**Как не стать жертвой мошенников в мире IT-технологий**

С развитием современных технологий кардинальным образом меняется жизнь нашего

общества, но несмотря на несомненные блага, которые несут своим развитием

 высокие технологии, имеются и негативные последствия такого прогресса.

Так, по данным статистической отчетности на территории Республики Хакасия

 в 2019 г. рост количества противоправных деяний, совершенных

с использованием информационно-телекоммуникационных технологий или

в сфере компьютерной информации, составил 37 %, всего зарегистрировано

таких преступлений 1412. Аналогичная тенденция наблюдается и

в текущем году - 36 %, с 209 до 285. Абсолютное большинство таких

преступлений составляют хищения денежных средств со счетов банковских карт.

Однако гражданам не стоит паниковать и снимать свои сбережения с пластиковых

карт, ведь банковский счет надежное место для хранения своих сбережений.

Одним из распространенных способов обмана является звонок потерпевшему

под видом работника службы безопасности банка (кредитного менеджера и т.д.)

о том, что с вашей карты пытались похитить денежные средства. После

таких слов доверчивый клиент самостоятельно сообщает реквизиты

своих банковских карт, включая код проверки подлинности карты

и пароли для подтверждения переводов денежных средств, которые приходят жертве

на мобильный телефон, привязанный к банковскому счету, затем денежные

средства пропадают со счетов доверчивого клиента в неизвестном направлении.

На самом деле это лишь один из способов обмана, фантазия злоумышленников

на данном направлении безгранична.

Однако не стать жертвой преступников довольно легко, достаточно запомнить

несколько простых признаков, по которым можно определить злоумышленников:

* звонки из банка о мошеннических действиях с вашими счетами

 (в таком случае банк просто их заблокирует, звонить в банк Вам придется

уже самостоятельно);

* попытки узнать реквизиты ваших банковских карт и счетов, тем более коды

 проверки подлинности карты (3 цифры на обороте карты), пин-коды и коды из

CMC оповещений банковских систем (все необходимые сведения настоящему работнику банка и так известны);

* попытки узнать какие-либо сведения о картах сторонних банков, которые имеются

 у Вас в наличии.

Еще один способ совершения таких преступлений - так называемые «фейковые»

магазины или объявления в сети «Интернет». Гражданам предлагается ознакомиться

с некоторыми рекомендациями при совершении таких покупок:

* пользоваться услугами проверенных интернет магазинов, с хорошим рейтингом,

 большим количеством положительных отзывов, продолжительным периодом работы;

* отдавать предпочтение магазинам, которые указывают свои реквизиты

в том числе адрес, который можно проверить через справочно-навигационные системы;

* выбирать магазины с подробным описанием товара и его фотографиями;
* обращать внимание на цену, безусловно, в интернет магазине товар может быть

 дешевле, чем в розничных магазинах Вашего места жительства, однако не стоит

 обманываться, цена на товар на 20 % и более ниже среднерыночной должны Вас

насторожить;

* покупая товар у частных лиц по интернет объявлениям обращать внимание

 на рейтинг продавца и ранее проданные им товары. Просить подробное фото товара,

с целью убедиться хотя бы в том, что товар у продавца действительно в наличии.

Следуя этим простым рекомендациям, Вы сможете полноценно пользоваться всеми

удобствами, которые несут современные технологии и обезопасить себя от потери

 своих денежных средств.

Пресс-служба прокуратуры Республики Хакасия (09.04.2020)