Приложение № 1
к «Регламенту обеспечения защиты
информации в целях противодействия
осуществлению незаконных
финансовых операций»

РЕКОМЕНДАЦИИ

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 используйте 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, особую опасность могут представлять файлы со следующими расширениями:

***ade, *adp, *bas, *bat;*chm, *cmd, *com, *cpl;*crt, *eml, *exe, *hlp;**

***hta, *inf, *ins, *isp; *jse,*lnk, *mdb, *mde; *msc,*msi, *msp, *mst; *pcd,**

***pif, *reg, *scr; *sct,*shs, *url, *vbs; *vbe,*wsf, *wsh, *wsc;**

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 прочие отчуждаемые носители информации.) 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 обеспечение из недостоверных или сомнительных источников. Как правило, оно 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 удаления 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 Страховщика, позвонив по телефону +7 (495)980-98-50.

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. 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.

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

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.

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.

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 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 действующего актуального антивирусного программного обеспечения с актуальными вирусными базами;

• несоблюдение Вами настоящих рекомендаций.

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.