УТВЕРЖДАЮ
Генеральный директор
ООО «Москва Сити Секьюритиз»

_____ /Куринов Н.Б./
«31» мая 2019 года

Рекомендации клиентам Общества с ограниченной ответственностью «Москва Сити Секьюритиз» по защите информации в целях противодействия незаконным финансовым операциям

(вступает в силу «01» июня 2019 года)

Москва

1. Общие положения

1.1 Кража учетных данных – хищение личных данных Клиента Общества с ограниченной ответственностью «Москва Сити Секьюритиз» (далее – Общество) 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.

1.2 Задачи защиты информации сводятся к минимизации ущерба и предотвращению злонамеренных воздействий. Для обеспечения надлежащей степени защищенности необходимо использование комплексного подхода, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Общества, так и на стороне Клиента.

1.3 Риски получения несанкционированного доступа к информации связаны с:

- «фишингом» (использованием ложных ресурсов сети Интернет с целью осуществления финансовых операций лицами, не обладающими правом их осуществления);
- воздействием вредоносного кода.

1.4 Фишинг – попытка перехвата личных данных Клиента. Один из самых распространенных способов фишинга заключается в отправке электронных писем от мошенников, которые выдают себя за представителей известной компании. Как правило, в электронных письмах от мошенников содержится ссылка на небезопасную страницу web-сайта. На этой странице лицу обычно предлагается ввести персональные данные. При этом Клиент может полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

1.5 Антивирусная защита осуществляется с целью исключения возможностей появления на персональных компьютерах, с которых осуществляется работа с системой, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения (далее – ПО), либо на перехват информации, в том числе паролей.

1.6 Средства и методы защиты информации, применяемые у Общества, позволяют обеспечить необходимый уровень безопасности при осуществлении операций с денежными средствами и иными активами и предотвратить мошеннические операции по счетам Клиентов при условии выполнения Клиентами рекомендаций, изложенных в данном документе.

2. Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код)

2.1 При наличии технической возможности на персональном компьютере Клиента должно быть установлено антивирусное ПО.

2.2 Антивирусное ПО должно регулярно обновляться. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т. е. не требующий ответов пользователя при обнаружении вирусов. Лечение (удаление) зараженных файлов должно производится антивирусным средством 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 осуществляется согласно расписанию, выставленному в настройках антивирусного средства.

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 использовании сети Интернет для обмена почтовыми сообщениями необходимо применять антивирусное ПО, разработанное специально для почтовых клиентов.

2.6 При возникновении подозрения на наличие компьютерного вируса (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.) рекомендуется приостановить работу с системой до полного устранения неисправностей.

2.7 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 (игровые сайты, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.

2.8 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, на котором пользователю под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов

известных компаний, которым пользователь доверяет, и предназначены для сбора конфиденциальной информации обманным путем.

3.2 Рекомендуется перед просмотром электронного письма всегда проверять адрес отправителя. Строка «Отправитель» может содержать адрес электронной почты в официальном формате, который является почти точной копией адреса настоящей компании. Необходимо соблюдать бдительность, так как изменить адрес электронной почты отправителя очень просто.

3.3 Необходимо внимательно читать текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если в письме содержаться слова на иностранном языке, специальные символы и т. д., возможно, это электронное письмо отправлено мошенниками.

3.4 Необходимо обращать внимание на обезличенные обращения в электронном письме, такие как «Уважаемый пользователь», или обращения по адресу электронной почты. Необходимо помнить, что типичное фишинговое письмо начинается с обезличенного приветствия. В электронном письме, направленном Обществом в адрес Клиента, будет персонифицированное обращение, в том числе по имени и отчеству Клиента/представителя Клиента, либо в случаях массовой рассылки уведомлений или разного рода информационных сообщений типовое обращение от лица Общества будет иметь следующий вид:

«Уважаемый Клиент ФИО полностью!

[текст сообщения]

С уважением,
ООО «Москва Сити Секьюритиз»

3.5 Необходимо помнить, что многие мошеннические электронные письма содержат призывы к безотлагательным действиям, пытаясь заставить лицо действовать быстро и необдуманно. Многие поддельные сообщения электронной почты пытаются убедить лицо в том, что его счету угрожает опасность, если немедленно не обновить критически важные данные. При получении подобных сообщений рекомендуется не предпринимать никаких действий, указанных в сообщении, а незамедлительно связаться с сотрудниками Общества.

3.6 Необходимо внимательно анализировать ссылки. Ссылки могут быть почти точной копией подлинных, однако они могут перенаправить на мошеннический web-сайт. Если

ссылка выглядит подозрительно или не соответствует требованиям безопасности (например, начинается с http:// вместо https://), не следует переходить по этой ссылке.

4. Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

4.1 Рекомендуется регулярно производить смену пароля для работы со своими учетными данными. Пароль должен соответствовать требованиям к сложности: длина пароля должна быть не менее 8 символов и представлять собой сложное сочетание строчных и прописных букв, цифр и символов.

4.2 Рекомендуется хранить ключевую информацию на отчуждаемом носителе (USB-накопителе), который рекомендуется хранить в сейфе или запираемом шкафу, исключив возможность несанкционированного доступа.

4.3 Рекомендуется использовать различные уникальные пароли для различных web-сайтов и систем, использование которых предполагает введение конфиденциальных данных.

4.4 В случае обнаружения того, что пароль скомпрометирован, рекомендуется незамедлительно сменить пароль на новый, удовлетворяющий требованиям п. 4.1.

4.5 Если в процессе работы Клиент столкнулся с тем, что ранее действующий пароль не срабатывает и не позволяет войти в Личный кабинет, необходимо как можно быстрее обратиться к сотрудникам Общества для получения инструкций по смене пароля.

4.6 Информация о логинах, паролях и кодах доступа является конфиденциальной и не подлежит раскрытию третьим лицам. Общество не рассылает электронных писем, SMS или других сообщений с просьбой уточнить конфиденциальные данные Клиента (в т.ч. пароли и т.п.).

4.7 Рекомендуется не пересылать файлы с конфиденциальной информацией для работы в Личном кабинете по электронной почте или через SMS-сообщения.

4.8 Рекомендуется исключить возможность физического доступа к компьютеру, с которого Клиент осуществляете работу в системе, посторонних лиц.

4.9 Необходимо незамедлительно обращаться к Обществу в том случае, если Клиент получил уведомление системы об операции, которую не совершал.