ПАМЯТКА О ПРОФИЛАКТИКЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Наиболее типичные способы совершенияпреступлений с использованием современных технологий:

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;

Хищения денежных средств с использованием приложений-сервисов для продажи товаров, например: «Авито», «Юла» и прочих приложений. Злоумышленники по телефону вводят граждан в заблуждение относительно своего намерения продать товар, в то же время узнают реквизитыбанковской карты и списывают денежные средства;

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

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

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;

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.

Противодействовать мошенническим действиям с использованием икт можноследующими способами:

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

Никогда не общайтесь по телефону с лицами, которыепредлагают различные бонусы, выигрыши, скидки, бесплатные услуги и т.д., не сообщайте им персональные данные, не переходите по незнакомым и подозрительным ссылкам в сети «Интернет»;

Запрещайте доступ мобильных приложений к информации, хранящейся на Вашем телефоне;

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;

Внимательно читайте условия пользовательских соглашений приложений и онлайн-сервисов;

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

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;

Отвечать на телефонные звонки только по официальным номерам телефона банка.