АКЦИОНЕРНОЕ ОБЩЕСТВО «ФИНФОРТ МП»
(АО «ФИНФОРТ МП»)

УТВЕРЖДЕНА
Приказом ВРИО Генерального директора
АО «Финфорт МП»
№ МП66/24ОД от «13» ноября 2024 года.

Памятка по информационной безопасности для клиентов АО «Финфорт МП»

(версия – 1.2)

Москва
2024

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Памятка по информационной безопасности для клиентов АО «Финфорт МП» (далее – Памятка) разработана в рамках исполнения Федерального закона № 211-ФЗ от 20.07.2020 «О совершении финансовых сделок с использованием финансовой платформы» и в соответствии с требованиями Положения Банка России № 757-П от 20.04.2021 «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» для клиентов АО «Финфорт МП».

1.2. Использование клиентами АО «Финфорт МП» дистанционных каналов обслуживания сопряжено с риском получения несанкционированного доступа к их конфиденциальной информации и осуществления несанкционированных переводов денежных средств со счетов лицами, не обладающими правом их осуществления.

1.3. В настоящей памятке приведены рекомендации по информационной безопасности для клиентов АО «Финфорт МП», следование которым позволит снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

1.4. Для уточнения информации, связанной с информационной безопасностью, или при подозрении на мошеннические действия, клиенту необходимо обратиться в Call-центр АО «Финфорт МП» по номеру телефона 8 (800) 600-30-37 или по электронной почте info@finorma.ru.

1.5. Настоящая памятка является нормативным документом АО «Финфорт МП» и подлежит опубликованию в открытом доступе на официальном сайте.

2. РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. К общим причинам возникновения рисков информационной безопасности относятся:

- установка на устройство клиента вредоносного программного обеспечения, которое позволит злоумышленнику получить доступ к конфиденциальной информации (в том числе перехватывать информацию, вводимую с клавиатуры (логины, пароли, реквизиты банковских карт и пр.)), а также осуществлять критичные (значимые) операции от имени клиента;
- получение конфиденциальных данных (пароля, SMS-кода, кодового слова, реквизитов банковской карты и пр.) путем обмана и злоупотребления доверием:
  - злоумышленник может связаться с клиентом по телефону и использовать любую легенду (например, представиться сотрудником АО «Финфорт МП», банка, правоохранительных органов, прокуратуры, ФСБ, Центрального Банка России, Росфинмониторинга, Социального Фонда России и т.д.), чтобы убедить клиента сообщить ему необходимые данные;
  - злоумышленник может направлять поддельные сообщения по электронной почте или SMS, мотивирующие клиента предоставить конфиденциальную информацию злоумышленнику или совершить действия на устройстве (перейти на поддельный сайт, открыть вложение к письму, содержащее вредоносное программное обеспечение, и пр.), которые также позволят злоумышленнику получить доступ к личному кабинету клиента и/или его конфиденциальным данным;

- кража устройства или несанкционированный доступ к устройству, с которого клиент осуществляет доступ к услугам и сервисам финансовой платформы, что позволит злоумышленнику получить доступ к личному кабинету клиента и к конфиденциальной информации, хранимой на устройстве;
- использование утерянного или украденного телефона (SIM-карты) для получения SMS-кодов, которые применяются для подтверждения критичных (значимых) операций, что позволит злоумышленнику обойти защиту.

2.2. Перечень причин возникновения рисков информационной безопасности, определенный п. 2.1 настоящей Памятки, не является исчерпывающим. Причины возникновения рисков зависят от конкретной ситуации.

3. РЕКОМЕНДУЕМЫЕ МЕРЫ ЗАЩИТЫ

3.1. **Обеспечение конфиденциальности информации**

3.1.1. Никогда не передавайте третьим лицам конфиденциальную информацию, позволяющую получить доступ в личный кабинет клиента финансовой платформы, а также получить возможность осуществления финансовых операций (логины, пароли, SMS-коды, кодовые фразы и слова, сведения о банковских картах, PIN-коды и пр.).

3.1.2. При поступлении телефонных звонков или при личных встречах следует помнить следующее:

- сотрудники АО «Финфорт МП», банков, правоохранительных органов, прокуратуры, ФСБ, Центрального Банка России, Росфинмониторинга, Социального Фонда России и т.д. никогда не запрашивают логины, пароли, SMS-коды, кодовые фразы и слова, сведения о банковских картах, PIN-коды и другую информацию, позволяющую получить доступ в личный кабинет клиента, а также получить возможность осуществления финансовых операций;
- сотрудники АО «Финфорт МП» никогда не требуют оплаты – ни при регистрации, идентификации, оформлении заявок, ни для подтверждения данных или для привязки банковской карты, а также ни в каких иных случаях;
- сотрудником АО «Финфорт МП», банка, правоохранительных органов, прокуратуры, ФСБ, Центрального Банка России, Росфинмониторинга, Социального Фонда России и т.д. может представиться любой человек (в том числе злоумышленник);
- если поступивший звонок кажется подозрительным, необходимо сбросить его и самостоятельно перезвонить в Call-центр АО «Финфорт МП» (контактная информация указана в п. 1.4 настоящей памятки и на официальном сайте);
- если действия сотрудника кажутся подозрительными, то не выполняйте его требования до уточнения информации в Call-центре АО «Финфорт МП» (контактная информация указана в п. 1.4 настоящей памятки и на официальном сайте).

