РЕКОМЕНДАЦИИ КЛИЕНТАМ ПО СОБЛЮДЕНИЮ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

1. Общие положения.

1.1. Общество с ограниченной ответственностью Инвестиционная компания «КРЭСКО Финанс» (далее – Общество) в целях соблюдения требований Положения Банка России №684-П от 17.04.2019 «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» уведомляет своих клиентов о потенциальных рисках несанкционированного доступа к защищаемой информации с целью проведения финансовых операций неуполномоченными лицами.

1.2. Основные термины:

Защищаемая информация — это информация, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, используемых Обществом, а именно:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде;

-информация, необходимая Обществу для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

- информация об осуществлённых Обществом и его клиентами финансовых операциях;

- ключевая информация средств криптографической защиты информации, используемой Обществом и его клиентами при осуществлении финансовых операций.

Устройство - это любое устройство (компьютер, планшет, мобильный телефон), с помощью которого клиент осуществляет финансовые операции.

Основные риски несанкционированного доступа к защищаемой информации неуполномоченными лицами, в том числе с использованием вредоносных программ, включают:

- риск раскрытия конфиденциальной информации (о счетах, операциях, персональных данных и т.д.);

- риск выполнения юридически значимых действий без согласия клиента (операции с активами, изменение регистрационных данных и т.п.);

- риск воздействия на носители информации, что может привести к нарушению обязательств по договору или невозможности использования сервисов Общества.

1.3. Несанкционированный доступ к защищаемой информации возможен через удаленный доступ к устройствам клиента вследствие взлома или получения данных для проведения операций.

1.4. Применяемые в Обществе средства защиты информации обеспечивают высокий уровень безопасности и снижают риски мошенничества при условии выполнения клиентами рекомендаций настоящего документа.

2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. Используйте лицензионное программное обеспечение.

2.2. Регулярно обновляйте программное обеспечение и операционную систему.

2.3. Установите и своевременно обновляйте лицензионное антивирусное ПО с функцией автоматического обновления.

2.4. Проводите полную проверку жесткого диска на вирусы не реже одного раза в месяц.

2.5. Проверяйте на вирусы информацию, получаемую и передаваемую через телекоммуникационные каналы и внешние носители.

2.6. Контролируйте конфигурацию устройства и не допускайте несанкционированных изменений.

2.7. Не используйте права администратора без необходимости.

2.8. Используйте межсетевые экраны и устанавливайте программы только через IT-поддержку (в случае наличия последний).
2.9. Исключите бесконтрольный доступ к компьютерам.
2.10. Не используйте устройство для общения в социальных сетях, переписки в интернет-мессенджерах и посещения сомнительных сайтов.
2.11. При подозрении на наличие вирусов воздержитесь от использования системы до устранения проблемы.

3. Рекомендации по использованию паролей в целях защиты информации.

3.1. Не хранить логины и пароли в местах, доступных для посторонних.
3.2. Используйте сложные пароли длиной не менее 8 символов, включающие латинские буквы в верхнем и нижнем регистрах, цифры и специальные символы.
3.3. Избегайте использования простых паролей и осмысленных слов.
3.4. Регулярно меняйте пароли, особенно если есть подозрения на их компрометацию.
3.5. Избегайте многократного использования одного пароля.
3.6. По возможности откажитесь от функции сохранения пароля на устройстве (браузере, приложении).
3.7. При хранении пароля в электронном виде, храните пароль так, чтобы доступ к нему можно было получить, введя другой пароль (защищенные заметки, приложения по хранению паролей без доступа в сеть).

4. Рекомендации по защите от фальсифицированных интернет-ресурсов

4.1. Мошеннические сайты могут выглядеть как настоящие и собирать конфиденциальную информацию.
4.2. Всегда проверяйте адрес отправителя электронных писем.
4.3. Анализируйте текст писем на наличие подозрительных элементов.
4.4. Внимательно проверяйте ссылки в письмах и избегайте подозрительных URL.
4.5. Не открывайте вложения от неизвестных отправителей.
4.6. Относитесь ко всем неизвестным Интернет сайтам как к потенциально мошенническим и ограничивайте предоставляемую информацию, откажитесь от загрузки на устройства файлов с таких сайтов.

5. Рекомендации по защите мобильных устройств и СМС-подтверждений

5.1. Не оставляйте мобильное устройство без присмотра.
5.2. Установите парольную защиту на мобильное устройство.
5.3. Не устанавливайте приложения из сомнительных источников.
5.4. В случае проблемы с SIM-картой незамедлительно обратитесь к оператору связи и в Общество.
5.5. При утрате устройства обратитесь к оператору связи и заблокируйте доступ к мобильному приложению через Общество.
5.6. При смене номера телефона сообщите об этом Обществу.
5.7. Всегда проверяйте реквизиты платежа в СМС-подтверждениях.
5.8. При подозрительных СМС или электронных сообщениях о совершенных операциях немедленно свяжитесь с Обществом.

6. Рекомендации по защите информации при общении с незнакомцами

6.1. Никогда не раскрывайте конфиденциальную информацию незнакомым лицам, включая логины, пароли, данные банковских карт, номера счетов и другие личные данные.

6.2. Будьте осторожны при получении звонков, сообщений или писем от неизвестных отправителей, представляющихся сотрудниками банков или других организаций. Настоящие сотрудники никогда не будут запрашивать конфиденциальную информацию таким образом.
6.3. Если вы получили подозрительное сообщение или звонок с просьбой предоставить конфиденциальную информацию, немедленно прекратите общение и свяжитесь с Обществом по официальным контактам для подтверждения подлинности запроса.
6.4. Никогда не переходите по ссылкам и не открывайте вложения в сообщениях от незнакомцев, особенно если они запрашивают ввод личных данных или финансовой информации.
6.5. Избегайте общения с незнакомцами в интернет-мессенджерах и социальных сетях по вопросам, связанным с финансами или личной информацией.
6.6. Регулярно проверяйте настройки конфиденциальности в социальных сетях и мессенджерах, чтобы ограничить доступ к вашей личной информации для посторонних лиц.
6.7. При общении через интернет-мессенджеры и социальные сети избегайте использования общедоступных или незашифрованных сетей Wi-Fi, так как это может привести к перехвату вашей информации злоумышленниками.
6.8. Будьте внимательны к любым предложениям о помощи или выгодных сделках от незнакомых лиц, так как они могут быть мошенническими.
6.9. Используйте только официальные и проверенные каналы связи для обсуждения вопросов, связанных с финансовыми операциями и личными данными.
6.10. Мошенники могут использовать чужие имена, взломанные аккаунты, сгенерированные голосовые сообщения и видео для получения конфиденциальной информации. Всегда проверяйте подлинность таких сообщений и не доверяйте непроверенным источникам.
6.11. Если вы подозреваете, что ваша информация могла быть скомпрометирована в результате общения с незнакомцем, немедленно обратитесь в Общество и примите меры для защиты своих данных, включая изменение паролей и уведомление соответствующих служб безопасности.