Правила безопасности при работе с интернет-банком МКБ Онлайн

1. Убедитесь в том, что соединение установлено по протоколу https, адресная строка содержит символ замка слева или справа от адресной строки. Это означает, что работа в системе осуществляется по безопасному каналу.
2. Для входа в систему НЕ НУЖНО вводить номер Вашего мобильного телефона, номер банковской карты, CVV2/CVC2 код.
3. Для входа в систему МКБ Онлайн вам необходимо вводить логин и пароль, одноразовый СМС-код или код с карты уникальных цифровых кодов. Другие данные не используйте.
4. Заходите в МКБ Онлайн по ссылке с официального сайта МКБ, не переходите по ссылкам в письмах с сомнительным содержанием.
5. Проверяйте параметры операции в СМС с одноразовым кодом.
6. В случае утери мобильного телефона, на который приходят одноразовые СМС-коды, немедленно заблокируйте/замените SIM-карту и смените номер телефона для СМС-сообщений в системе online.mkb.ru
7. Подтверждение операций осуществляется только посредством одноразового СМС-кода, короткого кода, кода с карты уникальных цифровых кодов или биометрией (Face ID, Touch ID). Не подтверждайте операции с помощью паспортных данных, пароля, номера телефона и других персональных данных.
8. В случае возникновения подозрений на мошенничество заблокируйте систему через Контакт-центр, по СМС с текстом online на номер +79037672667 и как можно скорее сообщите о происшествии в Банк.
9. Информируйте Банк о смене номера мобильного телефона, о замене SIM-карты.
10. Ни при каких обстоятельствах не раскрывайте свой пароль никому, даже сотрудникам Банка!
11. Установите на свой компьютер антивирус и постоянно обновляйте его.
12. Используйте на своем компьютере только лицензионное программное обеспечение.
13. Обеспечьте своевременную (по возможности автоматическую) загрузку и установку последних обновлений программного обеспечения.
14. Не заходите на сайты с сомнительным содержанием и не открывайте без проверки файлы, полученные в почтовых сообщениях и на съемных носителях от неизвестных лиц.
15. Храните персональные данные (логин/пароль, средства защиты, одноразовые коды, полные номера банковских карт и их CVV-код) по отдельности и в недоступном месте для посторонних.
16. Помните, чем сложнее Ваш пароль, тем сложнее его взломать мошенникам. Используйте цифры и буквы разного регистра, не расположенные на клавиатуре последовательно. Длина пароля должна быть не менее 8 символов. Осуществляйте регулярную смену пароля.
17. Отменить или аннулировать совершенную операцию возможно только через отделение Банка. Мы не предлагаем это сделать в системе.
18. При подозрении на наличие вирусов, в частности, при неожиданном прекращении реагирования программ или всей операционной системы на ваши действия («зависание» компьютера), снижении скорости работы, подозрительной сетевой активности, иных сбоях воздержитесь от использования интернет-банка.
19. Всегда завершайте работу в системе через кнопку «Выход».

Правила безопасности при работе с мобильным приложением МКБ Онлайн

1. Используйте только официальное приложение из магазина Google Play, App Galery и отечественные магазины приложений: NashStore, RuStore
2. Подтверждение операций осуществляется только посредством одноразового СМС – кода короткого кода, кода с карты уникальных цифровых кодов или биометрией (Face ID, Touch ID). Не подтверждайте операции с помощью паспортных данных, пароля, номер телефона и других персональных данных.
3. Для входа в систему МКБ Онлайн вам необходимо вводить логин и пароль или короткий код / использовать функцию Touch ID/Face ID/. Другие данные не используйте.
4. Не заходите на сайты с сомнительным содержанием и не открывайте без проверки файлы, полученные в почтовых сообщениях и на съемных носителях от неизвестных лиц.
5. Установите на свой смартфон или планшет антивирус и постоянно обновляйте его.
6. Обеспечьте своевременную (по возможности автоматическую) загрузку и установку последних обновлений программного обеспечения.
7. Информируйте Банк о смене номера мобильного телефона, о замене SIM-карты. Для входа в приложение НЕ НУЖНО вводить номер Вашего мобильного телефона, номер банковской карты, CVV2/CVC2 код.
8. В случае утери мобильного телефона, на который приходят одноразовые СМС-коды, немедленно заблокируйте/замените SIM-карту, и смените номер телефона для СМС-сообщений в системе online.mkb.ru
9. В случае возникновения подозрений на мошенничество заблокируйте систему через Контакт-центр, по СМС на номер +79037672667 и как можно скорее сообщите о происшествии в Банк.
10. Ни при каких обстоятельствах не раскрывайте свой пароль никому, даже сотрудникам Банка!
11. Проверяйте параметры операции в СМС с одноразовым кодом.
12. Отменить или аннулировать совершенную операцию возможно только через отделение Банка. Мы не предлагаем это сделать в мобильном приложении.
13. Храните персональные данные (логин/пароль, средства защиты, одноразовые коды, полные номера банковских карт и их CVV-код) по отдельности в недоступном для посторонних месте.
14. Завершайте работу в приложении через «Завершение сессии».