Рекомендации Клиенту для обеспечения безопасности информации.

Акционерное общество «ФинИст» (далее – Компания) в рамках соблюдения требований Положения Банка России от 17.04.2019г. № 684-П «Положения 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 Компании о возможных рисках получения несанкционированного доступа к защищаемой информации:

1. Доступ со стороны третьих лиц может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянии счетов, подключенных услугах, персональных данных и иной значимой информации.
2. Доступ со стороны третьих лиц может повлечь за собой совершение 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.
3. Доступ со стороны третьих лиц может повлечь за собой деструктивное воздействие на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств по договору или невозможности использования сервисов компании для реализации своих намерений.

В целях предотвращения несанкционированного доступа к защищаемой информации и своевременному обнаружению воздействия вредоносного кода, Компания рекомендует следующее:

1. Рекомендации по защитным мерам для компьютера.

– Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е.должна быть отключена возможность загрузки с дискет, CD/DVD приводов, USB-flash дисков, загрузка по сети и т.п.;

– Доступ к изменению настроек BIOS должен быть защищен паролем;

– На компьютере необходимо использовать только лицензионное системное и прикладное программное обеспечение;

– На компьютере должна быть установлена только одна операционная система;

– Рекомендуется своевременно проводить обновления системного и прикладного программного обеспечения;

– В обязательном порядке должны быть установлены и регулярно обновляться антивирусные программы (например, Kaspersky, Dr.Web, Symantec, Avira, ESET, NOD32, McAfee). Отдавайте предпочтение российским разработчикам. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов и другого вредоносного программного обеспечения;

– Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему;

– Не устанавливать и не использовать на компьютере программы для удаленного управления (Например, RDP, TeamViewer, Radmin, Ammyy Admindр.);

– Для доступа к информационным системам не используйте общедоступные компьютеры (например, установленные в интернет-кафе, гостинице), публичные беспроводные сети (бесплатный Wi-Fi и прочее).

2. Рекомендации по защитным мерам для мобильного устройства.

– Устанавливать Приложения на мобильное устройство можно только из официальных репозиториев производителей мобильных платформ: AppStoreи Google Play;

– Установите на мобильное устройство антивирус и своевременно его обновляйте. Для платформы Android рекомендуем бесплатные приложения Dr.Web Light (доступен для загрузки из Google Play) и Kaspersky MobileAntivirus: AppLock & WebSecurity(доступен для загрузки из GooglePlay);

– Своевременно устанавливайте обновления безопасности операционной системы;
– Не взламывайте свой телефон (например, через Jailbreaking, реинжиниринг, принудительное получение root-прав), так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате ваш телефон становится уязвимым к заражению вирусным программным обеспечением;
– Не отключайте и не взламывайте встроенные механизмы безопасности вашего устройства;
– При наличии технической возможности включите шифрование данных на своём устройстве;
– Сохраняйте в тайне Ваши имя пользователя (логин), пароль для доступа в информационные системы и СМС-коды. Не сообщайте эти данные никому.

3. Рекомендации по парольной защите.

Учетные записи операционной системы должны быть защищены паролями с учётом следующих параметров:
– Длина пароля должна быть не менее 8 символов;
– В пароле обязательно должны присутствовать заглавные и прописные(верхнего и нижнего регистра) символы, цифры, а также специальные символы (например, #, %, ^, * и т.п.); примеры паролей (Hjf#48dft, 5$ma(fq5eR,%dEr*2fvw2);
– В качестве пароля не следует использовать имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
– В качестве пароля не следует использовать повторяющуюся комбинацию из нескольких символов, либо комбинацию символов, набираемых в закономерном порядке;
– Пароль должен меняться не реже 1 раза в 3 месяца, а также при компрометации (или подозрении в компрометации) пароля;
– При смене пароля новый пароль не должен совпадать с ранее используемыми паролями;
– Запрещено произносить вслух, записывать и хранить в любом доступном посторонним лицам месте пароли;
– Не храните логин и пароль в мобильном телефоне, смартфоне.

4. Работа с сообщениями.

– Не отвечайте на сообщения, требующие предоставить, подтвердить или уточнить вашу конфиденциальную информацию: пароли, логины, фамилию, имя, отчество, паспортные данные, номер мобильного телефона, на который поступают одноразовые пароли и другие данные;
– Не открывайте подозрительные файлы, поступившие Вам по электронной почте;
– Не отвечайте на полученное подозрительное сообщение и не переходите по ссылкам, указанным в сообщении.