Уважаемые клиенты!

Использование средств для дистанционного банковского обслуживания (пластиковые карты, интернет-банкинг и т.п.) всегда связано с повышенными рисками. Для того, чтобы работа в НС-ОНЛАЙН была не только удобной, но и более защищенной, просим Вас до начала работы ознакомиться с рекомендациями по безопасности.

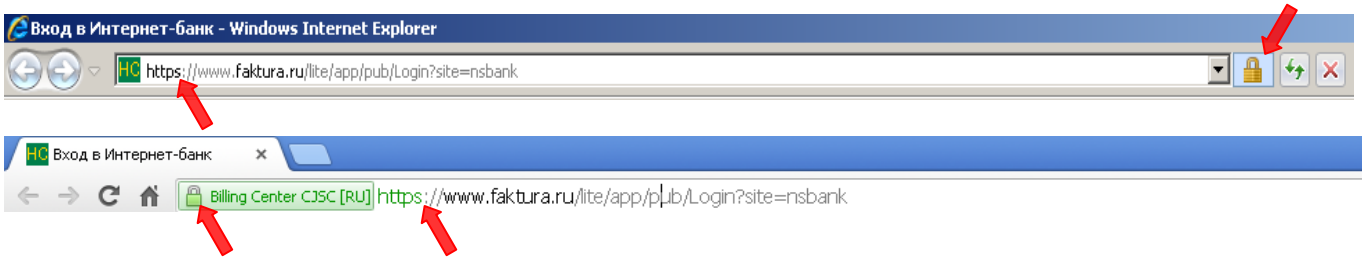
Распечатайте для себя эти рекомендации, чтобы в любой момент иметь их под рукой.

Как Банк защищает Вас:

Для обеспечения безопасности проводимых операций в НС-ОНЛАЙН используются следующие средства защиты:

Защищенное соединение (SSL-шифрование)

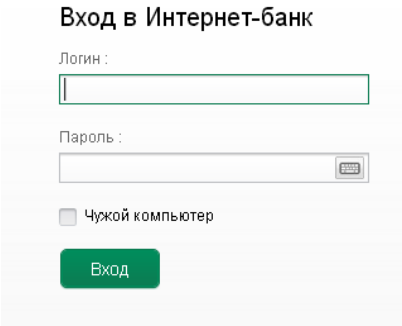
Соединение и работа с системой НС-ОНЛАЙН осуществляется через общедоступную сеть Интернет, поэтому для защиты канала, по которому компьютер пользователя соединяется с сервером, используется защищенный режим SSL. Признаком установки защищенного соединения является то, что адрес НС-ОНЛАЙН начинается с https:// (обязательно символ s), а в браузере появляется изображение замка (справа или слева от адресной строки, либо справа вверху/внизу браузера). Кликнув по замку, можно убедиться в подлинности сертификата.



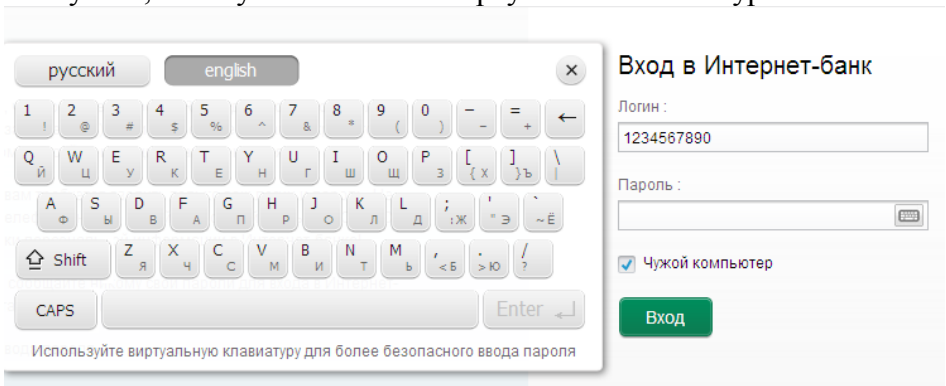
Виртуальная клавиатура

Виртуальная клавиатура повышает степень защищенности вашего пароля от перехвата злоумышленниками. Пользоваться виртуальной клавиатурой просто:

