Рекомендации по информационной безопасности при совершении финансовых операций

АО ВИМ Инвестиции ставит своей целью обеспечить предоставление услуг на высоком уровне и напоминает Вам о рисках мошенничества с использованием мобильной связи, социальных сетей, мессенджеров, электронной почты и систем дистанционного обслуживания. Например, Вы можете получить сообщение или звонок от мошенников, содержащие запрос Вашей конфиденциальной информации (персональные данные, финансовые сведения, пароли, коды из СМС и т.п.) или просьбу совершить определенные действия, по телефону, через мессенджеры, социальные сети, по электронной почте. В случае выполнении просьбы или инструкций злоумышленников, они могут попытаться осуществить несанкционированный доступ к Вашему компьютеру, мобильному устройству, личным кабинетам или получить критичные сведения о Вас для дальнейшего совершения незаконных финансовых операций от Вашего имени.

АО ВИМ Инвестиции доводит до сведения клиентов и контрагентов следующие рекомендации по безопасности информации:

1. Никому не сообщайте и не передавайте, а также не вводите свои данные на подозрительных сайтах и в приложениях: логины/пароли или одноразовые коды доступа для входа в систему или подтверждения операций, а также Ваши персональные данные (паспортные данные, ИНН, СНИЛС, дата рождения и пр.) и финансовые сведения. Сотрудники АО ВИМ Инвестиции никогда не спрашивают пароли и коды из СМС.
2. Обеспечьте защиту устройства, с которого Вы осуществляете финансовые операции:
    - Устанавливайте программное обеспечение из доверенных источников, настройте запрет на установку приложений из непроверенных источников;
    - Используйте средства защиты информации, такие как антивирусные программы (а также регулярно их обновляйте), персональный межсетевой экран, шифрование данных и дисков;
    - Не передавайте Ваше мобильное устройство или персональный компьютер другим людям и не оставляйте без присмотра с целью недопущения утери, кражи или совершения незаконных финансовых операций;
    - Не соглашайтесь на удаленное подключение к Вашему мобильному устройству или персональному компьютеру.
3. Дополнительно при работе в сети Интернет:
    - Будьте осторожны при получении сообщений со ссылками на сайты и вложенными файлами, они могут привести к заражению Вашего устройства вредоносным кодом (например, вирусами). Вредоносный код может попасть на Ваше устройство, если Вы откроете вложенный файл или перейдете по ссылке на сайт. Используя вредоносный код, злоумышленник может получить доступ к данным и приложениям на Вашем устройстве. Избегайте сомнительных сайтов в Интернете, поскольку вредоносный код в том числе может быть загружен с подобных сайтов;
    - Имейте в виду, что мошенники могут создавать поддельные сайты компании, используя схожую цветовую гамму и название АО ВИМ Инвестиции, направлять поддельные письма, якобы от лица АО ВИМ Инвестиции. Будьте максимально внимательны, проверяйте ссылки на сайты;
    - Внимательно проверяйте адресата, от которого пришло сообщение. Сообщение может быть от злоумышленника, который маскируется под сотрудника АО ВИМ Инвестиции или иных доверенных лиц, например, под представителей государственных ведомств и органов власти;
    - Незамедлительно информируйте АО ВИМ Инвестиции о попытках мошенничества или подозрении на них, если это имеет отношение к взаимодействию с АО ВИМ Инвестиции, а также если Вы получили уведомление о финансовых операциях, которые не совершали.