ЦЕНТРОФИНАНС
МИКРОФИНАНСИРОВАНИЕ

УТВЕРЖДАЮ
Генеральный директор
ООО МФК «Центрофинанс Север»
_____ Д.Н. Старшов
01 июня 2019 года

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ ПРОГРАММНЫХ КОДОВ, ПРИВОДЯЩИХ К НАРУШЕНИЮ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

Настоящим в целях противодействия незаконным финансовым операциям, во исполнении Положения Банка России № 684-П от 17.04.2019 года ООО МФК «Центрофинанс Север» доводит до сведения Клиентов рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код).

При использовании Клиентом дистанционного финансового обслуживания (личный кабинет) несоблюдение настоящих рекомендаций ООО МФК «Центрофинанс Север» может привести к рискам получения несанкционированного доступа (далее-НСД) к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, утечки персональных данных и иной защищаемой информации.

В целях предотвращения возможных негативных последствий вследствие реализации таких рисков рекомендуется:

1. 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 с помощью вредоносных программ[1] Злоумышленниками и использованы для получения доступа к Вашей защищаемой информации.
2. Не записывать логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции.
3. Не использовать функцию запоминания логина и пароля в браузерах для используемых платежных систем.
4. Не использовать одинаковые логин и пароль для доступа к различным системам.
5. 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.
6. Установить 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. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер,

---

[1] Вредоносные программы - любое программное обеспечение, предназначенное для получения несанкционированного доступа к ресурсам мобильного устройства/компьютера или к хранимой на них информации, с целью несанкционированного использования ресурсов или причинения вреда (нанесения ущерба) владельцу информации, путём копирования, искажения, удаления или подмены информации. Вредоносные программы способны самостоятельно (без ведома владельца устройства) создавать копии и распространять их различными способами, что приводит к полному разрушению информации, хранящейся на устройстве.

почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

7. По возможности совершать операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных и иной защищаемой информации.

8. Завершать сеанс работы с платежными системами, используя соответствующий пункт меню (например, «Выйти»).

9. 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.

10. 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. Будьте очень осторожны при получении сообщений с файлами-вложениями. Обращать внимание на расширение файла. Вредоносные файлы часто маскируются под обычные графические, аудио и видео файлы. Для того, чтобы видеть настоящее расширение файла, обязательно включать 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 устанавливать и не сохранять 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 удалить. Проверять все новые файлы, сохраняемые на компьютере. Периодически проверять компьютер полностью.

11. При регистрации на сторонних интернет-сайтах всегда изменять пароли, которые приходят Вам по электронной почте. При использовании браузера не переходить по ссылке и не нажимать на кнопки во всплывающих окнах. Избегать открытие сайтов, которые могут иметь незаконное и/или вредоносное содержание.

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

а) не допускать, чтобы вредоносные программы попадали на Ваш компьютер/мобильное устройство;

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.

13. 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.

14. В случае обнаружения подозрительных действий, совершенных от Вашего имени в личном кабинете, незамедлительно сменить логин и пароль и сообщить об инциденте в Службу технической поддержки Компании по телефону **8 800 222-94-24** или по электронной почте **support@lovizaim.ru**

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

16. Регулярно выполнять резервное копирование важной информации. В случае подозрения на заражение компьютера вредоносной программой, необходимо загрузить операционную систему с диска и проверить антивирусную программу.

17. При утере или хищении Вашего устройства, с которого осуществлялся вход в личные кабинеты некредитных финансовых организаций для осуществления финансовых операций, необходимо

обратиться в указанные организации для блокировки личного кабинета с указанием причины осуществления такой блокировки.

Дополнительно сообщаем, что настоящие Рекомендации носят диспозитивный информационный характер и призваны донести до сведения Клиентов:

- Информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом на осуществление таких операций;

- Информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) 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.