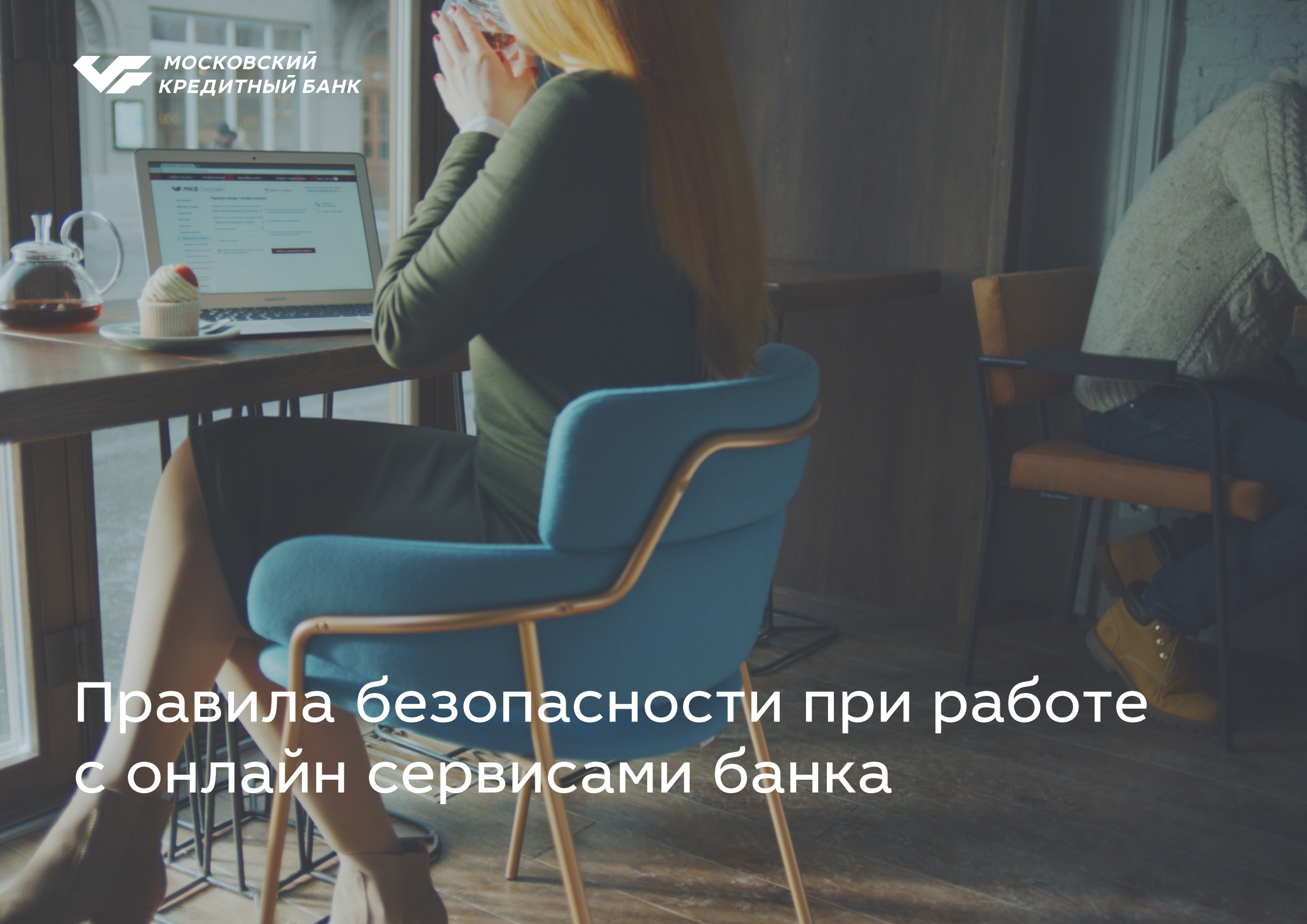

Правила безопасности при работе с онлайн сервисами банка

Правила безопасности при работе с интернет-банком МКБ Онлайн

- Убедитесь в том, что соединение установлено по протоколу https, адресная строка зеленого цвета и содержит символ замка слева или справа от адресной строки. Это означает, что работа в системе осуществляется по безопасному каналу.
- Для входа в систему НЕ НУЖНО вводить номер Вашего мобильного телефона, номер банковской карты, CVV2/CVC2 код.
- Для входа в систему МКБ Онлайн вам необходимо вводить логин и пароль, одноразовый SMS-код или код с карты уникальных цифровых кодов. Другие данные не используйте.
- Заходите в МКБ Онлайн по ссылке с официального сайта МКБ, не переходите по ссылкам в письмах с сомнительным содержанием.
- Проверяйте параметры операции в SMS с одноразовым кодом.
- Используйте виртуальную клавиатуру для ввода логина и пароля.
- В случае утери мобильного телефона, на который приходят одноразовые SMS-коды, немедленно заблокируйте/замените SIM-карту и смените номер телефона для SMS-сообщений в системе online.mkb.ru
- Подтверждение операций осуществляется только посредством одноразового SMS-кода или кода с карты уникальных цифровых кодов. Не подтверждайте операции с помощью паспортных данных, пароля, номера телефона и других персональных данных.
- В случае возникновения подозрений на мошенничество заблокируйте систему через Контакт-центр, по SMS с текстом online на номер +79037672667 и как можно скорее сообщите о происшествии в Банк.
- Информируйте Банк о смене номера мобильного телефона, о замене SIM-карты.
- Ни при каких обстоятельствах не раскрывайте свой пароль никому, даже сотрудникам Банка!
- Установите на свой компьютер антивирус и постоянно обновляйте его.
- Не заходите на сайты с сомнительным содержанием и не открывайте без проверки файлы, полученные в почтовых сообщениях и на съемных носителях от неизвестных лиц.
- Храните персональные данные (логин/пароль, средства защиты, одноразовые коды, полные номера банковских карт и их CVV-код) по отдельности и в недоступном для посторонних месте.
