МОСКОМБАНК
Commercial Bank of Moscow

РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

В области информационной безопасности АО «МОСКОМБАНК» рекомендует Клиенту:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Системы ДБО. Признаком установки защищённого соединения является наличие информации о протоколе https в адресной строке используемого клиентом браузера, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.

2. Осуществлять вход в Систему ДБО только через Сайт https://dbo.moscombank.ru (Интернет-банк), либо через мобильное приложение (Мобильный банк), которое может быть установлено на мобильное устройство из рекомендуемых Банком интернет-магазинов (репозиториев), таких как AppStore, Google Play, RuStore и другие, или путем загрузки и установки аналогичного официального приложения с официального Сайта Банка.

3. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену Банка: https://moscombank.ru или Системы ДБО https://dbo.moscombank.ru, сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефону (495) 109-00-14. Банк не осуществляет рассылку подобных электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Системы ДБО.

4. Не отлучаться от устройства с установленным ДБО в период активной сессии с Системой ДБО, либо завершить активную сессию ДБО.

5. Не передавать логины, пароли, пин-коды и коды доступа другим лицам, в том числе сотрудникам Банка для проверки работоспособности или настройки Системы ДБО, хранить их в надежном месте, исключающем доступ к ним посторонних лиц. Вся ответственность за сохранность и использование паролей, логина, пин-кода иного кода доступа для доступа в Систему ДБО, полностью лежит на Клиенте как единственном их владельце.

6. Банк рекомендует использовать виртуальную клавиатуру. Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками. Виртуальная клавиатура появляется при входе в Систему ДБО. При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе ДБО (если пароль содержит заглавную букву или символ, нажмите клавишу Shift, переключение между русским и английским алфавитом - клавиша Рус/Lat, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите Enter.

7. Исключить доступ посторонних лиц к компьютеру или мобильному устройству, использующемуся для работы в Системе ДБО. Осуществлять постоянный контроль отправляемых платежных электронных документов при работе в Системе ДБО, а также состояние своего личного счета.

8. Избегать работы в Системе ДБО при подключении к публичным точкам доступа Wi-Fi, в интернет-кафе и на других компьютерах общего пользования, контролировать информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему ДБО.

9. Не записывать используемый Пароль там, где доступ к нему могут получить посторонние лица.

10. Использовать только лицензионное, поддерживаемое производителем программного обеспечения (операционные системы, офисные пакеты), обеспечить автоматическое обновление системного и прикладного программного обеспечения, исключить использование самодельных «сборок» и взломанного программного обеспечения.

11. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе ДБО только с указанных Клиентом IP-адресов/сетей).

12. В случае выявления явных или косвенных признаков компрометации Логина или Пароля, а также обнаружения вредоносных программ в компьютере, используемом для работы в Системе ДБО, незамедлительно уведомить об этом Банк по телефону: (495) 109-00-14 либо лично явиться в Банк с целью блокирования скомпрометированных данных с последующей их заменой. К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

- обнаружение факта или угрозы использования (копирования) идентификаторов учетной записи или паролей доступа к Системе ДБО неуполномоченных лиц (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Системы ДБО, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение воздействия вредоносного кода в компьютере, планшете, мобильном устройстве, мобильном телефоне, используемом для работы в Системе ДБО.

13. В случае выявления явных или косвенных признаков компрометации пароля учетной записи Клиент должен сменить данный пароль самостоятельно.

14. Обеспечивать конфиденциальность использования логина, паролей, пин-кодов, кодов доступа, которые не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы ДБО в работоспособном состоянии.

15. Применять на устройствах, используемых для работы Системы ДБО, лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, антиспам-фильтры.

16. Производить периодическую (не реже 1 раза в 3 месяца) смену долговременного пароля, а также по требованию Банка и в случае компрометации. Пароли должны выбираться исходя из следующих требований:

- Длина пароля не менее 8 символов;

- Пароль должен состоять из больших и маленьких букв, цифр и специальных символов (+ = * и т.д.);
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (qwerty, qwerty123, 12345678 и т.д.);
- При смене пароля он должен отличаться от предыдущего не менее чем в 2х позициях.

17. Самостоятельно убедиться, либо что используемое оборудование и программное обеспечение настроено для работы с сетью Интернет по защищенному протоколу https.

18. Не использовать на своем устройстве любые средства удаленного (дистанционного) доступа, которые обычно практикуют IT-специалисты для удаленной (дистанционной) поддержки (например, TeamViewer, AnyDesk, Ammy Admin и т.п.). Удалить или заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

19. При использовании мобильного устройства установить на него антивирусное программное обеспечение и пароль доступа к устройству, не использовать мобильное устройство с расширенными правами (Jailbreak/Root), так как это значительно снижает уровень обеспечения безопасности устройства. Регулярно устанавливать обновления для Вашего устройства и установленного антивирусного программного обеспечения, защитить свое мобильное устройство кодом блокировки экрана, паролем или отпечатком пальца.

20. Не устанавливать на мобильное устройство, используемое для приема СМС-сообщений или Пуш-уведомлений с подтверждающим одноразовым Паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим Клиентам ссылки или указания на установку приложений.

21. При утрате мобильного устройства или SIM-карты, используемых для приема СМС-сообщений или Пуш-уведомлений с подтверждающим одноразовым Паролем, немедленно обратиться к своему оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Системе ДБО и проверки последних платежей.

