РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СИСТЕМЫ ДБО

Все термины, указанные в настоящем документе с заглавной буквы, используются в значении, определенном в Условиях предоставления дистанционного банковского обслуживания.

1. Общие рекомендации

1.1 Для доступа к мобильному устройству или в учетную запись на личном компьютере установите сложный пароль. Длина пароля должна быть не менее 7 символов. Пароль должен содержать символы минимум из 2 следующих символьных групп: цифры, заглавные и строчные буквы латинского алфавита.

1.2 Установите на свой компьютер/мобильное устройство лицензионное антивирусное программное обеспечение. Регулярно производите его обновление и полную антивирусную проверку компьютера/мобильного устройства, а также обновление операционной системы и используемых программ (браузера и иных прикладных программ). Используйте программное обеспечение только из проверенных и надежных источников.

1.3 Не храните на мобильном устройстве и/или компьютере конфиденциальную информацию о Вашем логине и пароле для доступа к Мобильному банку, Интернет-банку и/или Личному кабинету. Если такая необходимость все же есть, не храните информацию в явном виде.

1.4 Удаляйте конфиденциальную информацию в случае передачи мобильного устройства и/или компьютера другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек.

1.5 Обязательно сверяйте данные об операциях, указанные в полученных от Банка СМС-сообщениях, с данными по фактически совершенным операциям на предмет выявления несанкционированных операций.

1.6 После окончания работы в Интернет-банке, Мобильном банке или Личном кабинете обязательно завершайте сеанс, используя кнопку «Выход».

1.7 Ни при каких условиях не сообщайте /не передавайте информацию о Вашем логине, пароле, одноразовых паролях и иных сведениях, используемых для авторизации в каналах дистанционного обслуживания никому, включая сотрудников Банка. Также никому не сообщайте / не передавайте сведения о своем коде доступа, за исключением случая, когда Вам требуется сообщить информацию о коде доступа сотруднику Банка для авторизации в каналах дистанционного обслуживания.

1.8 При возникновении подозрений, что Ваши данные для доступа (логин или пароль) стали известны посторонним и/или в случае утери мобильного устройства незамедлительно заблокируйте доступ к Системе ДБО, обратившись в Банк по телефону 8 800 550 0770 и обязательно смените пароль.

2. Рекомендации по использованию Мобильного банка

2.1 Устанавливайте приложение Мобильный банк и его обновления только из приложений Apple AppStore / Google Play Market. Ссылки для установки указаны на сайте Банка www.letobank.ru. Издателем приложения Мобильный банк должны быть указаны: для операционной системы iOS - Leto Bank PJSC; для операционной системы Android - Leto Bank.

2.2 Не «взламывайте» систему защиты iPhone (jailbreak) и не открывайте «root» доступ для устройств на операционной системе Android, так как это делает уязвимым Ваше мобильное устройство.

2.3 Подключите элементы дистанционного управления (для дистанционной блокировки и дистанционного удаления данных с мобильного устройства при утрате мобильного устройства).

2.4 При утрате мобильного телефона (иного устройства), на который подключена услуга смс-информирования, направляются одноразовые пароли или на которое установлено приложение Мобильный банк, незамедлительно обратитесь к своему оператору сотовой связи для блокировки SIM-карты и в Клиентскую службу Банка для блокировки доступа к каналам Системы ДБО.

2.5 При смене номера телефона, обратитесь в Клиентский центр/Стойку продаж либо в Клиентскую службу Банка.

3. Рекомендации по использованию Интернет-банка

3.1. Прежде чем пройти авторизацию в Интернет-банке, убедитесь, что соединение происходит в защищенном режиме с использованием протокола HTTPS (появляется буква S в адресной строке: https://my.letobank.ru/ib), удостоверьтесь в правильности сертификата SSL-соединения. Ссылка для входа в Интернет-банк указана на сайте Банка www.letobank.ru.

3.2. Не пользуйтесь Интернет-банком в общедоступных местах, на компьютерах, безопасность которых вызывает сомнения (например, в Интернет-кафе, чужой компьютер). Если Вы все же заходили с чужого компьютера, смените пароль для входа в Интернет-банк с Вашего персонального компьютера, как только будет такая возможность.

3.3. Установите и используйте персональный брандмауэр (firewall) для входа в Интернет, это позволит предотвратить несанкционированный доступ к информации на Вашем компьютере.

3.4. Не пользуйтесь Интернет-банком на компьютере, который используется под учетной записью, имеющей права администратора системы, а также если имеется подозрение, что компьютер заражен вирусной программой. Симптомы заражения:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- произвольно, без участия пользователя, на компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь этого не инициировал;
- частые зависания и сбои в работе компьютера, медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.

3.5. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web-сайты, имеющие похожие адреса, или перенаправление на них с других ресурсов. К примеру, leto-bank.ru, letobahk.ru, letobamk.ru вместо верного letobank.ru. Внимательно проверяйте адрес сайта перед авторизацией или совершением операций. Если он отличается от https://my.letobank.ru/ib – не используйте данный сайт. Для входа в Интернет-банк перейдите по ссылке с сайта Банка www.letobank.ru или наберите адрес в браузере вручную.

4. Рекомендации по использованию Личного кабинета

4.1 Пользуйтесь Личным кабинетом через банкоматы/терминалы Банка, установленные в безопасных местах, оборудованных системой видеонаблюдения и охраны, (например, в государственных учреждениях, подразделениях Банка, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

4.2 Не пользуйтесь Личным кабинетом в банкоматах/терминалах, если:

- банкомат/терминал работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается);
- на банкомате/терминале установлены дополнительные устройства, не соответствующие конструкции банкомата/терминала;
- вблизи банкомата/терминала находятся подозрительные лица или есть вероятность, что люди, находящиеся в непосредственной близости, смогут увидеть указываемые Вами сведения и информацию, отображаемую на экране банкомата/терминала.

5. Дополнительные рекомендации

5.1 Банк рекомендует отслеживать информацию по вопросам информационной безопасности в связи с видоизменением способов мошеннических действий и информационных угроз.

Вам могут быть полезны следующие ресурсы:

- «Управление «К» предупреждает: будьте осторожны и внимательны!»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf
- «Вредоносные программы в интернете»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf
- «Владельцам пластиковых банковских карт»: http://mvd.ru/upload/site1/mvd1/liflets_out_2.pdf
- «Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf
- «Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf
- «Безопасный интернет – детям»: http://mvd.ru/upload/site1/mvd1/liflets_k_deti_06.pdf

5.2 Для обнаружения необходимости установки обновлений браузера рекомендуем Вам использовать сервис обнаружения уязвимостей: http://www.surfpatrol.ru/.

Внимание! По всем вопросам, связанным с дистанционным обслуживанием, Вы можете обратиться в Клиентскую службу Банка по одному из следующих телефонов:

- **8 800 550 0770** (для бесплатных звонков с любого телефона на территории Российской Федерации)**;**
- **+7 495 532 13 00** (для звонков из-за границы).