ПАМЯТКА
о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, о мерах по предотвращению несанкционированного доступа к защищаемой информации и защите информации от воздействия вредоносных кодов

В соответствии с требованиями 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 (утв. Банком России 20 апреля 2021 г. N 757-П) АО «ГУТА-Страхование» (далее — Компания) настоящим доводит до сведения своих клиентов:

- рекомендации по защите информации от воздействия вредоносного кода (далее — вредоносная программа), приводящих к нарушению штатного функционирования средств вычислительной техники (далее — компьютерные устройства), в целях противодействия незаконным финансовым операциям;
- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносных программ.

1. Возможные риски получения несанкционированного доступа к защищаемой информации

При осуществлении финансовых операций следует принимать во внимание риски финансовых потерь, связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также с воздействием вредоносных программ.
Указанные риски могут быть обусловлены, включая, но не ограничиваясь, следующими ситуациями:

1.1. Кража идентификатора и пароля доступа (в том числе SMS-кодов) или иных конфиденциальных данных посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

1.2. Установка на устройство вредоносной программы, которая позволит злоумышленникам осуществить операции от Вашего имени.

1.3. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь сервисами Компании для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

1.4. Получение идентификатора доступа, пароля, SMS-кодов и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Компании или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или бумажное письмо по почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства.

1.5. Перехват сообщений электронной почты и получение несанкционированного доступа к отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена такой информацией. В случае получения доступа к вашей электронной почте, отправка сообщений от Вашего имени в Компанию.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) и клиентских устройств для доступа к информационным системам Компании несет Клиент. Компания не несет ответственность в случаях финансовых потерь, понесенных Клиентами в связи с пренебрежением правилами информационной безопасности.

К основным причинам возникновения рисков получения несанкционированного доступа к защищаемой информации относятся:

- неограниченный доступ третьих лиц к Вашему устройству;
- неограниченный доступ третьих лиц к информации о паролях и логинах, используемых для доступа к информационным ресурсам;
- несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет»;
- утрата (потеря, хищение) Вашего устройства;
- отсутствие непроверенного программного обеспечения;
- отсутствие действующего актуального антивирусного программного обеспечения с актуальными вирусными базами;
- несоблюдение Вами рекомендаций настоящей Памятки.

Перечень причин возникновения рисков получения несанкционированного доступа к защищаемой информации не является исчерпывающим. Причины возникновения рисков получения несанкционированного доступа к защищаемой информации зависят конкретной ситуации.

2. Рекомендации по защите информации от вредоносного кода

2.1. Рекомендуется работа на устройстве под учетной записью пользователя без прав администратора (в случае компьютерных операционных систем). Также рекомендуется внимательное отношение к всплывающим запросам на предоставление доступа установленному ПО (в случае мобильных операционных систем).

2.2. На Вашем устройстве должно быть установлено лицензированное антивирусное программное обеспечение (ПО). Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, не требующих ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов должно производиться антивирусным ПО в автоматическом режиме.

2.3. Не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка должна осуществляться согласно расписанию, выставленному в настройках антивирусного ПО.

2.4. Рекомендуется подвергать 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 должно осуществляться в автоматическом режиме.

2.5. При обмене электронными почтовыми сообщениями (эксплуатации почтовых клиентов) необходимо применять антивирусное ПО, поддерживающее проверку почтовых клиентов.

2.6. При возникновении подозрения на заражение устройства компьютерным вирусом (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) или нарушения работоспособности компьютера необходимо осуществить внеплановую проверку на наличие вредоносного ПО

(желательно с использованием двух антивирусных ПО). После удаления вирусов и восстановления работоспособности компьютера необходимо произвести смену паролей, удовлетворяющим требованиям п. 4.1.

2.7. Рекомендуется не открывать файлы, полученные по электронной почте от неизвестных отправителей.

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

3.1. Мошеннический или поддельный web-сайт – это небезопасный web-сайт, где под каким-либо предлогом предлагается ввести конфиденциальную информацию (аутентификационные данные). Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете (например, сайта своей страховой компании), и предназначены для сбора конфиденциальной информации обманным путем.

3.2. Мошенники могут изменить адрес электронной почты в преднамеренных целях, поэтому перед просмотром электронного письма всегда проверяйте адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании, отличаясь от него только на один символ.

3.3. Внимательно читайте текст электронного письма. Электронные письма от известных компаний, как правило, не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., возможно, это – электронное письмо, отправленное мошенниками.

3.4. Старайтесь сохранять спокойствие. Многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить Вас действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить Вас в том, что Вашему счету или Вашим данным угрожает опасность, если Вы немедленно не предпримете действия, выгодные злоумышленникам.

3.5. Внимательно анализируйте ссылки (например, на virustotal.com). Поддельные ссылки могут быть почти точной копией подлинных, при этом 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 ней.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1. Рекомендуется регулярно менять пароли для работы со своими учетными данными в различных системах. Длина Вашего пароля должна содержать не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов. В качестве пароля не рекомендуется использовать даты рождения, имена родственников, клички питомцев и т.п.

4.2. Рекомендуется использовать уникальные пароли для различных web-сайтов и систем, на которых хранятся и обрабатываются Ваши конфиденциальные данные (например, портал Госуслуг, личный кабинет, онлайн-Банкинг и т. д.).

4.3. В случае компрометации или подозрении на компрометацию пароля, рекомендуется незамедлительно сменить пароль на новый, удовлетворяющий требованиям п. 7.1.

4.4. Никому передавайте и не разглашайте свои пароли.

4.5. Рекомендуется установить пароли на учётные записи пользователей операционной системы на компьютере.

4.6. Рекомендуется установить на устройство актуальное антивирусное ПО и своевременно обновлять ПО антивирусные базы.

4.7. Рекомендуется включить блокировку экрана для мобильных устройств и отключить показ любых паролей при вводе.

4.8. Рекомендуется исключить возможность физического доступа посторонних лиц к устройству, с которого Вы осуществляете доступ к сайтам и информационным системам.

4.9. Рекомендуется применять на устройстве для работы специализированные программные и аппаратные средства безопасности: средства защиты от несанкционированного доступа, персональные межсетевые экраны, антишпионское программное обеспечение и т.п., обеспечить регулярное автоматическое обновление программного обеспечения этих средств.

4.10. На устройстве, с которого осуществляется доступ к сайтам и информационным системам, содержащим конфиденциальную информацию, рекомендуется исключить посещение WEB-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т.п. Использование нелицензионного программного обеспечения повышает риск получения несанкционированного доступа злоумышленников с целью хищения информации.

4.11. Рекомендуется включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ; старайтесь периодически просматривать журнал и реагировать на ошибки.

4.12. При проблемах с доступом к сайтам и нужным онлайн-сервисам необходимо установить браузеры, которые поддерживают российский сертификат безопасности. Отечественный аналог позволит заменить иностранный сертификат безопасности в случае его отзыва или окончания срока действия.

Сертификат безопасности предназначен для аутентификации сайта в Интернете при установлении защищенного соединения, для передачи данных в зашифрованном виде, для подтверждения подлинности сайта и его принадлежности владельцу, а также для защиты онлайн-транзакций.

На текущий момент такая функциональность есть у Яндекс.Браузера и браузера «Атом».

ВНИМАНИЕ! При подозрении на компрометацию вашего устройства с которого осуществляется доступ, аутентификационных данных (логин/пароль) или фактах несанкционированного движения финансовых средств необходимо незамедлительно сообщить всю информацию на адрес электронной почты post@gutains.ru.