Рекомендации организации клиентам по защите информации от рисков ее использования в незаконных финансовых операциях

В целях обеспечения защиты информации и ее носителей от ее использования злоумышленниками с целью совершения незаконных финансовых операций организация рекомендует клиентам следующие меры:

1.Установить и регулярно обновлять операционную систему, антивирусные программы, файрволы и другие средства защиты от вредоносных кодов и иных способов несанкционированного доступа;

2.Не раскрывать полученных по электронной почте провоцирующих сообщений и ссылок, не скачивать программное обеспечение с сомнительных сайтов;

3.Установить пароли доступа пользователя к хранящейся в персональном компьютере информации;

4.Установить блокировку доступа к хранящейся в персональном компьютере информации при попытках несанкционированного доступа;

5.В случае использования электронной почты для передачи электронных документов и иных содержащих важную финансовую информацию сообщений применять PGP-ключ, обеспечивающий высокий уровень защищенности передаваемых сообщений между клиентом и организацией

6.Не предоставлять персональные данные, а также паспорт, иные удостоверяющие личность и содержащие персональные данные документы в организацию для сканирования без получения ею письменного согласия клиента на обработку этих данных;

7.Обеспечить надежное хранение и недоступность логинов, паролей, кодов доступа и носителей этих сведений при использовании банковских карт, Личного кабинета в банке и иных организациях;

8.Немедленно блокировать банковский счет или Личный кабинет в организации в случае утраты или некорректной работы банковской карты, пароля, кода доступа, мобильного устройства или SIM-карты, иных средств дистанционного управления счетом, в том числе с помощью мобильного телефона

9.Создавать резервные копии защищаемой информации на мобильных носителях, не предусматривающие удаленного доступа к ним через Internet(флэшки, лазерные диски);

10.В случае обращения к клиенту по телефону лиц, представляющихся сотрудниками банка или иной обслуживающей организации, за информацией о паролях, кодах доступа, о персональных данных и иной важной информацией отказывать в предоставлении информации и немедленно связываться с банком или организацией, от имени которой действовали эти лица;