Рекомендации по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средств вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

ООО «Страховые брокеры «АСТ» рекомендует своим клиентам предпринимать следующие меры по защите информации от вредоносного кода, в целях противодействия незаконным финансовым операциям.

1. **Основные меры защиты мобильных и вычислительных устройств.**

   1.1. Использование официального ПО:

   - Загружайте мобильные приложения только из официальных магазинов и сайтов (App Store, Google Play, RuStore и др.).
   - Используйте только лицензионное программное обеспечение из доверенных источников.

   1.2. Контроль доступа:

   - Установите сложный пароль, PIN-код или используйте биометрическую аутентификацию для доступа к устройству.
   - Не оставляйте устройство без присмотра и не передавайте его третьим лицам.
   - Храните логины и пароли в тайне, не записывайте их в доступных местах.

   1.3. Целостность системы:

   - Не используйте устройства с нарушенными защитными механизмами производителя.
   - Регулярно устанавливайте обновления безопасности операционной системы и приложений.

2. **Безопасность при сетевом обмене и проведении операций**

   2.1. Антивирусная защита:

   - Установите и регулярно обновляйте антивирусное ПО.
   - Обеспечьте постоянную работу антивируса и не отключайте его при совершении платежей.

   2.2. Гигиена электронной почты и сообщений:

   - Не открывайте вложения и не переходите по ссылкам из писем от неизвестных отправителей.
   - Будьте осторожны с ссылками в SMS, MMS и мессенджерах.

   2.3. Использование публичных сетей:

   - Избегайте использования публичных (открытых) Wi-Fi сетей для доступа к банковским сервисам.
   - Предпочтительно использовать мобильный интернет (3G/4G) или защищенную домашнюю сеть.

   2.4. Проверка подлинности:

   - Всегда проверяйте URL-адрес сайта в адресной строке браузера перед вводом данных.

- Не вводите персональную или платежную информацию на подозрительных ресурсах.

3. Действия при подозрении на инцидент:

- При подозрении на компрометацию учетных данных (паролей, SMS-кодов) или несанкционированное движение средств немедленно свяжитесь со своим банком по официальным каналам для блокировки доступа и следования дальнейшим инструкциям.
- Смените пароли ко всем критическим сервисам с другого (заведомо чистого) устройства.