ПАМЯТКА по безопасности при использовании удаленных каналов обслуживания ООО «МигКредит»

Меры безопасности

Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным.

При работе всегда проверяйте, что установлено защищенное ssl-соединение с официальными сайтом (https://migcredit.ru). В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера. Например, в браузере Microsoft Internet Explorer в правой части адресной строки располагается желтый замочек.

Помните, что Компания не рассылает своим клиентам ссылки или указания на установку Мобильных приложений через SMS/Push/MMS/e-mail–сообщения.

На Мобильных устройствах, которые Вы используете для доступа к МигКредит:

- используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты Вашего Мобильного устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.

Завершение работы с Приложением МигКредит выполняйте путем выбора соответствующего пункта меню.

Меры безопасности при работе с Устройствами самообслуживания

Внимание! Не совершайте на Устройстве самообслуживания никаких операций по указаниям посторонних лиц, позвонивших Вам и представившихся работниками Компании или других организаций.

Меры безопасности при работе с Мобильным приложением Компании

При утрате Мобильного устройства, на которое установлено Мобильное приложение Компании, Вам следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Компании для блокировки доступа в МигКредит.

При внезапном прекращении работы SIM-карты необходимо срочно обратиться к своему оператору сотовой связи за уточнением причин – в отношении Вас возможно проведение мошеннических действий третьими лицами.

Будьте внимательны – не оставляйте свое Мобильное устройство без присмотра, чтобы исключить несанкционированное использование Мобильного приложения.

Используйте только официальные Мобильные приложения Компании, доступные в официальных магазинах приложений производителей мобильных платформ. Обязательно убедитесь, что в поле «разработчик мобильного приложения» указан ООО «МигКредит».

Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваше Мобильное устройство. Используйте антивирусное программное обеспечение для Мобильного устройства, своевременно устанавливайте на него обновления антивирусных баз.

Не устанавливайте на свое Мобильное устройство нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваше Мобильное устройство становится уязвимым к заражению вирусными программами.

Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Компании.

Установите на Мобильном устройстве пароль для доступа к устройству, данная возможность доступна для любых современных моделей Мобильных устройств.

Не используйте Мобильное устройство для доступа к полнофункциональной версии МигКредит , для этого существуют специализированные Мобильные приложения.

Завершайте работу с Мобильным приложением Компании через завершение сессии.

Защита от SMS/Push-мошенничества

Мошеннические SMS-сообщения/Push-уведомления, как правило, информируют о блокировке Банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS-сообщении/Push-уведомлении номер телефона для уточнения информации. Перезвонившему Клиенту мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки Компании.

В случае получения подобных SMS-сообщений/Push-уведомлений настоятельно рекомендуем Вам:

- не перезванивать на номер телефона, указанный в SMS-сообщении/Push-уведомлении; не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИНе, CVV2/CVC2/ППК2 коде), Контрольной информации, Коде клиента Логине (Идентификаторе пользователя), Постоянном пароле, Одноразовых паролях, в т.ч. посредством направления ответных SMS-сообщений/Push-уведомлений;
- не проводить через Устройства самообслуживания никакие операции по инструкциям, полученным по Мобильным устройствам.

В ряде случаев Компания рассылает информационные SMS-сообщения/Push-уведомления, при этом:

- SMS-сообщения/Push-уведомления Компании всегда отправляются с номера «____[1]», в них указываются только официальные номера телефонов Компании, опубликованные на Официальном сайте Компании;
- SMS-сообщения/Push-уведомления Компании не рассылаются с официальных номеров телефонов Контактного Центра Компании.

Если полученное SMS-сообщение/Push-уведомление вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Компании по официальным номерам телефонов, размещенным на оборотной стороне карты или на Официальном сайте Компании.

В случае если Вы все же пострадали от SMS/Push-мошенничества, необходимо:

- немедленно обратиться в Контактный Центр Компании по официальным номерам телефонов и заблокировать карту, реквизиты которой были сообщены мошенникам или по которой были совершены мошеннические операции;

[1] Указан основной номер, для разных регионов возможна также рассылка с номеров _____.

- немедленно обратиться по телефону к оператору связи, в адрес которого переведены средства, с заявлением о мошенничестве и возврате средств (как правило, информация о номерах телефонов, на которые были переведены средства, сотовом операторе и номерах телефонов контактного центра сотового оператора указаны на чеке, полученном в Устройстве самообслуживания);
- подать через любое подразделение полиции заявление о совершенном мошенничестве на имя начальника управления «К» ГУВД\УВД.

Защита от e-mail мошенничества

Массовые мошеннические e-mail-рассылки, маскируясь под бренд ООО «МигКредит», как правило, предназначены для:

- заманивания получателей сообщений на сайты-«ловушки», на которых под различными предлогами мошенники попытаются получить персональные и конфиденциальные данные (ФИО, Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера банковских карт и их сроки действия, ПИНы, CVV2/CVC2/ППК2 коды, Код клиента и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц;
- принуждения под различными предлогами получателей писем на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла.

Признаки того, что e-mail-сообщение является мошенническим:

- сообщения замаскированы под официальные письма Компании и требуют от Вас каких-либо быстрых действий или ответа;
- адрес отправителя и тема сообщения замаскированы под обращения от имени Компании.

Примеры наименования отправителей мошеннических сообщениях:

- МигКредит (info@migcredit.ru)
- МигКредит России (migcredit.ru)
- МигКредит Информ (migcredit.ru)
- и пр.

Примеры тем сообщений в мошеннических рассылках:

- «Сообщение об увеличении задолженности»
- «Сообщение об увеличении долга»
- «Сообщение об увеличении задолженности на ДД.ММ.ГГГГ»

- письма содержат ссылки на интернет-ресурсы, похожие на официальные ресурсы Компании; URL-адрес ссылки в письме отличается от официального адреса (www.migcredit.ru), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Ваших персональных данных;
- к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть; в тексте содержатся явные опечатки или орфографические ошибки.

Обращаем Ваше внимание, что ООО «МигКредит» никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные и конфиденциальные данные (ФИО, Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера банковских карт и сроки их действия, ПИНы, CVV2/CVC2/ППК2 коды, Код клиента, данные документа, удостоверяющего личность, номер мобильного телефона и пр. информацию);
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в личный кабинет МигКредит по ссылкам в письмах.