ПРАВИЛА БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БАНКИНГА АО PPF БАНК

Банк не несет какой бы то ни было ответственности за потерю данных, утечку личных данных, а также за иные неблагоприятные события, произошедшие в результате несоблюдения указанных ниже рекомендаций.

Поддержку и сопровождение для клиентов, пользующихся электронным банкингом (далее по тексту – ЭЛБ) предоставляет Центр обслуживания, действующий в рабочие дни с 8:00 до 18:00, номер телефона +420 224 175 901 (для Интернет банкинга, далее по тексту – ИБ) и АПИ, или +420 224 175 995 (для Хоумбанкинга, далее по тексту – ХБ). С Центром обслуживания можно связаться и по адресу электронной почты customer.service@ppfbanka.cz.

1. **Посещайте лишь хорошо известные Вам веб сайты. Пользуйтесь лишь безопасными паролями и надежно храните их.**

   Посещая какой бы то ни было веб сайт, убедитесь, что домен соответствует содержанию сайта.

   Пользуйтесь исключительно услугами, достойными доверия. Всякий раз убедитесь, что имеете дело с соответствующим провайдером.

   Для доступа к собственным адресам электронной почты, к аккаунтам в социальных сетях и т.д. используйте достаточно сильные пароли – содержащие, по меньшей мере, 8 знаков, комбинацию прописных и строчных букв, цифр и специальных знаков.

2. **Не открывайте сообщения электронной почты от неизвестных адресатов и/или с подозрительными реквизитами. Скачивайте и открывайте лишь файлы, которые вы ожидаете и которые от известных Вам отправителей.**

   Не открывайте файлы в приложениях, не проходите по ссылкам, содержащимся в подобных письмах электронной почты. **Ни в коем случае не сообщайте какие бы то ни было важные личные данные в ответ на требования, содержащиеся в полученных письмах электронной почты.** Не скачивайте и не открывайте файлы, содержащие неизвестный контент.

   Банк по собственной инициативе никогда не рассылает письма электронной почты, содержащие ссылки на свой веб сайт. Банк посредством упомянутых писем электронной почты никогда не требует от своих клиентов, чтобы они таким образом сообщили данные, открывающие доступ в систему ЭЛБ.

3. **Установите антивирусную и антишпионскую программу, активируйте их регулярную актуализацию. Установите важные актуализации, прежде всего, операционной системы.**

   Регулярно устанавливайте все доступные актуализации операционной системы, поисковых программ, а также всех иных программ и приложений, установленных в компьютере.

   Пользуйтесь исключительно легальными версиями программного обеспечения – нелегальные версии могут содержать вирусы, троянские и иные вредоносные программы. Такие программы, в частности, могут отсылать Ваши пароли их создателям. Компьютерные программы скачивайте исключительно с веб сайтов их производителей. Для скачивания приложений в смартфоны пользуйтесь исключительно официальными источниками (Google Play, Apple Store, Windows Phone Store).

   Ограничите доступ других людей к вашему компьютеру. Никогда не используйте общедоступный компьютер для доступа к АПИ, ИБ или ХБ.

PPF banka a.s., Evropská 2690/17, P.O. Box 177, 160 41 Praha 6
T: (+420) 224 175 888, F: (+420) 224 175 980, E: info@ppfbanka.cz
www.ppfbanka.cz

PPF Banka

4. **Выполняя обычные задачи в сети Интернет, не пользуйтесь профилем пользователя, содержащим права администратора. Не позволяйте иным лицам подключаться к сети Интернет посредством Вашего профиля пользователя.**

   Для выполнения обычных задач в сети Интернет входите в систему как обычный пользователь, права администратора используйте лишь в совершенно необходимых случаях. **Покидая компьютер, всякий раз закрывайте экран или же завершите коммуникацию с АПИ и ИБ, и /или ХБ и закройте соответствующее приложение.**

5. **ИБ включайте лишь на хорошо известном Вам компьютере, используя ссылку на главной странице Банка. Входя в систему ИБ, проверьте, действительно ли Вы связались именно с Банком. Убедитесь, что связь безопасна и надежно обеспечена.**

   Если необходимо использовать неизвестный для Вас компьютер, после выхода из системы ИБ необходимо удалить историю просмотров.

