Рекомендации для клиентов по защите информации от воздействия вредоносных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, в целях противодействия незаконным финансовым операциям

В целях выполнения требований п. 1.13 Положения Банка России от 20.04.2021 № 757-П «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», ООО «СД «Депо-Плаза» доводит до своих клиентов информацию о рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, утечки персональных данных и иной защищаемой информации,

К защищаемой информации относится следующая информация:
• информация, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками ООО «СД «Депо-Плаза» и (или) клиентами ООО «СД «Депо-Плаза»;
• информация, необходимая ООО «СД«Депо-Плаза» для авторизации клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
• информации об осуществленных ООО «СД «Депо-Плаза» и его клиентами финансовых операциях;
• ключевая информация средств криптографической защиты информации, используемая ООО «СД «Депо-Плаза» и его клиентами при осуществлении финансовых операций.

В целях обеспечения защиты информации и носителей этой информации от использования ее злоумышленниками и предотвращения воздействия вредоносного кода рекомендуется клиентам соблюдать ряд следующих мер:

1. Обеспечение безопасности компьютера:

1.1. пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением, обеспечивающим защиту устройства от вредоносного кода (антивирусных программных комплексов);
1.2. своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений). Но помните, что ни одна антивирусная программа не обеспечивает 100% защиты.
1.3. антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.
1.4. ограничение доступа к компьютеру посторонних лиц;
1.5. по возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации;
1.6. организация надлежащего контроля за устройствами, с использованием которых совершаются действия в целях осуществления финансовых операций;
1.7. ограничение возможности инсталляции в память устройств программ и компонентов, полученных из ненадежных источников. Не запускать на своем компьютере программы, полученные из незаслуживающих доверия источников;
1.8. обеспечение сохранности и секретности аутентификационных данных для входа в информационные системы, а также ключей электронной подписи;
1.9. не использовать и не устанавливать программы для удаленного доступа к компьютеру (Radmin, TeamViewer, AmmyAdmin и т.п.). Удаленный доступ к компьютеру с использованием таких программ позволит злоумышленнику получить доступ к ключам электронной подписи, подключенным к данному компьютеру, и осуществить таким образом несанкционированные операции;
1.10. оперативное уведомление сотрудников ООО «СД «Депо-Плаза» об утрате (хищении) ключевых носителей и иных случаях компрометации ключей электронной подписи.

1.11. при подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования системы дистанционного банковского обслуживания и проведения платежей с помощью банковских платежных карт до исправления ситуации;

1.12. в случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, утраты (потери, хищения) устройства, с использованием которого осуществлялись финансовые операции, подать заявление на временное отключение от платежной системы, подать заявление о данном факте в правоохранительные органы и прекратить использование (обесточить) персонального компьютера и иных средств доступа в целях сохранения доказательной базы.

2. Пароли:

2.1. использование надежных паролей, содержащих не менее 8 различных символов (сочетание букв/цифр, большого/малого регистра). Регулярно производить смену паролей;

2.2. не сообщать посторонним лицам персональные данные или информацию о банковских картах (счетах) через сеть Интернет, логины и пароли доступов, историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к Вашей защищаемой информации;

2.3. не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции;

2.4. не использовать функцию запоминания логина и пароля в браузерах для используемых платежных систем;

2.5. не использовать одинаковые логин и пароль для доступа к различным системам;

2.6. в случае обнаружения подозрительных действий, совершенных от Вашего имени, незамедлительно сменить логин и пароль.

3. Безопасное использование информационно-телекоммуникационной сети Интернет:

3.1. при регистрации на сторонних интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте;

3.2. не передавать никакой персональной и иной конфиденциальной информации при получении писем по электронной почте от якобы представителей банков и иных финансовых организаций, если получение таких писем инициировано не Вами;

3.3. не переходить по ссылкам в таких письмах, не открывать вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение);

3.4. не звонить по телефонам, указанным в подобных письмах, и не отвечать на них. Для связи использовать номера телефонов и электронные адреса, указанные на официальных сайтах владельцев финансовых сервисов;

3.5. запрет на использование открытых общедоступных сетей Wi-Fi;

3.6. запрет запуска файлов, загруженных с ненадежных интернет-сайтов и полученных от неизвестных адресатов (в том числе, посредством электронной почты);

3.7. при входе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет;

3.8. воздерживайтесь от использования программ онлайнового общения на компьютере, используемом для работы в системе дистанционного банковского обслуживания;

3.9. исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ;

3.10. рекомендуем ограничить информационный обмен в сети Интернет только с надёжными информационными порталами и проверенными корреспондентами электронной почты;

3.11. важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто, в виде «интересной ссылки» в письме, от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.