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

В целях выполнения требований Положения Банка России от 17.04.2019 № 684-П «Об установлении обязательных 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, о мерах соблюдения информационной безопасности и способах пресечения хищения:

В целях обеспечения защиты информации и носителей этой информации от использования ее злоумышленниками и предотвращения возможных негативных последствий вследствие реализации указанных рисков, рекомендуется:

- 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.
- Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции.
- Не использовать функцию запоминания логина и пароля в браузерах для используемых платежных систем.
- Не использовать одинаковые логин и пароль для доступа к различным системам.
- Регулярно производить смену паролей. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат.
- По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.
- Завершать сеанс работы с платежными системами, используя соответствующий пункт меню (например, «Выйти»).
- При выполнении операций в платежных системах с использованием чужих компьютеров или иных средств доступа не сохранять на них персональные данные и другую информацию, а после завершения всех операций убедиться, что персональные данные и другая информация не сохранились.
- 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. Не переходить по ссылкам в таких письмах, не открывать вложенные приложения (такие ресурсы могут содержать вредоносное программное обеспечение). 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.
- При регистрации на сторонних интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте.
- Не запускать на своем компьютере программы, полученные из незаслуживающих доверия источников.
- Использовать антивирусное программное обеспечение и межсетевые экраны.
- Регулярно производить обновление системных и прикладных программных средств.
- В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно сменить логин и пароль и сообщить об инциденте информационной безопасности в Службу технической поддержки Банка или платежного сервиса.
- 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.

Рекомендации по защите информации от воздействия вредоносного кода.

- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

- Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
- Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что ни одна антивирусная программа не обеспечивает 100% защиты.
- 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.
- При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.
- При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ.
- Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.
- Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.
- Рекомендуем ограничить информационный обмен в сети Интернет только с надёжными информационными порталами и проверенными корреспондентами электронной почты.
- 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.
- 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.