Профилактика дистанционных хищений

Сотрудники полиции г. Макарьев напоминают жителям о необходимости проявлять бдительность при общении с малознакомыми людьми.

В последнее время большое распространение получили кражи и мошенничества, совершаемые дистанционными способами, то есть с помощью мобильной связи и сети «интернет».

Чтобы не стать жертвой преступления, необходимо следовать простым рекомендациям: никому не сообщайте PIN-код и CVV2-код карты (трехзначное число с обратной стороны), срок её действия и персональные данные владельца. Сотрудники банка не спрашивают данную информацию по сотовой связи; не при каких условиях не сообщайте кому-либо пароль от «Сбербанк онлайн»; не покупайте вещи и предметы на незнакомых сайтах; при звонках о родственниках, якобы попавших в сложную ситуацию, не паникуйте, прекратите разговор и сами им перезвоните. необходимо с ними поддерживать связь, разъясняя им, чтобы не впускали в дом незнакомцев, и при каких либо сомнениях звонили своим родственникам.

Интернет-мошенничество - памятка для граждан.

СИТУАЦИЯ 1.

Вы получили смс-сообщение о том, что ваша банковская карта заблокирована?

Никогда не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.

Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.

СИТУАЦИЯ 2.

Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

Никогда не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.

Помните о том, что интернет-магазин не может принимать оплатуза покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.

СИТУАЦИЯ 3.

Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

Никогда не отправляйте деньги незнакомым лицам на их электронные счета.

Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.

СИТУАЦИЯ 4.

Вы решили продать товар и после подачи объявления в ближайшие дни Вам звонит желанный покупатель и говорить что готов оплатить сразу всю сумму за товар, но ему необходимо узнать номер Вашей карты и пароли, которые поступят в смс-сообщении или другие данные с карты?

Никогда никому не сообщайте номер Вашей карты, пароли из смс-сообщений и другие реквизиты карты, иначе с Вашей карты похитят денежные средства. Для перевода денежных средств Вам, покупателю достаточно знать один номер Вашей карты и больше никакие сведения не требуются. Также можно предложить способ оплаты, через платежные переводы в банках на Ваше ФИО, тогда у Вас похитит денежные средства будет невозможно!

СИТУАЦИЯ 5.

Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы?

Никогда не переходите по ссылке, указанной в сообщении.

Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.

СИТУАЦИЯ 6.

Общаетесь в интернете и имеете аккаунты в соцсетях? К Вам обратился знакомый с просьбой одолжить ему денежные средства? Никогда не переводите деньги не связавшись с другом по телефону и не выяснив причину его просьбы, даже если в сообщении он пишет, что не может говорить.

Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.

Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно.

Помните о том, что видео и аудиотрансляции, равно как и логин вашей сетевой переписки, могут быть сохранены злоумышленниками и в последствии использованы в противоправных целях.

СИТУАЦИЯ 7.

Вам позвонили на телефон (сотовый или городской) под видом родственника и сказали, что попали в ДТП, в полицию и просят за решение вопроса перечислить денежные средства на карты, телефоны и др. счета?

Помните, что прежде чем расстаться с деньгами, необходимо связаться с родственником под видом, которого звонят злоумышленники и убедиться что с ним все в порядке. Также можно задать контрольный вопрос якобы родственнику (дата рождения, имя матери, адрес проживания) и злоумышленник сам закончит разговор.

Уголовный розыск МО МВД России «Макарьевский»