3.2. **Защита от SMS-мошенничества**

3.2.1. Мошеннические SMS-сообщения, как правило, содержат информацию, побуждающую выполнить указанные в сообщении действия (информируют о блокировке личного кабинета или банковской карты, о получении доступа к личному кабинету третьим лицом, о рекламных акциях, выгодных предложениях, выигрышах и т.п.). В результате выполнения таких действий клиентом, злоумышленник может получить доступ к его личному кабинету и/или конфиденциальным данным.

3.2.2. В случае получения подобных SMS-сообщений запрещается:
- перезванивать на номер телефона, указанный в сообщении;
- предоставлять конфиденциальную информацию (логины, пароли, SMS-коды, кодовые фразы и слова, сведения о банковских картах, PIN-коды и пр.), в том числе посредством направления ответных сообщений;
- проводить на устройствах какие-либо операции по инструкциям, полученным в сообщении;
- переходить по ссылкам, указанным в таких сообщениях.

3.2.3. Если полученное SMS-сообщение вызывает любые сомнения или опасения, необходимо обратиться в Call-центр АО «Финфорт МП» (контактная информация указана в п. 1.4 настоящей памятки и на официальном сайте)

3.3. **Безопасность при работе с электронной почтой**

3.3.1. Мошеннические e-mail-рассылки, предназначены, в основном, для:
- заманивания получателей писем на сайты-«ловушки», поддельные сайты, на которых под различными предлогами злоумышленник пытается получить конфиденциальную информацию (персональные данные, логины, пароли, SMS-коды, кодовые фразы и слова, сведения о банковских картах, PIN-коды и пр.), а также на таких сайтах часто размещается вредоносное программное обеспечение, заражающее устройства при посещении сайта;
- принуждения получателей писем под различными предлогами на открытие вложенных файлов, содержащих вредоносное программное обеспечение.

3.3.2. Признаки того, что электронное письмо является мошенническим:
- письмо замаскировано под официальные письма АО «Финфорт МП» или других организаций и требует каких-либо действий или ответа;
- адрес отправителя и тема сообщения замаскированы под обращения от имени АО «Финфорт МП» или других организаций;
- письма содержат ссылки на интернет-ресурсы, замаскированные (похожие) на официальные ресурсы АО «Финфорт МП» или других организаций;
- к письму прилагается файл-вложение, который настойчиво рекомендуют открыть;
- в тексте содержатся явные опечатки или орфографические ошибки.

3.3.3. АО «Финфорт МП» никогда не отправляет письма на электронную почту с просьбой подтвердить, обновить или предоставить конфиденциальную информацию, а также не просит зайти в личный кабинет по ссылке, указанной в письме.

3.3.4. При получении электронных писем:
- внимательно проверяйте отправителя письма;
- если письмо получено от доверенного отправителя:
  - при переходе по ссылке из такого письма убедитесь, что сайт подлинный и безопасный, прежде чем вводить конфиденциальные данные (см. п. 3.7.2 настоящей памятки);
  - если с такого сайта скачиваются файлы, то запустите антивирусную проверку перед их открытием;
  - запустите антивирусную проверку вложенных файлов (при наличии) перед их открытием;
- письма, полученные от недоверенных отправителей, необходимо удалить, не переходя по ссылкам из письма и не открывая вложенные файлы.

3.4. **Защита устройств**

3.4.1. Используйте на устройствах только лицензионное программное обеспечение, полученное из источников, гарантирующих отсутствие вредоносного программного обеспечения (например, официальные сайты производителей программного обеспечения). Использование взломанного программного обеспечения или программного обеспечения, полученного не с официального сайта производителя, опасно из-за возможного внедрения в такое программное обеспечение вредоносного кода.

3.4.2. Регулярно устанавливайте обновления операционной системы, брандмауэра и прикладного программного обеспечения, выпускаемые производителями программного обеспечения. Регулярные обновления программного обеспечения снижают риски заражения устройства.

3.4.3. Обеспечьте антивирусную защиту устройства в соответствии с разделом 3.5 настоящей памятки.

