Внимание!!!
Уважаемые клиенты Банка!
Обращаем ваше внимание, что Банком России выявлены случаи, когда с помощью вредоносной компьютерной программы подменяются платежные поручения, сформированные в системе 1С

Вредоносная компьютерная программа производит подмену реквизитов получателя (счет и ИНН получателя, но название оставляет неизменным). После подмены платежное поручение направляется в систему ДБО (дистанционное банковское обслуживание через доступ в Интернет).

Суть мошеннической схемы состоит в следующем:
1. Клиент формирует с помощью 1С платежное поручение и отправляет его на выгрузку в систему ДБО.

2. 1С, как правило, формирует текстовый файл **kl_to_1c.txt,** содержащий служебную информацию (перечень расчетных счетов, период, остатки и обороты по счетам и т.д.).

3. Вредоносная компьютерная программа отслеживает появление этого файла и производит подмену реквизитов получателя (счет и ИНН получателя, но название оставляет неизменным).

4. После подмены платежное поручение направляется в систему ДБО.

В целях безопасности клиентам-пользователям системы 1С рекомендуется не пренебрегать стандартными правилами:

1. Использовать антивирусное средство, поддерживать его базы в актуальном состоянии, не реже 1 раза в неделю проводить полное сканирование системы, в которой генерируется файл **kl_to_1c.txt.**

2. Выполнять все рекомендации по работе с вложениями, пришедшими из подозрительных источников, не открывать вложения-исполняемые файлы и не включать макросы в документах Microsoft Office, если не уверены в надежности отправителя.

3. Подтверждать платеж только после проверки всех реквизитов получателя средств.