Приложение №2
к Приказу Генерального Директора
ООО МКК «Востсибснаб»
№15 от «16» мая 2022 г.

РЕКОМЕНДАЦИИ
по противодействию совершения незаконных финансовых операций

ВВЕДЕНИЕ

Настоящий документ предназначен для ознакомления Клиентов ООО МКК «Востсибснаб» (далее по тексту - *«Общество»*) с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить им совершить незаконные финансовые операции от имени Клиентов Общества.

В настоящее время активно осуществляется внедрение современных цифровых технологий в различные сферы жизни и производства. Финансовые организации предлагают своим Клиентам большой выбор инструментов для удаленного взаимодействия, позволяющий Клиентам экономить своё время и совершать финансовые операции без личного визиты в офис финансовой организации.

Необходимо отменить, что использование технологий удаленного взаимодействия, несет с собой определенные риски, главным из указанных рисков является незаконное совершение злоумышленниками финансовых операций от имени Клиентов финансовых организаций с целью хищения денежных средств Клиентов.

Выполнение несложных рекомендаций, указанных в настоящем документе, позволит Клиентам Общества свести риск совершения незаконных финансовых операций от их имени к минимуму.

1 В целях предотвращения несанкционированного доступа рекомендуем следующие меры защиты:

1.1 Мобильный телефон используется Клиентами Общества для получения Уникального кода, одноразовых паролей в SMS-сообщениях:

1.1.1 При взаимодействии с Обществом указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (договор на услуги сотовой связи, заключен на Ваше имя);

1.1.2 Включите запрос пин-кода SIM – карты при включении телефона;

1.1.3 При поддержке телефоном соответствующей функции, выполните следующие действия:

включите блокированиеэкрана телефона после определенного времени неактивности;

включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокировки телефона;

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

включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона;

1.1.4 Установите запрет на установку в телефон приложений из ненадлежащих источников.

1.1.5 При установке новых приложений на телефон обращайте внимание за запрашиваемые ими разрешения. Не давайте приложениям разрешения на чтение SMS, если такой доступ не нужен им для выполнения их основных функций.

1.1.6 Не переходите по ссылкам из SMS и сообщений, особенно если Вы не ждали такие сообщения.

1.1.7 Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление).

1.1.8 В случае утраты телефона воспользуйтесь функцией поиска телефона, если ранее ее активировали. Если с использованием функции поиска найти телефон не удалось или Вы ранее не активировали эту функцию, обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном SIM-карты и выпуска новой;

1.1.9 Не сообщайте посторонним лицам, в том числе в сети Интернет, персональные данные или информацию о финансовых операциях, о банковских картах, логины и пароли доступов (в том числе Личного кабинета Клиента), историю операций, во избежание попадание информации к злоумышленникам и использование последними с целью получения доступа к защищаемой информации;

1.1.10 Не записывайте логин и пароль от Личного кабинета и иных приложений на бумаге, пин-код банковской карты (секретная комбинация цифр, используемая для подтверждения операций с Вашей банковской карты международной платежной системы международной платежной системы MasterCard, Visa или МИР) на бумаге, мониторе, клавиатуре и иных устройствах с использованием которых осуществляете финансовые операции.

1.1.11 Используйте разные пароли для ваших учетных записей. Если вы будете использовать одинаковые пароли, а злоумышленник узнает пароль от одной учетной записи, он сможет получить доступ ко всем остальным.

1.1.12 Используйте сложносоставные пароли, которые содержат прописные и строчные буквы, а также цифры и специальные символы. Не используйте личную информацию, которую легко узнать. Например: имя, фамилию или дату рождения; очевидные и простые слова, фразы, устойчивые выражения и наборы символов, которые легко подобрать.

1.1.13 По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.

1.1.14 Не переходите по ссылкам в письмах, не открывайте вложенные приложения, полученных по электронной почте от якобы представителей финансовых организаций, если получение таких писем инициировано на Вами. В таких письмах может содержатся вредоносное программное обеспечение).

1.1.15 Для осуществления взаимодействия с финансовыми организациями с целью получения необходимо информации используйте только номера телефонов и адреса электронной почты, указанных только на официальном сайте финансовой организации либо в официальных документах финансовой организации.

1.1.16 Используйте антивирусное программное обеспечение.

1.1.17 При утрате (хищении) устройства, с использованием которого им совершались действия в целях осуществления финансовой операции — незамедлительно сообщить доступными средствами связи Обществу.

1.1.18 При наличии несанкционированных действий с денежными средствами и иных незаконных финансовых операций — незамедлительно подать заявление о данном факте в правоохранительные органы.

2 В целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники:

2.1 **Вирусы** — это программы для компьютеров или мобильных устройств, предназначенные для нанесения вреда. Функционал вирусов может быть разным: показ нежелательной рекламы, кража паролей (в том числе, из SMS — сообщений) и данных

банковских карт, совершение незаконных финансовых операций от имени клиента.

Практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств.

Отсутствие вирусов на устройствах (компьютерах, сотовых телефонах, планшетах), с которых Вы работаете с системами дистанционного обслуживания Обществом, является залогом безопасности Ваших денежных средств.

2.2 Во избежание заражения вирусами Вашего мобильного устройства, следуйте таким советам:

2.2.1 Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление).

2.2.2 Осуществляйте регулярный контроль работоспособности антивирусных программ;

2.2.3 Создайте условия, при которых невозможно несанкционированное отключения средств антивирусной защиты.

2.2.4 Антивирусная защита должна обеспечивать сохранение безопасного состояния информации при любых сбоях;

2.2.5 Вынесите ярлык для запуска антивирусной программы на рабочий стол персонального компьютера и используйте его регулярно.

2.2.6 Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т. п.) и социальных сетей, которые Вы не ждете.

2.2.7 Установите запрет на установку в телефон приложений из ненадлежащих источников.