3.4.4. В целях предотвращения несанкционированного доступа к личному кабинету и/или конфиденциальной информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, рекомендуется:

- установить на устройство пароль для его разблокировки (требования к парольной защите описаны в разделе 3.6);
- не оставлять устройство без присмотра;
- не передавать устройство третьим лицам.

3.5. Не пытайтесь авторизоваться в личном кабинете с непроверенных устройств и устройств в общественных местах. Такие устройства могут отслеживать все вводимые данные.

3.6. В случае использования сетей Wi-Fi, используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если нет уверенности в достоверности имени точки доступа. Точки доступа WiFi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями злоумышленников, направленными на получение доступа конфиденциальной информации.

3.7. **Антивирусная защита**

3.7.1. Наличие на устройстве вредоносного программного обеспечения не обязательно сопровождается появлением баннеров, звуков, шифрованием или удалением файлов, замедлением производительности устройства или другой нетипичной и подозрительной активностью. Действие вредоносного программного обеспечения может быть направлено на передачу информации злоумышленнику (вводимая с клавиатуры информация (в том числе пароли, реквизиты банковских карт и другой конфиденциальной информации), файлы и пр.), такие действия могут быть незаметны на устройстве. По этой причине необходимо выполнение рекомендаций данного раздела на любом устройстве.

3.7.2. Для защиты от вредоносного программного обеспечения необходимо использовать лицензионное антивирусное программное обеспечение, обеспечивающее комплексную защиту и функционирующее в автоматическом режиме.

3.7.3. Антивирусное программное обеспечение должно регулярно обновляться.

3.7.4. Не реже одного раза в неделю необходимо проводить полное антивирусное сканирование на устройствах. В случае обнаружения подозрительных файлов их следует лечить, а при невозможности лечения – удалить.

3.7.5. Антивирусное программное обеспечение ни при каких обстоятельствах нельзя отключать.

3.8. **Парольная защита**

3.8.1. Для доступа к системам рекомендуется использовать сложные пароли, удовлетворяющие следующим требованиям:

- длина пароля должна быть не менее 8 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 (!@#$%^&*(),.?);
- не используйте пароли, представляющие собой осмысленные слова (например, password), дату рождения, номер телефона, имена супруга (супруги), детей, домашних животных и т. д., последовательности символов, последовательно расположенных на клавиатуре (например, qwerty), последовательности трех и более повторяющихся символов (например, 77777777, 111adZZZ).

3.8.2. Рекомендуется производить смену пароля, используемого для доступа к системам, не реже одного раза в 6 месяцев. При смене паролей не допускается повторяющиеся и схожие пароли (например: пароль1, пароль2, пароль3 и т.п.).

3.8.3. Необходимо использовать разные пароли для разных систем. Это поможет защитить другие системы при компрометации пароля для одной из систем.

3.8.4. При хранении паролей придерживайтесь следующих правил:

- при хранении паролей на бумажных носителях необходимо обеспечить надежную защиту таких носителей;
- не сохраняйте пароли в незашифрованном виде на устройствах;
- не используйте функцию «Сохранить пароль» в браузерах (так как в большинстве случаев пароли сохраняются в незашифрованном виде, и злоумышленник, получивший доступ к устройству, может воспользоваться ими).

3.8.5. Не сообщайте никому свои пароли.

3.9. **Безопасность при работе в сети Интернет**

3.9.1. При работе в сети Интернет следует помнить, что вредоносное программное обеспечение может быть размещено практически на любом сайте, поэтому крайне важно проводить антивирусную проверку всех скачанных файлов.

3.9.2. Прежде чем ввести конфиденциальные данные на сайте необходимо удостовериться в том, что:

- сайт использует защищенное соединение: в этом случае адресная строка в браузере начинается с «https://» (не с «http://»), а также в адресной строке должен быть символ замка, обозначающий наличие защищённого соединения, который может незначительно отличаться в зависимости от браузера;
- сайт подлинный: для этого необходимо сравнить адрес проверяемого сайта с адресом подлинного сайта (подлинный сайт можно найти в любой поисковой системе – обычно он отображается в первых трех результатах поиска).

3.9.3. При работе с финансовой платформой АО «Финфорт МП» убедитесь, что соединение установлено именно с официальным сайтом по адресу: https://finorma.ru.

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Соблюдение указанных рекомендаций и своевременное обращение в АО «Финфорт МП» при риске компрометации конфиденциальной информации помогут существенно снизить угрозу мошенничества.

4.2. Информационное взаимодействие с АО «Финфорт МП» следует осуществлять только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты, обычная и электронная почта и пр.), реквизиты которых указаны на официальном сайте АО «Финфорт МП».

4.3. АО «Финфорт МП» не несет ответственности за безопасность каналов связи, программ и аппаратных средств, которые используются клиентом для доступа к финансовой платформе.