General Invest

РЕКОМЕНДАЦИИ КЛИЕНТАМ ООО КОНЦЕРН «ДЖЕНЕРАЛ-ИНВЕСТ»

ПО СОБЛЮДЕНИЮ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ КОДОВ

1. Общие положения.

1.1. Общество с ограниченной ответственностью Концерн «ДЖЕНЕРАЛ-ИНВЕСТ» (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 клиентов Общества о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

1.2. Под защищаемой информацией понимается информация, получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, используемых Обществом, а именно:

1.2.1. информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Общества и (или) клиентами Общества;

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

1.2.3. информация об осуществленных Обществом и его клиентами финансовых операциях;

1.2.4. ключевая информация средств криптографической защиты информации, используемой Обществом и его клиентами при осуществлении финансовых операций (в случаях, предусмотренных договорами на оказание услуг).

1.3. Под устройством в настоящем документе понимается устройство, с использованием которого клиент осуществляет финансовые операции. К таким устройствам относятся персональные и портативные компьютеры, а также мобильные телефоны.

1.4. К основным рискам получения несанкционированного доступа к защищаемой информации неуполномоченными лицами, в том числе с использованием вредоносных программ, относятся:

- Риск разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию счетов, подключенных услугах, персональных данных, иной значимой информации.

- Риск совершения юридически значимых действий, включая совершение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента.

- Риск воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов Общества для реализации своих намерений.

1.5. Несанкционированный доступ к защищаемой информации происходит посредством удалённого доступа к устройствам клиента в результате взлома защиты устройства или получения данных для проведения операции и/или доступа к защищаемой информации (коды доступа, коды СМС-подтверждения и т.д.) с помощью методов, основанных на особенностях психологии людей («Фишинг», «Троянский конь» и т.д.), а также вследствие заражения устройства клиента вредоносной программой.

Цель фишинга – перехват личных данных клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

Техника «Троянский конь» предполагает расчет злоумышленника на любопытство, страх и другие эмоции пользователей. В этих целях пользователю отправляется по электронной почте письмо, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу, компромат на сотрудника и т.п.; на самом деле в письме находится вредоносная программа.

Заражение устройства клиента осуществляется также через спам-рассылку СМС или ММС-сообщения, сообщения электронной почты, сообщения, в том числе в мессенджерах, содержащих ссылки на

внешние ресурсы, или при переходе по ссылкам на ресурсы сети Интернет. При переходе по ссылкам вредоносная программа устанавливается на устройство клиента.

1.6. Средства и методы защиты информации, применяемые в Обществе, позволяют обеспечить необходимый уровень безопасности и минимизировать мошеннические действия со стороны неуполномоченных лиц при условии выполнения клиентами рекомендаций, изложенных в настоящем документе.

2. Рекомендации по защите информации от воздействия вредоносного кода.

2.1. Пользуйтесь компьютерами с установленным лицензионным программным обеспечением.

2.2. Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

2.3. Обязательно установите и своевременно обновляйте на компьютере лицензионное антивирусное программное обеспечение с функцией автоматического обновления вирусных баз. Антивирусное ПО должно запускаться автоматически, с загрузкой операционной системы.

2.4. Не реже одного раза в месяц должна осуществляться полная проверка жесткого диска компьютера на предмет наличия вирусов и вредоносного программного кода.

2.5. Рекомендуется подвергать предварительному антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование внешних носителей информации должно осуществляться в автоматическом режиме.

2.6. Необходимо принять меры по контролю за конфигурацией устройства, с использованием которого осуществляется информационный обмен с Обществом, и не допускать несанкционированных программно-аппаратных изменений конфигурации.

2.7. Не используйте права администратора без необходимости. В повседневной практике входите в систему с учетной записью пользователя, не имеющего прав администратора.

2.8. При работе в сети Интернет используйте межсетевые экраны. Не устанавливайте каких-либо программ с сайтов, которые вы посещаете. Все программные средства должна устанавливать только ваша служба IT-поддержки.

