УТВЕРЖДЕНО
Приказом Генерального директора
АО «Финансовый Маркетплейс Сравни.ру»
от «17» ноября 2021 № 42

Памятка
по информационной безопасности для Потребителей АО «Финансовый Маркетплейс Сравни.ру»

Редакция 01/2021

г. Москва

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

В рамках исполнения Федерального закона № 211 «О совершении финансовых сделок с использованием финансовой платформы» от 20 июля 2020 года и в соответствии с требованиями положений Политики по информационной безопасности АО «Финасовый Маркетплейс Сравни.ру» (далее – Оператор ФП), разработана настоящая Памятка для Потребителей Оператора ФП.

В настоящей Памятке приведены рекомендации Потребителям Оператора ФП по снижению рисков воздействия вредоносного программного обеспечения и несанкционированного доступа к информации. Оператор ФП доводит до вашего сведения, что использование Дистанционных каналов обслуживания сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Потребителей и осуществления несанкционированных переводов денежных средств со счетов неуполномоченными лицами.

К конфиденциальной информации Потребителей относится:

- смс-коды, приходящие от финансовой платформы;
- информация о дате и времени встречи с представителем в рамках идентификации;
- иная информация Потребителя, обрабатываемая Оператором ФП;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации;
- информация о банковских счетах и остатках денежных средств;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных Потребителей распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения Потребителями права распоряжения денежными средствами.

Настоящая Памятка по информационной безопасности для Потребителей Оператора ФП (далее — Памятка) является нормативным документом Оператора ФП и подлежит публикованию в открытом доступе на официальном сайте.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Оператор ФП – АО «Финансовый Маркетплейс Сравни.ру».

Потребитель финансовых услуг (Потребитель) — физическое лицо, являющееся потребителем финансовых услуг, присоединившееся к Договору об оказании услуг оператора финансовой платформы в порядке, установленном Правилами платформы, в целях совершения Финансовых сделок.

ПО – программное обеспечение.

Дистанционные каналы обслуживания – это технологии предоставления услуг Потребителю с использованием средств телекоммуникаций без его непосредственного визита.

Вредоносное программное обеспечение – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам информационных систем или к информации, хранимой в информационных системах, с целью несанкционированного использования ресурсов информационных систем или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу информационных систем, и/или владельцу сети информационных систем, путем копирования, искажения, удаления или подмены информации.

Антивирусное программное обеспечение (АПО) – специализированная программа для обнаружения вирусов, в том числе нежелательных (считающихся вредоносными) программ и восстановления заражённых такими программами файлов, а также для предотвращения заражения файлов или операционной системы вредоносным кодом.

Компрометация — событие, дающее основание полагать, что защищаемая информация стала доступна постороннему лицу, в результате чего ее дальнейшее использование представляется небезопасным.

Устройство — любое средство автоматической обработки информации, используемое при информационном взаимодействии с системами и сервисами Оператора ФП (к примеру, персональный компьютер, мобильный телефон и т. п.).

Личный кабинет - персональная страница Потребителя на Сайте Оператора ФП, доступ к которой предоставляется Потребителю посредством прохождения процедуры Авторизации.

3. ОБЩИЕ РЕКОМЕНДАЦИИ

3.1 Используйте на ваших устройствах только лицензионное программное обеспечение, полученное из источников, гарантирующих отсутствие вредоносного ПО.

3.2 Регулярно устанавливайте обновления операционной системы, брандмауэра и прикладного программного обеспечения, выпускаемые компаниями-производителями.

3.3 Не рекомендуется устанавливать на устройства программные средства, предназначенные для удаленного управления компьютером.

3.4 Располагайте ваши мониторы и печатающие устройства таким образом, чтобы исключить или ограничить несанкционированный доступ других лиц к отображаемой и печатаемой информации.

3.5 В случае ухода от Устройства, на котором произведен вход в Личный кабинет Оператора ФП даже на непродолжительное время, рекомендуется блокировать Устройство.

4. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ ПАРОЛЬНОЙ ЗАЩИТЫ

4.1 Не записывайте ваши пароли на бумажных носителях, не сохраняйте их в файлах на жестком диске или в незашифрованном виде на ваших устройствах, не используйте функцию «Сохранить пароль», так как в большинстве случаев программы сохраняют пароли в незашифрованном виде, и злоумышленник, получивший доступ к вашему компьютеру, может воспользоваться ими.

4.2 Никому и никогда не сообщайте логин, постоянный пароль, одноразовый пароль, коды из смс и прочие идентификаторы, позволяющие получить доступ к личному кабинету Оператора ФП, в том числе вашим родственникам или системным администраторам вашей компании, а также сотрудникам Оператора ФП.

4.3 Для доступа к автоматизированным системам рекомендуется использовать сложные пароли, удовлетворяющие следующим требованиям:

- длина пароля должна быть не менее 12 символов;
- пароль должен включать в себя символы из всех следующих групп: букв латинского алфавита в верхнем регистре (A-Z), букв латинского алфавита в нижнем регистре (a-z), цифр (0-9), специальных символов и знаков пунктуации (!@#$%^&*(),.?).

4.4 Не используйте простые пароли, представляющие собой осмысленные слова (например, password), дату рождения, номер телефона и т. д., последовательности символов, последовательно расположенных на клавиатуре (например, qwerty), последовательности трех и более повторяющихся символов (например, 77777777, 111adZZZ).

4.5 Рекомендуется производить смену пароля, используемого для доступа к автоматизированным системам, не реже одного раза в 90 дней.

5. РЕКОМЕНДАЦИИ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

5.1 Для защиты от вредоносного ПО рекомендуется использовать лицензионное антивирусное ПО, обеспечивающее комплексную защиту и функционирующее в автоматическом режиме.

5.2 Антивирусное программное обеспечение должно регулярно обновляться.

5.3 Не реже 1 (одного) раза в неделю проводите полное антивирусное сканирование на ваших устройствах. В случае обнаружения подозрительных файлов их следует удалить, а при невозможности удаления — поместить в карантин.

5.4 Не отключайте антивирусное программное обеспечение ни при каких обстоятельствах.

5.5 Не пытайтесь авторизоваться в личном кабинете Оператора ФП с непроверенных устройств и устройств в общественных местах. Такие устройства могут отслеживать все вводимые данные, в том числе авторизационные.

5.6 Не подключайтесь к личному кабинету Оператора ФП с устройства, которое подключено к небезопасной Wi-Fi сети.

6. РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

6.1 Не посещайте Интернет-сайты сомнительного содержания.

6.2 Не переходите по гиперссылкам (ссылки могут вести на зловредные и мошеннические ресурсы), содержащимся в электронных письмах, полученных вами от неизвестных отправителей, а также не открывайте файлы, вложенные в них (это могут быть вредоносные вложения). Такие письма рекомендуется немедленно удалять.

6.3 Всегда проверяйте, чтобы веб-адрес Интернет-сайта, указанный в адресной строке вашего веб-браузера, начинался с префикса https:// (отображается в виде «закрытого замка»), а не http://. Кроме того, подлинность веб-адреса должна быть подтверждена SSL-сертификатом международного сертификационного центра

7. ЗАКЛЮЧИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ

7.1 Не распространяйте и не указывайте свои персональные данные, номера счетов, банковских карт и т.д.

7.2 Включите функцию запроса PIN-кода для SIM-карты, к номеру которой привязан личный кабинет Оператора ФП.

7.3 Для работы с Оператором ФП и исключения возможности компрометации учетной записи используйте только подтвержденный номер телефона, зарегистрированный на ваше имя.

7.4 В случае утери или замены SIM-карты, телефонный номер которой привязан к личному кабинету Оператора ФП — сообщите в контактный центр Оператора ФП (**8 800 600 81 35**).

Прошито, пронумеровано
и скреплено печатью

5 (Пять)

листа (ов)

Генеральный директор
АО «Финансовый Маркетплейс Сравни.ру»

С.И. Леонидов