Народный Капитал

Юридический адрес:
РФ, 119002, г. Москва, пер. Серебряный, д. 5, пом.1
ИНН/КПП 7704489013/770401001
ОГРН: 1197746284405
Тел. (495)12-00-771, +7(927) 48-112-36
nkap.kpk@gmail.com

р/с 407 018 106 380 000 027 82
к/с 301 018 104 000 000 002 25
БИК 044525225
ПАО СБЕРБАНК

РЕКОМЕНДАЦИИ
по противодействию совершению незаконных финансовых операций

Настоящий документ предназначен для ознакомления пайщиков КПК «Народный капитал» с рекомендациями по предотвращению доступа злоумышленников к информации, которая может позволить им совершить незаконные финансовые операции от имени пайщиков.

Следует отметить, что использование пайщиками КПК «Народный капитал» технологий удаленного взаимодействия, позволяющих совершать финансовые операции без визита в офис Кооператива, несет с собой определенные риски, главным из указанных рисков является незаконное совершение злоумышленниками финансовых операций от имени пайщиков с целью хищения денежных средств.

Выполнение несложных рекомендаций, приведенных в настоящем документе, позволит пайщикам свести риск совершения незаконных финансовых операций от их имени к минимуму.

Рекомендации

При использовании мобильного телефона рекомендуется придерживаться следующих советов:

При взаимодействии с Кооперативом указывайте в качестве основного номера телефона номер, который принадлежит Вам лично (контракт на услуги сотовой связи, заключен на Ваше имя).

Устанавливайте мобильные приложения на телефонный аппарат, который принадлежит Вам и постоянно находится в Вашем распоряжении.

Включите запрос пин-кода SIM-карты при включении телефона.

При поддержке телефоном соответствующей функции, выполните следующие действия:

1. Включите блокирование экрана телефона после определенного времени неактивности.

2. Включите запрос пин-кода телефона, отпечатка пальца или графического ключа для разблокирования телефона.

3. Установите запрет на отображение информации из вновь поступивших сообщений на экране блокировки.

4. Включите и настройте функцию поиска, удаленного блокирования и удаленной очистки потерянного телефона.

5. Установите запрет на установку в телефон приложений из ненадежных источников.

При установке новых приложений на телефон обращайте внимание на запрашиваемые ими разрешения. Не давайте приложениям разрешение на чтение SMS, если такой доступ не нужен им для выполнения их основных функций.

Не переходите по ссылкам из SMS и сообщений, особенно если Вы не ждали такие сообщения.

Регулярно обновляйте операционную систему телефона и установленные в телефоне приложения (не отключайте автоматическое обновление).

В случае утраты телефона воспользуйтесь функцией поиска телефона, если ранее ее активировали. Если с использованием функции поиска найти телефон не удалось или Вы ранее не активировали эту функцию, обратитесь с паспортом в офис своего сотового оператора для блокирования утерянной вместе с телефоном SIM-карты и выпуска новой.

Дополнительно к действиям, указанным в предыдущем абзаце, рекомендуем проинформировать Кооператив об утере телефона.

Защита от вирусов

Вирусы – это программы для компьютеров или мобильных устройств, предназначенные для нанесения вреда. Функционал вирусов может быть разным: показ нежелательной рекламы, кража паролей (в том числе, из SMS-сообщений) и данных банковских карт, совершение незаконных финансовых операций от имени пайщика. Практически все вирусы имеют функцию собственного распространения или заражения всех доступных им устройств.

Во избежание заражения вирусами Вашего компьютера, следуйте таким советам:

1. Регулярно обновляйте операционную систему и установленные в ней приложения (включите автоматическое обновление).

2. Установите и регулярно обновляйте (не отключайте автоматическое обновление) антивирусную программу.

3. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.

4. Проверяйте антивирусной программой файлы, полученные из Интернета или со съемных носителей (флешек) до их использования.

Во избежание заражения вирусами Вашего мобильного устройства:

1. Регулярно обновляйте операционную систему и установленные в ней приложения (не отключайте автоматическое обновление).

2. Не открывайте файлы и не переходите по ссылкам, пришедшим в сообщениях электронной почты, служб мгновенных сообщений (Skype, WhatsApp, Viber и т.п.) и социальных сетей, которые Вы не ждете.

3. Установите запрет на установку в телефон приложений из ненадежных источников.