– Обратите внимание, что на странице входа должны вводиться **только логин и пароль**, никакой дополнительной информации запрашиваться не должно;

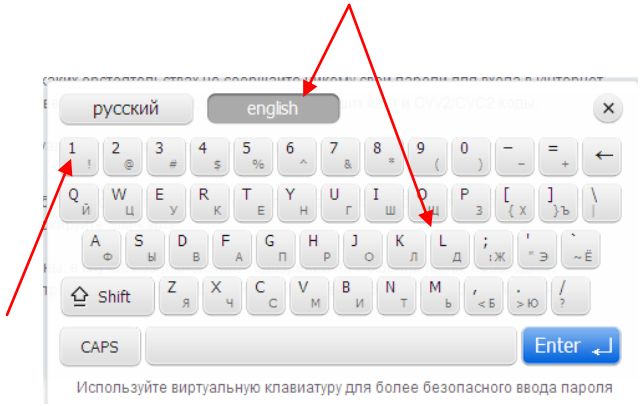


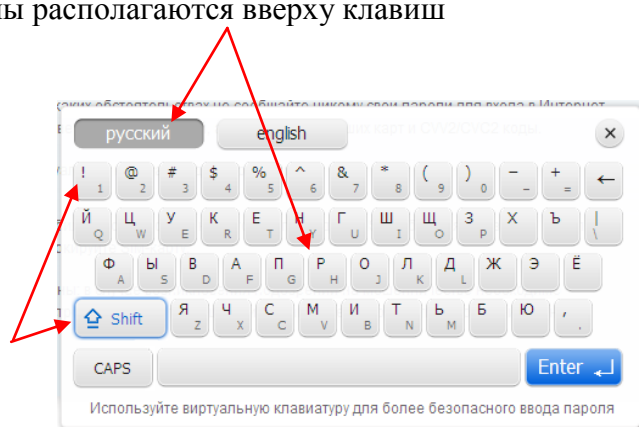
– после ввода логина при переходе на поле пароль, виртуальная клавиатура появится сама. Пожалуйста, пользуйтесь именно виртуальной клавиатурой!



– при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к НС-ОНЛАЙН;

– если необходимо ввести заглавную букву или символ нажмите клавишу **Shift**, переключение между заглавными и строчными – клавиша **Caps**, переключение между русским и английским алфавитом – клавиши **русский** и **english**, удаление предыдущего символа – клавиша **<--**. Активные символы располагаются вверху клавиш

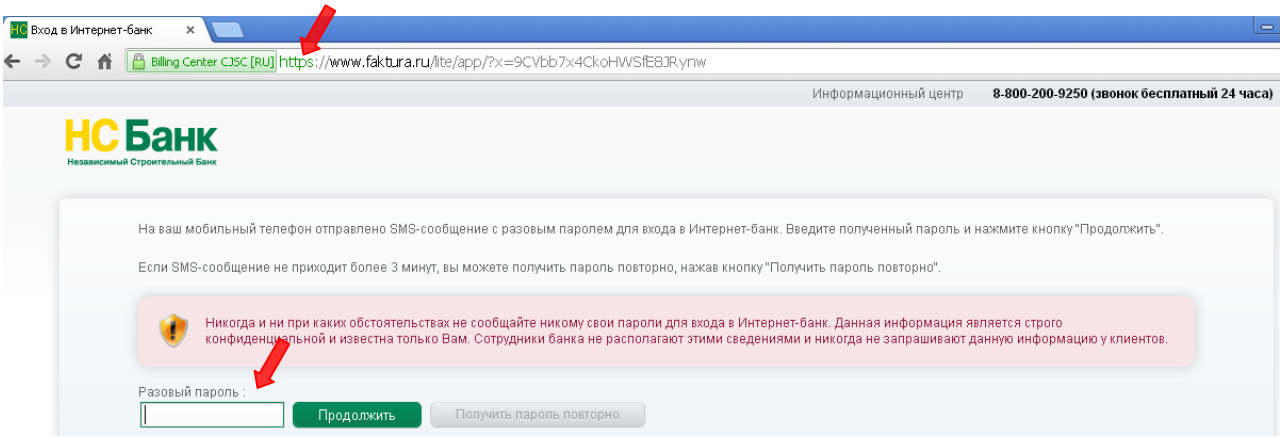




– для окончания набора пароля нажмите **Enter**.

