Приложение № 7 к Условиям дистанционного банковского обслуживания физических лиц в системе Интернет-Банк «ББР Онлайн» ББР Банк (АО), утвержденное Приказом от __.__.2018 №___ и введенное в действие с __.__.2018

Руководство

по обеспечению безопасности при работе с системой Интернет–Банк «ББР Онлайн»

В соответствии с рекомендациями Банка России сообщаем Вам дополнительную информацию, необходимую для предотвращения неправомерного и несанкционированного доступа к информации клиентов Банка, при осуществлении дистанционного банковского обслуживания

1. Требования по защите Мобильного устройства, самостоятельно реализуемые Клиентом:

- регулярно обновляйте программы, операционную систему и прошивку Вашего Мобильного устройства. Обновления, как правило, предоставляются автоматически. При покупке нового устройства убедитесь, что обновления для операционной системы вашей модели доступны по запросу;
- на Мобильном устройстве, с которого планируется осуществлять подключение к Мобильному банку, должно быть установлено программное обеспечение, препятствующее проникновению и запуску вредоносных программ;
- Мобильное устройство не должно быть подвергнуто операциям повышения привилегий/ взлома операционной системы устройства (jail-break, rooting);
- устанавливайте на Мобильное устройство программы только от надежных и проверенных поставщиков, например, App Store, Google Play. И хотя платные сервисы или игры можно бесплатно получить у непроверенных поставщиков, вполне вероятно, что вместе с ними Вы установите на свое устройство вредоносное программное обеспечение;
- регулярно проверяйте пользовательские права и политику конфиденциальности, которую Вы приняли. Например, права на информацию о доступе к чтению SMS / PUSH или хранилищам данных. Многие приложения требуют излишние права на доступ к ресурсам Мобильного устройства;
- на Мобильном устройстве, использующем операционную систему Android, настройками должна быть запрещена установка приложений из непроверенных источников;
- используя Мобильное устройство, на котором установлен Мобильный банк, осуществляйте избирательную навигацию в информационно-телекоммуникационной сети «Интернет», не посещайте неизвестные сайты и не устанавливайте сомнительные приложения;
- не подключайте Мобильное устройство к компьютерам, безопасность которых не может быть гарантирована;
- измените код доступа по умолчанию и PIN-код SIM-карты. Не используйте ваш год рождения или другие легко угадываемые комбинации чисел. Настройте свое Мобильное устройство так, чтобы оно каждый раз запрашивало пароль или секретный шаблон. Используйте процедуру Аутентификации доступа к Мобильному устройству (ввод пароля для разблокировки Мобильного устройства), прежде чем приступить к совершению операций через Мобильный банк;
- если Мобильное устройство и/или SIM-карта украдены, незамедлительно сообщите об этом в Банк. Заблокируйте SIM-карту обратившись к Оператору мобильной связи.

2. Требования технической защиты стационарных и/ или переносных устройств, самостоятельно реализуемые Клиентом:

- Перед вводом Логина и Пароля обязательно убедитесь в том, что в адресной строке браузера указан Адрес Системы https://bbr.ru/;
- ограничите физический доступ к компьютеру, на котором используется система Интернет–Банк «ББР Онлайн», исключите бесконтрольный доступ в помещение, в котором он установлен. Если используете ноутбук, то не оставляйте его без присмотра;
- не доверяйте обслуживание этого компьютера посторонним лицам, не допускайте его использование посторонними лицами;
- используйте на компьютере только лицензионное программное обеспечение, дистрибутивы которого получены из надежных источников;
- установите на компьютер антивирусное программное обеспечение, обеспечьте автоматическое обновление антивирусных баз. Настройте еженедельное проведение полной антивирусной проверки компьютера;
- организуйте автоматическую установку обновлений безопасности операционной системы и другого установленного на компьютере программного обеспечения по мере их выпуска производителями;
- минимизируйте состав установленного на компьютере программного обеспечения;

