ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ЖЁЛУДЬ»
(Ломбард)
ИНН 5609194489 ОГРН 1205600003311 КПП 560901001
Адрес местонахождения: 460052, Оренбургская область, город Оренбург, улица Салмышская 39/1, офис 1

Рекомендации
по соблюдению защиты информации при использовании сети интернет

В соответствии с требованиями 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» Общество с ограниченной ответственностью «Жёлудь» (Ломбард) (далее по тексту - Общество) доводит до вашего сведения основные рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

При обмене информацией через сеть Интернет необходимо:
• Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
• Не вводить персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах (мошеннический или поддельный web-сайт – это небезопасный web-сайт, на котором Вам под каким-либо предлогом предлагается ввести конфиденциальную информацию. Зачастую эти web-сайты являются почти точной копией web-сайтов известных компаний, которым Вы доверяете, и предназначены для сбора конфиденциальной информации обманным путем);
• Ограничить посещения сайтов сомнительного содержания;
• Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ у третьих лиц;
• Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
• Не открывать файлы полученные (скачанные) из неизвестных источников.

При работе на компьютере необходимо:
• Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
• Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
• Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы (не реже одного раза в неделю в автоматическом режиме должна осуществляться полная проверка жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода. Проверка осуществляется согласно расписанию, выставленному в настройках антивирусного средства. Рекомендуется подвергать антивирусному контролю любую информацию, получаемую и передаваемую по

телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование должно осуществляться в автоматическом режиме.)

• Использовать специализированные программы для защиты информации, средства контроля конфигурации устройств;

• Использовать сложные пароли;

• Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам

При работе с Мобильного устройства необходимо:

• Не оставлять свое Мобильное устройство без присмотра, чтобы исключить его несанкционированное использование;

• Использовать только официальные Мобильные приложения;

• Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщений, Push-уведомлении или по электронной почте, в том числе от имени Общества;

• Установить на Мобильном устройстве пароль для доступа к устройству