РЕКОМЕНДАЦИИ
по защите информации в целях противодействия незаконным финансовым операциям

1. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и воздействием вредоносных кодов.

1.1. В соответствии с требованиями Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций (утв. Банком России 17.04.2019 № 684-П) ООО МФК «Русские деньги» (далее — Общество) настоящим Общество доводит до сведения своих клиентов:

– рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее — вредоносный код), в целях противодействия незаконным финансовым операциям;

– информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

– информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

1.2. При осуществлении финансовых операций следует принимать во внимание риски финансовых потерь, связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также с воздействием вредоносных кодов. Указанные риски могут быть обусловлены, включая, но не ограничиваясь, следующими ситуациями:

– кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества, и/или несанкционированный доступ к сервисам Общества с этого устройства, что может повлечь за собой получение третьими лицами доступа к защищаемой информации;

– кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV/CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа;

– установка на устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от Вашего имени;

– использования злоумышленниками утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты от несанкционированных финансовых операций, что позволит им обойти защиту;

– получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. Ф.И.О., паспортные данные, путем обмана и/или злоупотребления доверием, когда злоумышленник представляется работником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные, или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

– перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Обществом. Или в случае получения доступа к вашей электронной почте, отправка сообщений от Вашего имени в Общество;

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несет Владелец учётных данных.

Общество не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

2. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации и защите информации от воздействия вредоносных кодов.

2.1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Общества, к таким мерам включая, но не ограничиваясь могут быть отнесены:

– использование только лицензированного программного обеспечения, полученного из доверенных источников;

– запрет на установку программ из непроверенных источников;

– наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя;

– настройка прав доступа к устройству с целью предотвращения несанкционированного доступа;

– хранение, использование устройства с целью избежать рисков кражи и/или утери;

– своевременные обновления операционной системы;

– активация парольной или иной защиты для доступа к устройству;

– в случае обнаружения злонамеренного программного обеспечения на компьютере или ином устройстве после его удаления незамедлительно смените логин и пароль;

– не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

2.2. Обеспечьте конфиденциальность:

– храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: логины, пароли, коды, кодовое, а в случае компрометации немедленно примите меры для смены и/или блокировки;

– соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Общества.

2.3. Проявляйте осторожность и предусмотрительность:

– будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет-ссылку, может получить доступ к любым данным и информационным системам на вашем устройстве;

– внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц;

– будьте осторожны при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта;

– будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код;

– не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

– анализируйте информацию в прессе и иных общедоступных специализированных источниках о последних известных критичных уязвимостях и вредоносных кодах;

– осуществляйте звонок в Общество только по номеру телефона, указанному в договоре и на официальном сайте. Важно учесть, что от лица Общества не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.;

– если вы самостоятельно связались с Обществом, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в личный кабинет;

– имейте в виду, что если Вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы;

– при утере, краже телефона, планшета, персонального компьютера, используемого для доступа к системам Общества необходимо:

a. незамедлительно проинформировать Общество через отдел по работе с клиентами;

b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;

c. сменить пароль, воспользовавшись другим доверенным устройством;

– при возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в личный кабинет, обратившись в Общество по телефону техподдержки. В случае утраты, а также при возникновении любых подозрений, что Ваши логин и пароль стали известны третьим лицам (в том числе представившимся сотрудниками Общества), незамедлительно предпринимайте меры для блокировки личного кабинета. Вы можете сделать это, связавшись с Обществом по телефону техподдержки;

– помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства;

– лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас;

– контролируйте свой телефон. В случае выхода из строя сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи;

– регулярно выполняйте резервное копирование важной информации;

– поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

2.4. При работе на компьютере необходимо:

– средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п;

– доступ к изменению настроек BIOS должен быть защищен паролем;

– на компьютере должна быть установлена только одна операционная система;

– использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т. д.);

– своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т. д.);

– использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;

– использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;

– использовать сложные пароли;

– локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему;

– не устанавливать и не использовать на компьютере программы для удаленного управления (например, RDP, TeamViewer, Radmin, Ammyy Admin др.);

– для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

2.5. При работе с мобильным устройством необходимо:

– при взаимодействии с Обществом указывать в качестве основного номера телефона номер, который принадлежит Вам лично (контракт на услуги сотовой связи, заключен на Ваше имя);

