Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать транзакции от лица клиента

Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц,

ООО "УК "АБСОЛЮТ Эссет Менеджмент" (далее – Общество) в рамках соблюдения требований 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 20.04.2021 №757-П) уведомляет клиентов Общества о возможных рисках несанкционированного доступа к защищаемой информации:

1. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риски разглашения информации конфиденциального характера: сведений об операциях, активах, состоянию лицевых счетов, персональных данных, иной значимой информации.

2. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риски совершения юридически значимых действий, включая: совершение операций с доступными активами, внесение изменений в регистрационные данные клиента, использование счетов и находящихся на них активов для прикрытия иных действий, носящих противоправный характер, совершения иных действий против воли клиента.

3. **Несанкционированный доступ со стороны третьих лиц** может повлечь за собой риск деструктивного воздействия на носители информации и их содержимое, что в свою очередь может привести к воспрепятствованию своевременного исполнения своих обязательств или невозможности использования сервисов компании для реализации своих намерений.

4. **Вредоносные программы** способны самостоятельно, то есть без ведома клиента создавать свои копии и распространять их различными способами.

II. Рекомендации по защите информации от противоправного доступа

1. Не сообщайте посторонним лицам персональные данные или информацию через Интернет, включая логины и пароли доступа к клиентским ресурсам Общества, историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к вашим активам.

2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

3. Не используйте функцию запоминания логина и пароля в браузерах.

4. Не используйте одинаковые логин и пароль для доступа к различным системам.

5. Не пользуйтесь системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых вы не уверены. По возможности совершайте операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и (или) информации о доступе к клиентским ресурсам Общества.

6. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу). После возвращения к своему средству доступа обязательно смените логин и пароль.

7. Не открывайте ссылки, указанные в сомнительном письме, в котором вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

8. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные.

9. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

10. При использовании ЭП не позволяйте третьим лицам производить за вас генерацию ключей.

11. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что за пользование нелицензированным программным обеспечением предусмотрена уголовная ответственность в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на ваш компьютер.

12. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения и обновляйте антивирусные базы. В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.

13. Не запускайте на своем компьютере программы, полученные из незаслуживающего доверия источника.

14. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

15. Не храните незашифрованные личные данные на жестком диске, так как эти данные могут быть похищены злоумышленниками и использованы для получения доступа к вашим активам.

16. Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с вами можно было оперативно связаться.

17. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

18. Для обеспечения конфиденциальности операций пользуйте только защищенное соединение через HTTPS. Защищенное соединение предотвращает перехват или фальсификацию передаваемых данных.

19. В случае утраты устройства необходимо изменить пароли доступа к ресурсам, на которые производился вход.

III. Рекомендации по защите информации от воздействия вредоносного кода

1. Вредоносные программы

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» до полного разрушения информации, хранящейся на дисках компьютера.

2. Антивирусные программы ваши первые защитники

Антивирусные программы – основное средство борьбы с вредоносными программами. Установите современное лицензионное антивирусное программное обеспечение, осуществляющее постоянный контроль за компьютером и мобильным устройством. Периодически запускайте полную проверку компьютера. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

3. Обновления - это полезно и безопасно

Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

4. Проверяйте новые файлы

Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращайте внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио и видео файлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов. Подозрительные сообщения лучше немедленно удалять. При открытии ссылок, полученных по электронной почте, скопируйте ссылку, вставьте в адресную строку используемого браузера и убедитесь, что адрес соответствует интересующему вас ресурсу. Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте компьютер полностью.

5. Будьте бдительны и осторожны

По возможности не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их. При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой. При использовании браузера не переходите по ссылке и не нажимайте на кнопки во всплывающих окнах. Старайтесь избегать сайтов, которые могут иметь незаконное и/или вредоносное содержание. Проверяйте все съемные носители информации (USB-Flash, CD/DVD-диски, карты памяти SD и т.п.) до начала их использования. Избегайте использования привилегированных учетных записей (например, Администратор) для ежедневного использования. Для выполнения большинства операций достаточно прав обычного пользователя. Периодически удаляйте программное обеспечение, которое больше не нужно.

6. Резервное копирование гарантия безопасности

Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

7. Тактика борьбы с вредоносными программами

Вредоносные программы представляют собой файлы, которые срабатывают при активировании на компьютере. Тактика борьбы с ними достаточно проста:

а) не допускать, чтобы вредоносные программы попадали на ваш компьютер;

б) если они к вам все-таки попали, ни в коем случае не запускать их;

в) если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба. Самый действенный способ оградить от вредоносных программ свой почтовый ящик – запретить прием сообщений, содержащих исполняемые вложения.

8. Расширение файла – это важно (!)

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. Помните, что в сети Интернет действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы. Если ваш компьютер или мобильное устройство подверглось заражению, рекомендуется обратиться к квалифицированным специалистам, а также сменить пароли от доступа в кабинет, электронной почты, учетных записей в социальных сетях и т.п. с помощью не зараженного устройства.