22. Принимать звонки и СМС от Банка только номеров телефонов Банка: +74951090014, +74956091919, +73833358811.

В области социальной инженерии АО «МОСКОМБАНК» рекомендует Клиенту:

1. Обращать внимание на следующие признаки мошенничества:
- мошенник обращается с неизвестного номера телефона;
- мошенник представляется сотрудником Банка, Центрального Банка, Федеральных органов исполнительной власти (полиция, следователи, сотрудники Федеральной службы безопасности);
- Клиенту предлагается или какая-то выгода или описывается проблема и предлагается путь решения;
- от Клиента требуют сообщить номера карты, ПИН-код, логин и пароль от банковских приложений, подтвердить код по СМС, перейти по ссылке в СМС или e-mail сообщении, т.е. провести компрометацию конфиденциальных данных;
- от Клиента требуют провести мгновенную оплату, перевод денежных средств;
- от Клиента требуют быстрого принятия решения, немедленной реакции;

- возражают против того, чтобы Клиент позвонил позже, препятствуют разъединению телефонного звонка.

2. Учитывать следующие типичные случаи мошенничества:

Предложение мошенника	**Ваши действия**
Ваша карта заблокирована СМС-сообщение о якобы заблокированной карте, требуют сообщить ПИН-код или совершить действия в банкомате	Не переходите по ссылкам, перезвоните в Ваш банк. Помните, банк никогда не будет запрашивать номер карты, ПИН, иные коды
Родственник в беде Требование крупной суммы денег за решение проблем родственника, который якобы попал в беду. Мошенник представляется сотрудником полиции.	Обратите внимание на входящий телефон, наверняка он мобильный. Положите трубку и свяжитесь с Вашим родственником напрямую.
Требуется помощь в социальной сети Ваш знакомый по социальной сети описывает несчастье, которое случилось с ним или его родственниками, знакомыми и публикую номер карты/телефона, на которую идет сбор средств.	Перезвоните Вашему знакомому, не вступайте в переписку, аккаунт под контролем мошенника.
Выигрыш СМС/e-mail-сообщение о крупном выигрыше, предлагают перейти по ссылке	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вирусная атака СМС/ e-mail-сообщение содержит ссылку на какой-либо интернет ресурс, содержащий вредоносную программу, дающую доступ к карте	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вам положена компенсация Для получения компенсации Вам предлагают авансом оплатить пошлины, проценты, доставку, страховку и т.п.	Все предложения, требующие каких-то немедленных платежей являются мошенническими, положите трубку
Ошибочный перевод средств просят вернуть денежный средства за якобы ошибочный перевод	Не делайте поспешных действий, вначале проверьте действительно ли Вам приходила неизвестная сумма.
Карта заблокирована звонок «сотрудника банка», предлагают разблокировать карту, для чего просят сообщить реквизиты карты, код на обратной стороне, ПИН-код.	Положите трубку. Сотрудник банка не будет запрашивать реквизиты карты и коды.
«Сотрудник банка» проводит проверку данных или оказывает услугу и просит подтвердить «проверочный код» «Вам по СМС должен поступить код, сообщите и проблема будет решена»	Положите трубку, сотрудники банка не высылают никаких СМС-кодов. Если Вы подтвердите код с Вас спишут деньги.
Звонок из банка — просят перевести деньги на безопасный счет «Сотрудник банка» сообщает, что поступило	Положите трубку, сотрудники банка не высылают никаких СМС-кодов.

заявление на закрытие счета, как будете забирать деньги. Потом говорят, что это мошенничество и предлагают сделать немедленно перевод на «безопасный счет», предлагают диктовать номер карты, ПИН-код, код на обратной стороне карты	
Предоплата товара на сайте На различных площадках в интернете Вы обнаружили товар по привлекательной цене, но требуется перевод авансом на карту, по телефону.	Изучите продавца, отзывы о нем, историю, позвоните, предложите оплату при доставке. Ни в коем случае не оплачивайте авансы.
Просьба дать в долг От Ваших, друзей знакомых по социальной сети приходит просьба срочно прислать денег в долг	Перезвоните Вашему знакомому, уточните информацию. Не вступайте в переписку в этой же социальной сети, аккаунт Вашего знакомого скорее всего мошеннический.
Одобрение кредита «Сотрудник банка» сообщает об одобрении кредита на выгодных условиях. Для доступа к кредиту, надо внести плату за рассмотрение, за страхование, за выезд курьера и т. п. Плату внести предлагают через терминал/банкомат	Банк никогда не предлагает кредиты с предварительной оплатой каких-либо сопутствующих услуг.
<u>Продление договора оператора связи</u> «Сотрудник оператора связи» сообщает об окончании договора на мобильную связь и предлагает продлить его онлайн присылая ссылку, либо просит ввести код, который он уже выслал. В это время мошенник уже пытается взломать личный кабинетв ЕСИА «Госуслуги» и код это от двухфакторной аутентификации при входе на портал.	Немедленно положите трубку. Зайдите на портал ЕСИА «Госуслуги» и сбросьте пароль от входа. Позвоните на горячую линию портала ЕСИА «Госуслуги» и расскажите об инциденте для быстрой блокировки личного кабинете и смены пароля.