2.9. Исключите возможность бесконтрольного доступа посторонних лиц (гостей, посетителей) к вашим компьютерам.

2.10. Рекомендуем ограничить информационный обмен в сети Интернет только надежными информационными порталами и проверенными корреспондентами электронной почты. Не используйте компьютер, с которого Вы осуществляете информационный обмен с Обществом, для общения в социальных сетях, переписке в интернет-мессенджерах, а также для посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), так как именно через подобные ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.11. При подозрениях на наличие вирусов на компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), следует полностью воздержаться от использования систем информационного обмена до устранения проблемы.

3. Рекомендации по использованию паролей в целях защиты информации.

3.1. Используемые логины и пароли запрещается записывать и хранить в местах, доступных посторонним лицам. Необходимо хранить пароль в тайне и предпринимать необходимые меры предосторожности для предотвращения его несанкционированного использования.

3.2. Для доступа к устройству рекомендуется использовать сложные пароли, удовлетворяющие следующим требованиям:

- Длина пароля должна быть не менее 8 символов.
- Пароль должен содержать символы трех приведенных далее групп: букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр, специальных символов и знаков пунктуации.

3.3. Не используйте простые пароли, представляющие собой осмысленные слова, дату рождения, номер телефона и т.д., последовательности повторяющихся на клавиатуре символов, последовательности трех и более повторяющихся символов.

3.4. Рекомендуется регулярно менять пароли; в случаях, если пароль стал известен постороннему лицу или у пользователя есть подозрения, что пароль стал известен постороннему лицу, пароль подлежит обязательному изменению.

4. Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

4.1. Мошеннический или поддельный web-сайт — это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете. Они предназначены для сбора конфиденциальной информации обманным путем. Ввод логина и пароля на таком сайте приводит к получению этих данных злоумышленниками, то есть к разглашению идентификационных данных.

4.2. Перед просмотром входящего электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании. Подделать адрес электронной почты отправителя очень просто, поэтому будьте внимательны.

4.3. Внимательно читайте текст электронного письма. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это электронное письмо, отправленное мошенниками.

4.4. Опасайтесь безличных обращений, таких как «Уважаемый пользователь», или обращения по адресу электронной почты. Типичное фишинговое письмо начинается с обезличенного приветствия. Не открывайте вложений, прикрепленных к подобным письмам.

4.5. Внимательно анализируйте ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить Вас на мошеннический web-сайт. Если ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не переходите по этой ссылке.

4.6. Не открывайте вложений, прикрепленных к письмам от неизвестных отправителей.

5. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами при использовании мобильных устройств и кодов СМС подтверждения.

5.1. Мобильное устройство клиента не должно оставляться без присмотра, чтобы исключить несанкционированное использование мобильного приложения.

5.2. Рекомендуется установить парольную защиту на мобильное устройство.

5.3. Не устанавливайте на устройство программы и приложения из сомнительных источников.

5.4. В случае неожиданного прекращения работы SIM-карты телефона следует незамедлительно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены SIM-карты, а также в Общество для выявления возможных несанкционированных операций.

5.5. При утрате (потере, хищении) мобильного устройства, на которое установлено мобильное приложение, следует незамедлительно обратиться к своему оператору сотовой связи для блокировки SIM-карты, заблокировать доступ в мобильное приложение при помощи специалистов Общества, а также обратиться в Общество для выявления возможных несанкционированных операций.

5.6. При смене номера телефона рекомендуется незамедлительно сообщить об этом Обществу.

5.7. При подтверждении Ваших операций одноразовым СМС-паролем, всегда обращайте внимание на реквизиты платежа, а также сумму, указанные в полученном СМС-сообщении. Они должны соответствовать реквизитам Вашей операции.

5.8. В случае поступления на мобильный номер телефона СМС-оповещения или электронного сообщения о совершенной операции, немедленно связаться с Обществом любым возможным способом либо лично явиться в Общество, если операция не была Вами осуществлена.