6. **Сертификат подписи системы ХБ храните не в компьютере, а на диске USB, который после завершения работы в системе ХБ отключайте от компьютера.**

7. **Чтобы сохранить сертификат пользователя в АПИ, используйте безопасное хранилище, для доступа к которому требуется пароль или ПИН-код.**

8. **Регулярно контролируйте движение средств на счетах, а также платежи посредством Дебетовой карточки. Установите в системе ИБ рассылку SMS или сообщений по электронной почте об избранных Вами изменениях на счете.**

   В системе ИБ можно установить рассылку сообщений о входе Пользователя в систему, об осуществленных транзакциях, о платежах посредством карточек и т.д. **Можно также установить рассылку сообщений иным лицам, нежели пользователям ИБ** – например, владельцам Дебетовых карточек. Подробнее см. Часть III Руководства пользователя для ИБ.

9. **Установите Лимиты Платежных поручений для Пользователей. В системе ИБ установите, по крайней мере, для одного Пользователя возможность авторизации от имени Клиента.**

   Можно установить Лимиты Времени и Транзакций, а также их комбинации.

   В системе ИБ Пользователь, обладающий правом авторизации требований от имени Клиента, может задать требование о блокировке иных Пользователей в случае возникновения каких бы то ни было подозрений относительно злоупотребления системой ИБ. Блокировка будет осуществлена в течение нескольких минут. Подробнее см. Коммерческие условия АО «ППФ банка» для Интернет банкинга и Часть III Руководства пользователя для ИБ.

10. **Пристально отслеживайте, действительно ли Вы подтверждаете заданное Вами платежное распоряжение или требование по отношению к Банку.**

    Перед подтверждением всегда сверяйте правильность введенных данных (например, сравните со счетом-фактурой, почтовой квитанцией и т.д.).

11. **Надежно храните все Элементы. Не сообщайте никому свои данные для доступа в систему, примите меры, чтобы их никто «не подсмотрел» в процессе их введения. Регулярно меняйте пароли для доступа систему ЭЛБ.**

    Все документы, полученные Вами от Банка (например, тексты договоров, конверты с данными для обеспечения доступа в систему ЭЛБ и т.д.) считайте конфиденциальными и храните в безопасном месте. **Если Вы откроете кому бы то ни было доступ к личным данным и/или Элементам безопасности, то тем самым Вы даете данному лицу возможность злоупотребить ими или же сообщить их третьим лицам.** Формируя пароль для входа в систему ЭЛБ, не пользуйтесь предсказуемыми данными, такими как имена, даты рождения, номера телефонов и т.д.

12. **Постоянно держите при себе мобильный телефон, предназначенный для рассылки СМС-кода доступа в систему АПИ или ИБ. ОТП-код и/или USB диск с размещенным на нем сертификатом подписи для доступа в систему ХБ храните в безопасном месте.**

    Данные, содержащиеся в памяти мобильного телефона, должны быть защищены посредством PIN-кода и иных элементов обеспечения безопасности, в зависимости от особенностей данного аппарата. ОТП-код и/или диск USB желательно хранить под замком.

PPF banka a.s., Evropská 2690/17, P.O. Box 177, 160 41 Praha 6
T: (+420) 224 175 888, F: (+420) 224 175 980, E: info@ppfbanka.cz
www.ppfbanka.cz

13. **Пристально отслеживайте, действительно ли Вы подтверждаете заданное Вами платежное распоряжение или требование по отношению к Банку.**

    Перед подтверждением всегда сверяйте правильность введенных данных (например, сравните со счетом-фактурой, почтовой квитанцией и т.д.).

14. **Уделяйте надлежащее внимание всем предупреждениям, которые выдает Ваши компьютер, а также тем, которые появляются на сайте Банка, и руководствуйтесь ими.**

15. **Немедленно свяжитесь с Банком, если система ЭЛБ или иных электронных банковских услуг ведет себя не стандартным образом, а именно:**

    - Если по электронной почте поступает сообщение, содержащее ссылку на веб сайт Банка;
    - Если у Вас возникло подозрение, что данные обеспечения доступа были взломаны;
    - Если ваш компьютер заражен или на вашем компьютере обнаружен вымогатель;
    - Если система ЭЛБ ведет себя подозрительно, например, СМС-коды не поступают, СМС-код содержит искаженные данные о платежи, необычное наименование сервера, данные имеют иную визуальную форму, появились новые шаги в процессе входа в систему и т.д.;
    - Если Вы лишились ОТП Токена или мобильного телефона, на который Вы получали СМС-код;
    - Если Вы лишились диска USB, на котором хранится сертификат доступа;
    - Если Вы выявили неправомерные отклонения в осуществленных транзакциях.

PPF banka a.s., Evropská 2690/17, P.O. Box 177, 160 41 Praha 6
T: (+420) 224 175 888, F: (+420) 224 175 980, E: info@ppfbanka.cz
www.ppfbanka.cz