– устанавливать мобильное приложение Общества на телефонный аппарат, который принадлежит Вам и постоянно находится в Вашем распоряжении. Включите запрос пин-кода SIM-карты при включении телефона;

– устанавливать приложения на мобильное устройство можно только из официальных репозиториев производителей мобильных платформ: AppStore, Google Play и Huawei AppGallery;

– установите на мобильное устройство антивирус и своевременно его обновляйте. Для платформы Android рекомендуем бесплатные приложения Dr.Web Light (доступен для загрузки из Google Play) и Kaspersky Mobile Antivirus: AppLock & Web Security (доступен для загрузки из Google Play);

– своевременно устанавливайте обновления безопасности операционной системы;

– не взламывайте свой телефон (например, через Jailbreaking, реинжиниринг, принудительное получение root-прав), так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате ваш телефон становится уязвимым к заражению вирусным программным обеспечением;

– не отключайте и не взламывайте встроенные механизмы безопасности вашего устройства;

– включите блокирование экрана телефона после определенного времени неактивности;

– включите запрос пин-кода телефона, отпечатка пальца, «FaceID» или графического ключа для разблокирования телефона;

– установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки;

– включить и настроить функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона;

– установите запрет на установку в телефон приложений из ненадежных источников;

– при установке новых приложений на телефон обращайте внимание на запрашиваемые ими разрешения;

– не давайте приложениям разрешение на чтение СМС, если такой доступ не нужен им для выполнения их основных функций;

– при наличии технической возможности включите шифрование данных на своём устройстве;

– сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в информационные системы и СМС-коды. Не сообщайте эти данные никому;

– не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в СМС-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества.

2.6. При обмене информацией через сеть Интернет необходимо:

– не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;

– не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;

– ограничить посещения сайтов сомнительного содержания;

– не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;

– не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;

– открывать файлы только известных Вам расширений (docx, png, xlsx и т. д.);

– не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, кодовое слово, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные;

– не отвечайте на полученное подозрительное сообщение и не переходите по ссылкам, указанным в сообщении.

2.7. Рекомендации по парольной защите:

– длина пароля должна быть не менее 8 символов;

– в пароле обязательно должны присутствовать заглавные и прописные (верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.); примеры паролей (Hjf#48dft, 5$ma(fq5eR, %dEr*2fvw2);

– пароль не должен содержать словарных слов (passw0rd, football, shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей – Cthutq);

– в качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты,

номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

– в качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;

– пароль не должен быть копией или комбинаций паролей, используемых Вами в других системах (операционная система компьютера, электронная почта, развлекательные ресурсы в Интернет и т.п.);

– пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля;

– при смене пароля новый пароль не должен совпадать с ранее используемыми паролями;

– запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли;

– не храните логин и пароль на компьютере, в мобильном телефоне, смартфоне, а также на иных электронных носителях, доступ к которым могут получить третьи лица;

– выбирайте кодовое слово таким образом, чтобы его было сложно угадать даже людям, которые хорошо Вас знают. Не выбирайте в качестве кодового слова Ваше имя или фамилию, имена и фамилии близких Вам людей, даты рождения и другую информацию о Вас, которая известна многим людям. Не сообщайте кодовое слово никому кроме сотрудников Компании, отвечающих на Ваш звонок на горячую линию Компании. Если Вы записываете кодовое слово чтобы его не забыть, не храните запись с кодовым словом в местах, доступных для других лиц.

2.8. Рекомендации при работе в личном кабинете Общества:

– необходимо помнить, что сайты, визуально напоминающие сайт с Личным кабинетом, создаются специально для незаконного получения информации. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта Компании или Личного кабинета, клиенту необходимо незамедлительно сообщить об этом Обществу по всем возможным контактам, указанным на официальном сайте Общества в сети «Интернет» по адресу: https://russkiedengi.ru. Во избежание использования таких ресурсов необходимо удостовериться, что при подключении к Личному кабинету защищённое соединение было установлено исключительно с официальным сайтом Компании. Прежде чем ввести логин и пароль, необходимо проверить по информации из SSL-сертификата подлинность сайта.

– рекомендуется внимательно анализировать ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить потенциальную жертву злоумышленников на мошеннический web-сайт. Если ссылка выглядит подозрительно (ссылка с ошибками или заменой сходных по начертанию символов) или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не рекомендуется переходить по этой ссылке

– после окончания работы в личном кабинете обязательно завершайте сеанс работы.