**Уважаемые клиенты!**

Обращаем Ваше внимание на то, что системы дистанционного банковского обслуживания (системы ДБО) являются постоянной мишенью для разного рода злоумышленников. Создаваемые и распространяемые ими вредоносные программы направлены на кражу денег со счетов клиентов.

Вы сможете защитить свой компьютер от вредоносного кода, если будете следовать приведенным ниже рекомендациям:

Используйте только лицензионное программное обеспечение, полученное из надежных источников. Взломанное или загруженное с сомнительных интернет-ресурсов программное обеспечение может содержать в себе вредоносный код.

Регулярно устанавливайте (или не отключайте автоматическое) обновления для операционной системы и программ, выпускаемые их производителями.

Используйте на своем компьютере учетную запись с правами администратора/root только тогда, когда Вам нужно изменить настройки системы или установить программное обеспечение. Для повседневной работы создайте и используйте учетную запись с ограниченными правами.

Не посещайте сомнительные сайты и сайты, распространяющие пиратское программное обеспечение или аудио/видео файлы. Большинство подобных сайтов может заразить Ваш компьютер различного рода вирусами.

Используйте современные антивирусные программы и регулярно обновляйте как антивирусные базы, так и компоненты самих антивирусных программ.

Регулярно проводите полное сканирование системы антивирусной программой.

Если Вы получили по электронной почте сообщение от неизвестного отправителя с вложенным файлом или интернет-ссылкой, ни в коем случае не открывайте вложение и не проходите по интернет-ссылкам.

Не доверяйте настройку Вашего компьютера и установку программ случайным людям.

Мобильные устройства также могут быть подвержены заражению вредоносным кодом, если Вы используете мобильный банкинг, Банк рекомендует следовать приведенным ниже правилам:

Так же, как и в случае с почтой на компьютере, будьте очень внимательны, когда переходите по ссылкам, присланным адресатами из Вашего списка контактов, и ни в коем случае не переходите по ссылкам, присланными неизвестным адресатом.

Никогда не делайте неофициальную «перепрошивку» Вашего устройства для расширения прав доступа к системе.

Устанавливайте все программы на мобильное устройство лично и только из проверенных источников (App Store и Google Play).

Если Вам пришло SMS с паролем для платежа, который Вы не совершали, известите об этом банк! Ни в коем случае не вводите и никому не сообщайте пришедший пароль!

В случае утери мобильного телефона, на который приходят SMS с разовым паролем, немедленно заблокируйте SIM-карту! Если Вы сменили номер мобильного телефона – обязательно сообщите в банк.

Если Вам пришло уведомление о блокировке SIM-карты - немедленно сообщите в банк для блокировки доступа в систему ДБО!

Запишите контактный телефон банка. Если Вас просят связаться с банком по другому номеру, это может означать попытку мошенничества.

Не указывайте номер мобильного телефона, на который приходят SMS с разовым паролем, в социальных сетях и других открытых источниках.

Проверяйте, какие программы запущены на Вашем устройстве и что они выполняют.

Будьте особенно внимательны, подключаясь к сети Wi-Fi в общественных местах, и ни в коем случае не подключайтесь к неизвестным Wi-Fi точкам. Владелец такой точки может загрузить на Ваше устройство вредоносную программу.

Внимательно следите за предложениями Банка о внедрении новых средств защиты. Новые угрозы появляются постоянно и оперативное внедрение современных средств защиты - важное условие обеспечения сохранности Ваших финансов.

В случае подозрения на заражение Вашего компьютера или мобильного устройства программами, содержащими вредоносный код, рекомендуем проверить остаток денежных средств на Вашем банковском счете и прекратить использовать данный компьютер или мобильное устройство для осуществления банковских платежей, а также незамедлительно обратиться к квалифицированным IT-специалистам.

Для завладения чужими деньгами мошенники идут на различные хитрости и одна из них - создание фальшивых сайтов. Они создают подложный сайт, который выглядит почти так же, как сайт банка или сайт, с помощью которого Вы производите финансовые расчеты через Интернет. Затем, обманным путем, пытаются добиться того, чтобы Вы посетили этот сайт и ввели на нем свои конфиденциальные данные. Приведенные ниже рекомендации помогут снизить риск несанкционированного доступа к Вашей конфиденциальной информации и избежать потери денежных средств.

Пользуйтесь последними версиями программ для просмотра интернет-сайтов и лицензионных антивирусных программ.

