ПЕРЕЧЕНЬ МЕР БЕЗОПАСНОСТИ

БПС-Сбербанк настоятельно рекомендует при пользовании системой Сбербанк Онлайн соблюдать следующие меры информационной безопасности:

- Для входа в Сбербанк Онлайн требуется только идентификатор (логин) и пароль. В случае если от Вас требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона, других личных данных), следует выйти из Сбербанк Онлайн и связаться с Банком.
- Отмена операций в Сбербанк Онлайн не предусмотрена. БПС-Сбербанк никогда не запрашивает пароли для отмены операций при пользовании Сбербанк Онлайн. Если Вам предлагается ввести пароль для отмены операции, следует выйти из Сбербанк Онлайн и связаться с Банком.
- При получении сеансового SMS-пароля убедитесь, что SMS-сообщение поступило от короткого имени BPSSBERBANK.
- Проверяйте, что установлено защищенное SSL-соединение (в правом нижнем углу браузера должен быть виден значок закрытого замка) с официальным сайтом Сбербанк Онлайн (https://i.bps-sberbank.by).
- Ни при каких обстоятельствах не разглашайте никому, включая сотрудников Банка, логин и пароль доступа, дополнительный пароль для подтверждения операций. Это Ваша личная конфиденциальная информация.
- Не пользуйтесь услугой Сбербанк Онлайн непосредственно через Интернет-обозреватель мобильного устройства (телефона, планшета и пр.), на который приходят сообщения с сеансовым SMS-паролем. Для мобильных устройств существуют собственные версии системы.
- При утрате мобильного устройства, на который Банк отправляет SMS-сообщения с сеансовым SMS-паролем или неожиданным прекращением работы SIM-карты, Вам следует оперативно обратиться к своему оператору сотовой связи и заблокировать SIM-карту.
- Пользуйтесь дополнительными возможностями Сбербанк Онлайн по повышению уровня безопасности (настройка видимости карт и счетов, изменение логина и пароль доступа, значения дополнительного пароля, номера мобильного телефона для доставки сеансового SMS-пароля и пр.). Для настройки используйте пункт «Безопасность» Личного меню.
- В целях повышения информационной безопасности необходимо изменять пароль доступа в систему Сбербанк Онлайн на регулярной основе (не реже, чем 1 раз в 90 дней).
- Не устанавливайте на мобильное устройство, на который Банк отправляет сеансовый SMS-пароль, приложения, полученные из неизвестных Вам источников. Помните, что БПС-Сбербанк не рассылает ссылки или указания на установку приложений через SMS/MMS/Email — сообщения.
- На сайте Сбербанк Онлайн всегда указаны официальные контактные телефоны: 148, Velcom, Life:), МТС 5 148 148.
- В целях безопасности Вы можете в пункте «Безопасность» Личного меню сформировать Журнал авторизации пользователя, чтобы отслеживать дату и время входа в Сбербанк Онлайн, платформу и IP-адрес компьютера, с которого осуществлялся вход в систему Сбербанк Онлайн.
- Для корректного закрытия сессии следует совершать выход из Сбербанк Онлайн с помощью кнопки Выход.
- При подозрении, что от Вашего имени осуществляются несанкционированные вами операции, Банк по своей инициативе может временно на срок до 2 часов заблокировать услуги Сбербанк Онлайн/Мобильный банк. Для возобновления потребуется связаться с Банком и подтвердить легитимность подключения и сделанных операций.
- Установите на Ваш компьютер антивирусные программы и старайтесь их своевременно обновлять. Обратите внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о вашем пароле доступа.
- Установите и используйте персональный брандмауэр (firewall) на Вашем компьютере для входа в Интернет, это позволит предотвратить несанкционированный доступ к информации на компьютере.