- Помните, чем сложнее Ваш пароль, тем сложнее его взломать мошенникам. Используйте спец. символы, цифры и буквы разного регистра. Длина пароля должна быть не менее 9 символов.
- Отменить или аннулировать совершенную операцию возможно только через отделение Банка. Мы не предлагаем это сделать в системе.
- Всегда завершайте работу в системе через кнопку «Выход».

Правила безопасности при работе с мобильным приложением МКБ Мобайл

- Используйте только официальные приложения из магазинов App Store, Google Play.
- Подтверждение операций осуществляется только посредством одноразового SMS - кода или кода с карты уникальных цифровых кодов. Не подтверждайте операции с помощью паспортных данных, пароля, номер телефона и других персональных данных.
- Для входа в систему МКБ Мобайл вам необходимо вводить логин и пароль или короткий код / использовать функцию Touch ID. Другие данные не используйте.
- Не заходите на сайты с сомнительным содержанием и не открывайте без проверки файлы, полученные в почтовых сообщениях и на съемных носителях от неизвестных лиц.
- Установите на свой смартфон или планшет антивирус и постоянно обновляйте его.
- 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.
- В случае утери мобильного телефона, на который приходят одноразовые SMS-коды, немедленно заблокируйте/замените SIM-карту, и смените номер телефона для SMS-сообщений в системе online.mkb.ru
- В случае возникновения подозрений на мошенничество заблокируйте систему через Контакт-центр, по SMS на номер +79037672667 и как можно скорее сообщите о происшествии в Банк.
- Ни при каких обстоятельствах не раскрывайте свой пароль никому, даже сотрудникам Банка!
- Проверяйте параметры операции в SMS с одноразовым кодом.
- Отменить или аннулировать совершенную операцию возможно только через отделение Банка. Мы не предлагаем это сделать в мобильном приложении.
- Храните персональные данные (логин/пароль, средства защиты, одноразовые коды, полные номера банковских карт и их CVV-код) по отдельности в недоступном для посторонних месте.
- Завершайте работу в приложении через «Завершение сессии».

Download on the App Store

GET IT ON Google Play