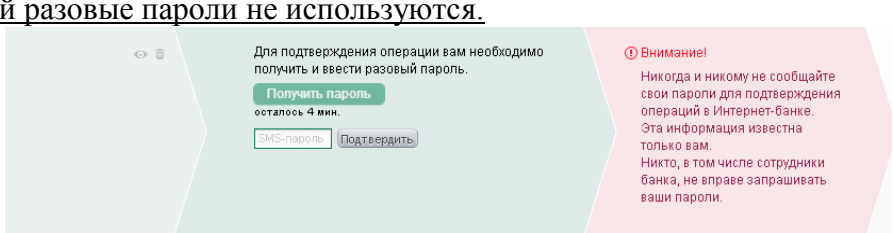
Разовые пароли для входа в НС-ОНЛАЙН

Разовый пароль используется для входа в НС-ОНЛАЙН и для проведения платежных операций. Для получения разового пароля необходим мобильный телефон, номер которого был указан Вами при подключении услуги НС-ОНЛАЙН. Разовый пароль присылается в sms-сообщении. При вводе разового пароля для входа в НС-ОНЛАЙН снова обратите внимание на заголовок страницы и на то, что никакой дополнительной информации, кроме разового пароля (например, номер Вашего мобильного телефона), запрашиваться не должно:



Разовые пароли для проведения операций

Для совершения операций: после ввода всех необходимых платежных данных, система предложит ввести разовый пароль для совершения операции. Для получения разового пароля нужно нажать на кнопку «Получить пароль», после чего пароль будет доставлен в sms-сообщении на Ваш мобильный телефон (порядок получения разового пароля подробно изложен в Руководстве пользователя). Обратите внимание, что разовый пароль может только подтвердить платёж, для отмены платежей разовые пароли не используются.



Текст sms-сообщения, которое содержит разовый пароль, также содержит краткую информацию о реквизитах платежа. *Например, для оплаты мобильной связи сообщение будет выглядеть так:*

Пароль XXXXXX
До ДД.ММ чч:сс мск
N номер перевода

Сумма: 100.00 RUR,
Тел. 916…
МТС

Как Вы можете позаботиться о себе:

Обновляйте операционную систему и другие программы на Вашем компьютере.

Используйте лицензионную операционную систему. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые компанией-производителем. Копируйте обновления только с официальных сайтов компаний-производителей.

Используйте дополнительные средства безопасности

Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.

Установите и обновляйте антивирус на Вашем компьютере.

Вирусные программы могут запоминать и отсылать всю информацию злоумышленникам. Используйте современное, лицензионное антивирусное программное обеспечение и следите за его регулярным обновлением. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

Если у Вас есть подозрение, что Ваши логин и пароль украдены, как можно быстрее смените Ваш пароль в Интернет-банке или заблокируйте доступ в Интернет-банк по телефону

8-800-200-9250

Для входа в НС-ОНЛАЙН нужен только логин, пароль и специальный разовый пароль

На первой странице НС-ОНЛАЙН не должно быть никаких дополнительных полей для ввода такой информации, как разовый пароль, номер Вашего мобильного телефона или пластиковой карты. Если появились такие поля – сообщите об этом по телефоне, указанному выше. Разовый пароль для входа в НС-ОНЛАЙН запрашивается на следующей странице. Разовый пароль для входа в НС-ОНЛАЙН высылается в sms-сообщении и не содержит никаких реквизитов платежей.

Никому не говорите Ваш пароль и разовый пароль.

Пароли в НС-ОНЛАЙН (на вход и на подтверждение операции) – это Ваша личная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте никому свои пароли, включая сотрудников Банка. Сотрудники Банка никогда не просят сообщить или ввести куда-либо конфиденциальную информацию (пароль или разовый пароль).

Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, потому что это может привести к его краже и компрометации.

Проверяйте адрес НС-ОНЛАЙН, он должен начинаться с https://www.faktura.ru/...

