда можете посмотреть на нашем сайте www.trust.ru

Банк никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, криптографические ключи и пр.);
- не отправляет сообщения с формой для ввода Ваших персональных данных;

Рекомендуемые действия для юридических лиц при обнаружении несанкционированного платежа

Действия в случае несанкционированного платежа
PDF, 265 КБ

В случае утери ключей или подозрении на мошенничество обязательно свяжитесь с нами:

+7 495 647-98-77 (для жителей Москвы)
8 800 200-22-09 (для жителей других регионов, звонок по России бесплатный).
cb@trust.ru

Банк обращает Ваше внимание на то, что выполнение вышеописанных

рекомендаций позволит существенно минимизировать риски несанкционированного
списания денежных средств с ваших счетов.