


**Рекомендации по безопасному использованию  
системы дистанционного банковского обслуживания  
физических лиц «Инбанк–online»**

1. Для доступа к системе дистанционного банковского обслуживания (ДБО) физических лиц «Инбанк–online» используйте адрес <https://online.in-bank.ru/> или ссылку с официального сайта Банка (<https://in-bank.ru/>).  
Не рекомендуется осуществлять вход в систему ДБО по ссылкам, размещенным на сторонних сайтах или полученным по электронной почте, т.к. это может привести к компрометации Ваших учетных данных.
2. При обращении к системе ДБО «Инбанк–online», необходимо убедиться, что в начале адресной строки браузера, перед адресом <https://online.in-bank.ru/>, расположена иконка с изображением замка , означающего, что подлинность сайта подтверждена и соединение с сервером защищено.
3. Для работы с мобильных устройств в системе ДБО «Инбанк–online» доступна версия мобильного клиента. Приложение «Инбанк-online» необходимо устанавливать только из официальных магазинов приложений - Google Play или App Store.
4. Для входа в систему ДБО используется имя пользователя (логин) и пароль, созданные Клиентом самостоятельно при регистрации. Не сообщайте свой логин и пароль третьим лицам, включая сотрудников Банка.
5. Для доступа к устройствам, предназначенным для работы в системе ДБО «Инбанк–online», используйте пароль (код) или биометрическую идентификацию.
6. Не сохраняйте Ваш логин и пароль к системе ДБО в браузерах, текстовых файлах на компьютере, либо на других носителях информации, потому что это может привести к их компрометации и несанкционированному использованию.  
При подозрении на компрометацию логина/пароля в системе ДБО, необходимо незамедлительно обратиться в Контактный центр Банка.
7. Все операции в ДБО, в том числе первичная регистрация, подтверждаются SMS-сообщением с паролем (кодом), которое отправляется на номер мобильного телефона Клиента. Никому не сообщайте полученный пароль, в том числе и сотруднику Банка, не оставляйте телефон без присмотра.  
При утере/краже телефона или внезапном прекращении работы SIM-карты необходимо незамедлительно обратиться к провайдеру мобильной связи для блокировки/замены SIM-карты, а также в Контактный центр Банка для блокировки доступа в систему ДБО.
8. Своевременно устанавливайте доступные обновления операционной системы и приложений на устройство, с которого осуществляется вход в систему ДБО. Используйте антивирусное программное обеспечение, своевременно устанавливайте на него обновления антивирусных баз. Регулярно проводите полную антивирусную проверку всего устройства.
9. Не устанавливайте на устройство, с которого осуществляется вход в систему ДБО, приложения из неофициальных (недоверенных) источников. Не вносите изменения в операционную систему, т.к. это отключает механизмы защиты и может стать причиной вирусного заражения.
10. Не рекомендуется осуществлять вход в систему ДБО «Инбанк–online» с использованием чужих устройств, общедоступных сетей Wi-Fi (кафе, гостиницы, метро, офисные центры и т.п.), осуществлять обработку платежной информации в присутствии посторонних лиц.

**Сотрудники Банка, при осуществлении звонка Клиенту Банка, не запрашивают информацию о номере пластиковой карты, её сроке действия, CVV2/CVC2-коде, PIN-коде, логине/пароле для доступа в систему ДБО, кодовом слове, коде подтверждения из SMS!**

**Передача вышеуказанной информации другому лицу (в том числе сотруднику Банка) означает, что Вы предоставляете возможность другим лицам проводить операции по Вашим счетам.**

**При любых подозрениях на мошенничество следует незамедлительно обратиться в Контактный центр Банка по телефону +7 (495) 229-12-34 или 8 (800) 555-22-65.**

С уважением ООО «Инбанк»