- не допускайте установку на компьютер никаких программ для удаленного управления (Remote Administrator, VNC, Team Viewer и т.п.), заблокируйте на нем работу встроенного сервиса удаленного доступа к рабочему столу;
- полностью запретите или минимизируйте доступ по локальной сети к компьютеру;
- минимизируйте количество пользователей компьютера, установите для них надежные пароли, обеспечьте периодическую смену этих паролей;
- не работайте на компьютере под учетными записями, имеющими административные права. Административная учетная запись может использоваться только для установки программного обеспечения;
- настройте в BIOS компьютера возможность загрузки операционной системы только с основного жесткого диска, установите пароль на загрузку компьютера и вход в настройки BIOS;
- минимизируйте использование с этого компьютера иных интернет-ресурсов, не относящихся к работе в Системе, обновлению программного обеспечения и обновлению антивирусных баз. Использование компьютера для посещения посторонних интернет-ресурсов значительно повышает риск его заражения вредоносными программами;
- не используйте на компьютере средства электронной почты, программы обмена мгновенными сообщениями, сайты социальных сетей. Злоумышленники часто используют эти сервисы для рассылки вредоносных вложений, ссылок на сайты, распространяющие вредоносные программы или фишинговые сайты;
- установите на компьютер персональный межсетевой экран, настройте его таким образом, чтобы с компьютера был возможен доступ только к Системе, а также производителей установленного на компьютере программного обеспечения (включая антивирусную программу) для загрузки обновлений.

3. Общие организационные меры по защите информации, реализуемые Клиентом:

- следуйте рекомендациям по обеспечению безопасности, рассылаемым Банком по Системе;
- по всем вопросам, связанным с работой Системы, обращайтесь в службу технической поддержки Банка.
- регулярно, не реже 1 раза в 3 месяца, проводите смену пароля на вход в Систему;
- установленный Пароль для входа в Систему должен быть сложен для угадывания (отличаться от последовательности одинаковых символов, даты или года рождения Клиента и т.д.);
- никогда и никому не сообщайте пароль для входа в Систему, а Кодовое слово используйте исключительно для Аутентификации при обращении в Банк по телефонной связи. Следите за тем, чтобы Кодовое слово не стало известным посторонним лицам;
- ежедневно контролируйте операции по Вашим счетам, направляя в Банк запрос промежуточной выписки;
- завершайте работу с документами и банковскими счетами путем выхода из Системы (Меню → Выход);
- при подозрении, что Коды подтверждения стали известны посторонним лицам и/ или утрачена Карта одноразовых паролей, а также при получении уведомлений об Операциях по счету, которых точно не совершалось, незамедлительно обращайтесь в Банк и блокируйте свою учетную запись;
- в случае внезапного нарушения работы при работе с Системой, незамедлительно проинформируйте об этом Банк и проконтролируйте полученные Банком от Вашего имени платежные документы. Зафиксированы случаи, когда злоумышленники, отправив с компьютера «жертвы» платежный документ, выводили компьютер из строя для сокрытия следов преступления и уничтожения улик. После совершения хищения они стараются помешать «жертве» своевременно узнать о произошедшем и принять меры к остановке мошеннического платежа;
- Вы можете подключить Мобильное устройство или ноутбук к интернет-сервису, который позволяет дистанционно обнаружить потерянное или украденное устройство и, в случае необходимости, удаленно уничтожить все данные;
- если к Вам обращаются по телефону или электронной почте и, представляясь сотрудниками Банка, просят сообщить Ваш пароль или отправить Код подтверждения – не делайте этого, незамедлительно сообщите о произошедшем в Банк. Если к Вам обращаются с просьбой отправить по Системе платежный документ, для того, чтобы «вернуть ошибочно перечисленные средства» – сначала позвоните в Банк чтобы подтвердить легитимность данного запроса;
- если вы решили продать старое устройство, то не забудьте стереть личную информацию. Верните аппарат к заводским установкам.

Помните, что при работе со своими счетами в системе Интернет–Банк «ББР Онлайн» следует быть настолько же внимательными и бдительными, как при обращении с наличными деньгами в Вашем кошельке!