

**РЕКОМЕНДАЦИИ МКК «ХОРОШИЕ ДЕНЬГИ» (ИНН 5027285088, КПП 500901001)
ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ
ФИНАНСОВЫМ ОПЕРАЦИЯМ**

Настоящие рекомендации разработаны во исполнение требований Положения Банка России от 17.04.2019 N 684-П "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", Письма Банка России от 6 августа 2019 г. N 56-1-11/448 и предназначены для ознакомления клиентов ООО МКК «Хорошие деньги» (далее по тексту – Клиент) с рекомендациями по предотвращению незаконного доступа к информации, которая может позволить третьим лицам совершать незаконные финансовые операции от имени клиентов Общества.

1. Риски получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Использование цифровых технологий повышает удобство взаимодействия Клиента с Обществом и другими финансовыми организациями. Однако, это одновременно влечет за собой возникновение рисков незаконного совершения злоумышленниками финансовых операций от имени клиентов финансовых организаций с целью хищения денежных средств клиентов.

Вот некоторые из рисков, на которые необходимо обратить внимание (список не является исчерпывающим):

- 1.1. Утеря или передача третьим лицам данных для входа в Личный кабинет Клиента.
 - 1.2. Завладение и неправомерное использование злоумышленниками персональных данных Клиента (утера Клиентом паспорта, использование злоумышленниками паспортных данных, полученных незаконным путем).
 - 1.3. Завладение злоумышленниками устройством, с которого клиент входит в Личный кабинет, в платежные сервисы.
 - 1.4. Вход в Личный кабинет и на страницы платежных сервисов с использованием незащищенного соединения.
 - 1.5. Заражение устройства Клиента вирусами, вредоносными программами.
2. Меры 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.

Общество приводит следующие рекомендации для предотвращения несанкционированного доступа:

- 2.1. Не допускайте утерю документа, удостоверяющего личность. В случае утери незамедлительно обратитесь в органы внутренних дел, тогда Ваш паспорт будет внесен в базу недействительных.
 - 2.2. Соблюдайте конфиденциальность и не передавать третьим лицам данные для входа в Личный кабинет, пароли, пин-коды. Не рекомендуется записывать и хранить в местах, доступных посторонним лицам логин и пароль для входа в Личный кабинет и платежные сервисы.
 - 2.3. Не пересылайте файлы с конфиденциальной информацией по открытым каналам связи, по электронной почте или через SMS-сообщения.
 - 2.4. В случае, если войти в Личный кабинет не получается, незамедлительно обратитесь в службу поддержки клиентов по номеру телефона 8 (800) 600-76-56.
 - 2.5. Незамедлительно обратитесь к оператору и заблокируйте SIM-карту в случае ее утери. Включите запрос пин-кода SIM-карты при включении телефона. Включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокирования телефона, при наличии таких функций. Включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона, при наличии.
 - 2.6. Используйте на устройствах только лицензионное программное обеспечение. Загружайте приложения только из официальных источников (Google Play, Apple AppStore).
 - 2.7. Не используйте незащищенное соединение для входа в Личный кабинет и при безналичной оплате.
 - 2.8. Во избежание попадания на сайт-двойник, внимательно проверяйте в адресной строке адрес сайта, с которого Вы входите в Личный кабинет, или на котором производите оплату.
 - 2.9. Не рекомендуется использовать средства удаленного администрирования на устройстве, предназначенного для доступа к Личному кабинету, для осуществления электронных платежей.
 - 2.10. Не переходите по рекламным ссылкам из «всплывающих окон».
 - 2.11. Не открывайте письма, смс, полученные от неизвестных отправителей, не переходите по ссылкам в таких письмах.
 - 2.12. Не рекомендуется работать с Личным кабинетом и платежными сервисами на устройствах общего пользования (рабочий компьютер, «Интернет-кафе» и т.п.)
3. Меры по предотвращению установки вредоносного программного обеспечения и заражения устройств вирусами.

Вирусами называются программы для устройств, специально созданные для нанесения вреда. Вирусы способны проникнуть в устройство, в том числе с целью кражи данных банковских карт, установленных паролей, совершения незаконных финансовых операций от имени клиента.

Существует множество видов вирусов, приводим некоторые примеры:

- «Троянский конь» – проникает на устройство под видом обычной программы. Это программы, осуществляющие различные действия, которые пользователь не санкционировал: сбор информации о платежных картах и её передачу злоумышленнику, удаление или злонамеренное изменение информации на устройстве.

- «Фишинг» – перехват личных данных. Выражается, например, в отправке электронных писем от мошенников, которые выдают себя за работодателей, или представителей известных компаний. Как правило, в таких письмах содержится ссылка на зараженную страницу, на которой предлагается ввести свои персональные данные, после чего информация похищается. Такая же рассылка может производиться по SMS («SMS - Фишинг»).

Во избежание заражения вирусами Вашего устройства необходимо:

- 3.1. Обновлять операционную систему и установленные в ней приложения (можно включить автоматическое обновление).
- 3.2. В обязательном порядке установить на устройства программы антивирусной защиты. Не забывайте вовремя обновлять программы. Не реже одного раза в неделю в автоматическом режиме осуществляйте полную проверку устройств на предмет наличия вирусов и вредоносного программного кода.
- 3.3. Никогда не переходите по ссылкам из SMS-сообщений и сообщений в мессенджерах, электронной почте, поступивших от неизвестных источников, особенно если Вы не ждали такие сообщения.

Следуя этим рекомендациям Вы сможете минимизировать риски совершения от Вашего имени незаконных финансовых операций.