Будьте внимательны при получении почтовых сообщений от неизвестных отправителей и почтовых сообщений с предложением перейти по ссылке (переход по данной ссылке может привести на фальшивый сайт или заразить Ваш компьютер вирусом), ввести данные Вашей банковской карты или логин и пароль от системы ДБО для приостановки ошибочного платежа, подтверждения или обновления чего-либо, ввести персональные данные. Никогда не реагируйте на письма с сомнительным содержанием или рекламой. Не доверяйте предложениям с сайтов, если они слишком хороши, чтобы быть правдой.

Всегда проверяйте правильность адреса сайта, на том ли сайте Вы вводите свой пароль (фальшивые сайты зачастую очень похожи на свои оригиналы, различия могут заключаться лишь в одной букве).

Следите за тем, чтобы при входе в систему ДБО Банка было установлено защищенное соединение, в верхней строке программы для просмотра интернет-сайтов, где отображается адрес сайта, должна присутствовать буква s после http – https:/.

Всегда проверяйте наличие значка шифрования соединения, рядом с адресом сайта, в виде закрытого замочка.

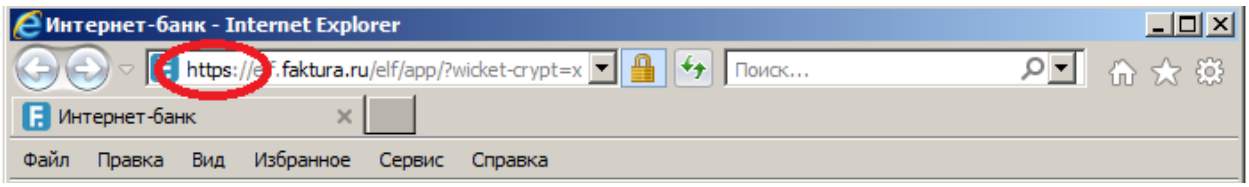
Будьте бдительны, не заходите на сайты онлайн магазинов, кликая по ссылкам в почтовых сообщениях, рекламе на сайтах, сенсационным новостям и ссылкам в социальных сетях.

В случае получения писем, в которых Вас просят от лица Банка сообщить свои конфиденциальные данные, уведомьте Банк о получении такого сообщения и ни в коем случае не следуйте инструкциям и требованиям данного письма.

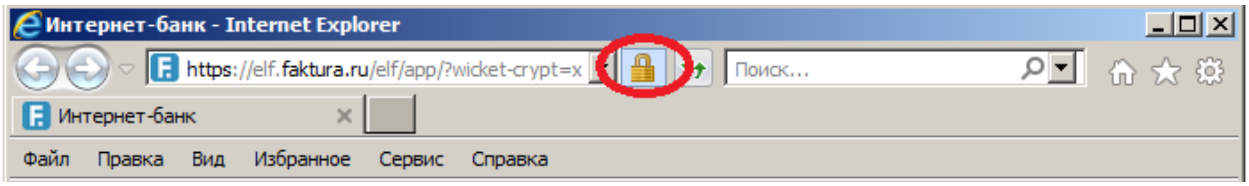
Аккуратность и внимательность при пользовании Интернетом помогут Вам избежать несанкционированного доступа мошенников к Вашим денежным средствам.

Как визуально можно проверить, на настоящем ли сайте Вы находитесь:

1. Посмотрите вверх страницы клиента в системе ДБО, адрес должен начинаться с https (обязательно с буквой s)




2. Справа или слева от этой строки должна быть картинка с закрытым замочком.




В некоторых программах для просмотра интернет-сайтов такой замочек может выглядеть и по-другому, например, так:


3. Кликнув на замочек – можно проверить подлинность сертификата шифрования (т.е. кто шифрует этот сайт и действительно ли он имеет на это право, не истёк ли срок действия сертификата).

4. На странице для входа в систему ДБО должны запрашиваться только Ваш логин и пароль. Если на этой странице Вас просят ввести номер пластиковой карты, ПИН-код или другую дополни-

тельную информацию – не вводите никакой информации и незамедлительно сообщите об этом в банк.

5. Обращайте внимание на дизайн сайта, элементы дизайна, правописание названий, адреса и телефоны для обратной связи. Как правило, на поддельных сайтах указывают телефоны мошенников, позвонив по которым Вы рискуете оказаться их жертвой. Контактные телефоны банка можно найти на официальном сайте: **https://nsbank.ru**