Утверждено:
Генеральный директор АО «Управляющая компания «Система Профит»
И.Г. Кирия
28 июня 2019 г.

Рекомендации клиентам Акционерного общества «Управляющая компания «Система Профит» по защите информации в целях противодействия незаконным финансовым операциям

Екатеринбург

1. Общие положения

Акционерное общество «Управляющая компания «Система-Профит» настоящим доводит до сведения Клиентов рекомендации по защите информации от воздействия программных кодов, о возможных рисках получения несанкционированного доступа к защищаемой информации лицами, не обладающими правом их осуществления, о мерах по предотвращению несанкционированного доступа к защищаемой информации, в от числе при у трате (хищении, потере) 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 вредоносного кода.

Кража учетных данных – это хищение личных данных Клиента Акционерного общества «Управляющая компания «Система Профит» (далее - Управляющая компания) и их незаконное использование для выполнения несанкционированных операций от имени Клиента. Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий для предотвращения таких ситуаций. При этом необходимо использовать комплексный подход, а вопросам информационной безопасности уделять достаточное внимание, как на стороне Брокера, так и на стороне Клиента.

2. Рекомендации по защите информации от воздействия вредоносного кода (вредоносная программа)

2.1 Вредоносная программа – это программа, наносящая вред мобильному устройству/компьютеру или иному устройству, на которых она запускается. Вредоносные программы способны самостоятельно (то есть без ведома владельца устройства), создавать свои копии и распространять их различными способами, что может привести к полному разрушению информации, хранящейся на устройстве, а также хищению личных данных Клиента.

2.2 При наличии технической возможности на персональном компьютере Клиента должно быть установлено ПО, которое должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политики безопасности, то есть не требующий ответов пользователя при обнаружении вирусов. Лечение и удаления вирусов должно производиться в автоматическом режиме.

2.3 Не реже одного раза в неделю в автоматическом режиме должна производиться полная проверка жесткого диска персонального компьютера либо другого устройства, с использованием которого Клиентом совершались действия в целях осуществления финансовой операции на предмет наличия вирусов и вредоносного программного кода. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по средствам телекоммуникационным каналам, а также информацию на съемных носителях. При наличии технической возможности сканирование должно производиться в автоматическом режиме.

2.4 Рекомендуется не использовать компьютер, с которого Клиент осуществляет операции с денежными средствами и иными активами, для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания, так как именно через эти ресурсы сети Интернет чаще всего распространяют вредоносные программы.

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

3.1 Рекомендуется не вводить конфиденциальную информацию на поддельных или небезопасных web – сайтах, которые зачастую являются почти точной копией web – сайтов известных компаний, которым ранее Клиент доверял.

3.2 Рекомендуется не отвечайте на подозрительные электронные письма с просьбой выслать пароль и другие конфиденциальные данные. Подобное письмо наверняка создано злоумышленниками.

3.3 Рекомендуется перед просмотром электронного письма проверять адрес отправителя, так как строка «отправитель» может содержать адрес электронной почты, который является почти точной копией адреса настоящей компании. Соблюдайте бдительность.

3.4 Рекомендуется обращать внимание на обезличенные обращения в электронном письме и помнить, что многие мошеннические письма содержат призывы к безотлагательным действиям (например, что счету угрожает опасность, если немедленно не обновиться важная информация) пытаясь заставить действовать быстро и необдуманно.

3.5 Рекомендуется внимательно анализировать ссылки, так как они могут быть точной копией подлинных, однако перенаправлять на мошеннический web-сайт.

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программы файлы, полученные из ненадежных источников, скаченные с неизвестных web-сайтов, присланные по электронной почте и полученные из иных источников. Подозрительные файлы лучше немедленно удалять.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1 Рекомендуется регулярно производить смену паролей для работы со своими учетными данными, использовать различные уникальные пароли для различных web-сайтов и систем.

4.2 В случае обнаружения того, что пароль скомпрометирован, рекомендуется незамедлительно сменить пароль на новый, а если Клиент в работе столкнулся с тем, что действующий пароль не срабатывает и не позволяет войти в личный кабинет, то необходимо как можно быстрее обратиться с сотруднику Управляющей компании для получения инструкции по смене паролей.

4.3 Рекомендуется исключить возможность физического доступа к компьютеру с которого Клиент осуществляет работу в системе посторонних лиц.

4.4 Необходимо незамедлительно обратиться к сотруднику Управляющей компании в случае, если получили уведомление системы об операции, которую не совершали.

4.5 При утере или хищения устройства клиента, с которого осуществлялся вход в личный кабинеты некредитных финансовых организаций для осуществления финансовых операций, необходимо обратиться в указанные организации для блокировки личного кабинета с указанием причины осуществления такой блокировки.