ПАМЯТКА:
«Профилактика преступлений, совершаемых с использованием информационно-коммуникационных технологий»

Наиболее типичные способы совершения преступлений с использованием современных технологий

1) Звонки гражданам от псевдо-сотрудников банков с просьбой сообщить данные банковских карт (три цифры на оборотной стороне банковской карты, пин-код карты и т.д.) для предотвращения несанкционированного списания денежных средств и иных целей, которые должны уберечь гражданина от мошенничества. В то время как после сообщения гражданином необходимых мошеннику сведений, с банковской карты ничего не подозревающего человека списываются денежные средства, либо граждане сами по просьбе мошенников переводят под различными предлогами денежные средства на указанные мошенниками счета.

2) Хищения денежных средств с использованием приложений «Авито», «Юла» и прочих приложений, с помощью которых возможно приобрести товар, бывший в употреблении, либо продать такой товар различного рода. Злоумышленники по телефону вводят граждан в заблуждение относительно своего намерения продать товар, в то же время узнают реквизиты банковской карты и списывают денежные средства, либо просят внести залог под предлогом того, что имеется покупатель, готовый приобрести указанный в объявлении товар прямо сейчас.

3) Рассылка СМС-сообщений с содержанием: «Ваша карта заблокирована. Для разблокировки необходимо сообщить по номеру».

4) Интернет-магазины, где предлагается товар с предоплатой, однако в дальнейшем гражданину почтой приходит иной товар либо не приходит вовсе.

5) Способ, при котором взламываются аккаунты в социальных сетях или электронная почта, откуда мошенниками рассылаются лицам, имеющимся в списке контактов, сообщения с просьбой о займе на различную сумму, после которых лица направляют на указанный мошенником счет деньги.

6) Рассылка СМС-сообщений о выигрыше, для получения которого необходимо пройти по указанной мошенником ссылке, либо позвонить по номеру телефона, где укажут, что для получения выигрыша нужно внести денежные средства.

Способы уберечь себя и близких от мошеннических действий с использованием информационно-коммуникационных технологий:

1) никому не сообщайте реквизиты своих банковских карт, у сотрудников банка они имеются. Тот, кто их спрашивает – мошенник!

2) Никогда не общайтесь по телефону с лицами, которые предлагают различные бонусы, выигрыши, скидки, бесплатные услуги и т.д., не

сообщайте им персональные данные, не переходите по незнакомым и подозрительным ссылкам в сети «Интернет».

3) Запрещайте доступ мобильных приложений к информации, хранящейся на Вашем телефоне.

4) Устанавливайте надежные пароли на аккаунты в социальных сетях и электронную почту, с определенной периодичностью меняйте пароли. Не устанавливайте пароли, содержащие данные, которые легко подобрать. Если вас заблокировали, немедленно после обнаружения сообщите всем об этом, после чего сразу смените пароль.

5) Установите настройки приватности для своего телефона и социальной сети.

6) Не покупайте товары с использованием приложений и не вносите залог, пока не посмотрите лично вживую указанные товары и не убедитесь в их качестве;

7) Внимательно читайте условия пользовательских соглашений приложений и онлайн-сервисов.

8) Не участвуйте в деятельности онлайн-казино и иных сервисов, предлагающих «легкие деньги» с минимальными вложениями.

9) Также возможно проверить Интернет-ресурс на официальном сайте Роскомнадзора в Едином реестре доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

10) Отвечать на телефонные звонки только по официальным номерам телефона банка.