

РЕКОМЕНДАЦИИ

по защите информации от воздействия вредоносных программных кодов и несанкционированного доступа третьих лиц к защищаемой информации

Настоящим Общество с ограниченной ответственностью Инвестиционная компания «Тренд» в соответствии с п.1.13 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, утвержденного Банком России 20.04.2021 № 757-П, информирует Клиентов о мерах по предотвращению несанкционированного доступа к защищаемой информации.

В целях предотвращения несанкционированного доступа к информации, содержащейся в поручениях, требованиях, направляемых Вами в электронном виде с использованием средств вычислительной техники, и к иной конфиденциальной информации, в том числе о финансовых операциях, и противодействия осуществлению незаконных финансовых операций лицами, не обладающими правом их осуществления, а также в целях своевременного обнаружения программного кода, приводящего к нарушению штатного функционирования средств вычислительной техники (вредоносного кода), рекомендуем Вам соблюдать следующие меры:

1. Не сообщайте третьим лицам идентификаторы пользователя и пароли, предназначенные для использования Вами средств вычислительной техники (компьютер, планшет, ноутбук, мобильный телефон, смартфон и т.д.): логин, постоянный пароль, одноразовые пароли, контрольную информацию;
2. Не записывайте логины и пароли на бумаге, не храните их на видном месте (на рабочем столе, на мониторе, на/под клавиатурой и т.п.), не используйте в качестве места хранения в незащищенном виде логинов и паролей жесткие диски средств вычислительной техники. Храните указанную информацию в надежном месте, доступ к которому третьим лицам исключен;
3. При составлении пароля используется прописные и строчные буквы, цифры и специальные символы;
4. Регулярно, не реже чем раз в 3 (Три) месяца, производите смену пароля;
5. Не используйте одинаковые логин и пароль для доступа к разным устройствам и системам;
6. При работе с электронной почтой не открывайте письма и их вложения (при наличии), полученные от неизвестных отправителей, а также не переходите по ссылкам в этих письмах;
7. Используйте только лицензионное программное обеспечение;
8. Своевременно обновляйте программное обеспечение и его компоненты, только из проверенных источников, находящихся в ведении их разработчиков;
9. Своевременно устанавливайте обновления операционной системы, в особенности критические обновления безопасности;
10. Входите в систему под учетной записью пользователя, не имеющей прав администратора. Без необходимости не используйте учетную запись с правами администратора;
11. Не используйте средства удалённого администрирования (TeamViewer и подобные);
12. Своевременно обновляйте программы антивирусной защиты. По возможности используйте максимальный уровень безопасности в настройках антивируса. В таких случаях антивирусная система будет проверять все объекты и при обнаружении вирусов и вредоносных

кодов удалять их в автоматическом режиме, с уведомлением Вас о данной операции, но без требования дальнейшего действия. Также при обнаружении фишинговых сайтов, т.е. сайтов, имитирующих официальные сайты компаний, доступ на такие сайты будет ограничен в автоматическом режиме;

13. По возможности настраивайте автоматический запуск системы антивирусной защиты при старте операционной системы;

14. Не реже раза в неделю запускайте полную проверку средств вычислительной техники программами антивирусной защиты. Рекомендуется установить регламентное задание такой проверки;

15. При получении накопителей информации (флеш-накопители, CD/DVD диски, внешние жесткие диски и т.д.) производите полное сканирование программами антивирусной защиты всех файлов на этих накопителях. По возможности такое сканирование должно быть настроено на выполнение при подключении любого накопителя, в автоматическом режиме;

16. При работе в сети Интернет не допускайте установку программного обеспечения из недостоверных или сомнительных источников. Как правило они маскируются под установку плагинов;

17. Ограничьте работу в сети Интернет только с надежными сайтами;

18. Не используйте функцию сохранения (автозаполнения) логина и пароля в установках браузера;

19. Не используйте средства вычислительной техники, с которых Вы осуществляете финансовые операции, для общения в социальных сетях, посещения развлекательных сайтов (сайтов знакомств, игровых сайтов, распространяющих музыку, фильмы и т.д.), т.к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы;

20. Для совершения финансовых операций не используйте средства вычислительной техники, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного средства вычислительной техники;

21. При подозрении на наличие вредоносного кода на Вашем средстве вычислительной техники (зависание, замедление работы, активная работа жесткого диска в режиме покоя, самопроизвольные стирания файлов, необычная сетевая активность системы и т.д.), полностью воздержитесь от использования систем дистанционного финансового обслуживания до момента полной проверки системы;

22. Не оставляйте средства вычислительной техники без присмотра, при завершении работы блокируйте или выключайте их, что защитит Вас от несанкционированного доступа к финансовым операциям и установке вредоносного кода неавторизованными сторонними пользователями;

23. Не подключайтесь на своих средствах вычислительной техники к сторонним публичным WI-FI сетям, т.к. они не гарантируют защищенность передачи данных;

24. При утере средства вычислительной техники, с которого осуществлялись финансовые операции, Вам необходимо оперативно поставить в известность ООО ИК «Тренд», позвонив по телефону +7 (495) 151-41-00.