НС-ОНЛАЙН всегда доступен только по адресу https://www.faktura.ru/... Вас могут пытаться обмануть, предлагая оставить Ваши пароль и логин на поддельном сайте (например, http://faktura.comm.org). Если Вы обнаружите такой сайт, обязательно сообщите об этом по телефонам, указанным выше!

Разовый пароль действует только на подтверждение платежа.

Для отмены операции просто ничего не делайте и ничего не подтверждайте! Отменить операцию в НС-ОНЛАЙН при помощи разового пароля невозможно! Никто из сотрудников Банка никогда не попросит у Вас ввести разовый пароль для отмены операции.

Внимательно проверяйте параметры операции в sms-сообщении, содержащем разовый пароль.

Информация в нем должна совпадать с Вашей операцией в НС-ОНЛАЙН, которую Вы хотите подтвердить. Если эта информация не совпадает, не вводите разовый пароль и сообщите об этом по телефону, указанному выше!

Используйте для звонков в Банк номер телефона, указанный выше.

Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, который будет пытаться Вас обмануть. В случае подозрения на мошенничество звоните в службу поддержки НС-ОНЛАЙН только по номеру, указанному в этой памятке!

Проверяйте, используется ли защищенное соединение – https://www.faktura.ru/

Проверяйте, действительно ли соединение происходит в защищенном режиме SSL – справа или слева от адресной строки, либо справа вверху/внизу браузера должен быть изображен значок закрытого замка.

Корректно завершайте работу в НС-ОНЛАЙН

Завершение работы с системой выполняйте путем выбора соответствующего пункта меню «Выйти» - это удалит из браузера информацию о параметрах работы в НС-ОНЛАЙН.

Защитите свой мобильный телефон

Не устанавливайте на мобильный телефон, на который Банк отправляет sms-сообщения с подтверждающим разовым паролем, приложения, полученные от неизвестных Вам источников. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через sms/mms/email - сообщения.

При утрате мобильного телефона, на который Банк отправляет sms-сообщения с подтверждающим разовым паролем, Вам следует как можно оперативней обратиться к своему оператору сотовой связи и заблокировать телефонную SIM-карту.

Не заходите в НС-ОНЛАЙН с того же мобильного телефона, устройства, на который приходят sms-сообщения с подтверждающим разовым паролем.

Что делать, если Вам пришло SMS на подтверждение операции, которую Вы не совершали:

Вам пришло sms-сообщение для подтверждения операции, но Вы не совершаете никаких операций? Скорее всего, компьютер заражен вирусом.

Не используйте этот одноразовый пароль, даже если Вам позвонил сотрудник банка и попросил сделать это.

Установите или обновите антивирус.

Выполните полную проверку компьютера на вирусы.

Проверьте файл hosts на наличие в нем лишних адресов. Для того, чтобы сделать это, нужно открыть в Блокноте (Пуск -> Программы -> Стандартные -> Блокнот) файл C:/windows/system32/divers/ets/hosts. В этом файле не должно быть строки nsbank.ru или faktura.ru. Если такая строка есть – её необходимо удалить и сохранить файл.

Стандартно выполняемой (без символа # в начале строки) в файле hosts является только одна строка:

127.0.0.1 localhost

Если Вы сами не вносили изменений в этот файл, наличие других строк без символа # в начале строки может быть признаком вирусного заражения Вашего компьютера.

Проверьте SSL-сертификат при доступе к Интернет-банку (сделать это можно нажав на иконку замка в Вашем браузере). Сертификат должен быть действительным для faktura.ru (поле «Кому выдан).

Заходите в Интернет-банк с этого компьютера только после того, как Вы выполнили все рекомендации, перечисленные выше.

О факте такого SMS обязательно сообщите по телефону

8-800-200-9250

Что делать, если есть подозрение на мошенничество:

Если Вы получили подозрительное письмо или sms-сообщение, необходимо обратиться в службу поддержки по телефону

8-800-200-9250

Если есть подозрения, что Ваши логин и пароль стали известны кому-либо, обязательно смените пароль самостоятельно на незараженном компьютере или безопасно получите новый пароль в Банке.