ООО МКК «КапиталЪ-НТ»
ИНН 6623106990 КПП 631201001
ОГРН 1146623008707
Регистрационный номер записи в государственном реестре микрофинансовых организаций
001603465007766
443095, г. Самара, Стара-Загора, д. 202А, офис 301
Телефон 8 800 222 42 20 E-mail: info@belkacredit.ru

Рекомендации по защите информации в целях противодействия незаконным финансовым операциям

1. Общество с ограниченной ответственностью Микрокредитная компания «КапиталЪ-НТ» (Компания) в рамках соблюдения требований Положения Банка России от 17.04.2019 № 684-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» уведомляет своих клиентов, использующих автоматизированные системы для получения, подготовки, обработки, передачи и хранения информации в электронной форме о возможных рисках получения несанкционированного доступа к информации, с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции и необходимости защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники, своевременному обнаружению воздействия вредоносного кода. Для целей настоящих Рекомендаций под средствами вычислительной техники Компания понимает совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
2. Настоящие Рекомендации размещаются на официальном сайте Компании https://belkacredit.ru/
3. К причинам возникновения возможных рисков получения несанкционированного доступа к информации Компания относит:
    - Утрата (потеря, хищение) клиентом устройств вычислительной техники и карт памяти.
    - Отсутствие надлежащего программного обеспечения.
    - Отсутствие качественной антивирусной программной защиты.
    - Несоблюдение клиентом настоящих Рекомендаций.
    - Неограниченный доступ третьих лиц к средствам вычислительной техники.
    - Неограниченный доступ третьих лиц к информации о логинах и паролях, использующихсяпри работе с информационными ресурсами.
    - Несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет».

    Настоящий перечень причин возникновения рисков получения несанкционированного доступа к информации не является исчерпывающим.

4. В целях предотвращения несанкционированного доступа к информации и нарушения штатного функционирования средств вычислительной техники Компания рекомендует следующие меры защиты:

Для защиты мобильных устройств:

- своевременно устанавливать обновления безопасности операционной системы;
- при наличии технической возможности включить шифрование данных;
- не отключать и не взламывать встроенные механизмы безопасности;
- сохранять в тайне имя пользователя (логин), пароль для доступа в информационные системы, SMS-коды;
- защищать паролями учетные записи операционной системы;
- не хранить логин и пароль в мобильном телефоне, смартфоне, компьютере;
- регулярно обновлять пароли;
- не использовать одинаковые логин и пароль для доступа к различным системам;
- длина пароля должна быть не менее 8 символов;
- включать в пароль заглавные и прописные символы, цифры, а также специальные символы;
- не использовать функцию запоминания логина и пароля;
- не использовать в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
- не произносить вслух, не записывать и не хранить в любом доступном посторонним лицам месте пароли.

Для защиты персональных компьютеров:

- использовать исключительно лицензионное системное и прикладное программное обеспечение;
- установить на компьютер только одну операционную систему;
- не устанавливать и не использовать на компьютере программы для удаленного управления;
- установить и регулярно обновлять лицензионные антивирусные программы;
- своевременно проводить обновление системного и прикладного программного обеспечения;
- не использовать общедоступные компьютеры и публичные беспроводные сети для доступа к информационным системам;
- при передаче информации с использованием чужих компьютеров, после завершения всех операций убедиться, что персональные данные и другая информация не сохранились;
- не передавать персональные данные и иную конфиденциальную информацию при получении писем по электронной почте, 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);
- в случае обнаружения подозрительных действий, совершенных в компьютере, незамедлительно сменить логин и пароль;
- при обнаружении совершения незаконных финансовых операций – незамедлительно подать заявление о данном факте в правоохранительные органы и сохранить доказательства данного факта в устройстве;
- при работе с иными носителями информации перед началом работы осуществлять их проверку на предмет отсутствия компьютерных вирусов.

В целях защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники:

- обновлять антивирусныепрограммы на постоянной основе;
- осуществлять регулярный контроль работоспособности антивирусных программ;
- создать условия, при которых невозможно несанкционированное отключения средств антивирусной защиты;
- антивирусная защита должна обеспечивать сохранение безопасного состояния информации при любых сбоях;
- вынести ярлык для запуска антивирусной программы на рабочий стол персонального компьютера для ее регулярного использования.

5. Компания уделяет большое внимание безопасности Ваших данных, принимая все необходимые меры для их защиты и предупреждает своих клиентов о необходимости также проявлять осторожность, осведомленность и сознательность при обращении с информацией.