11. Новодеревеньковская межрайонная прокуратура разъясняет – О профилактике правонарушений, совершаемых с использованием информационно-телекоммуникационных технологий

В настоящее время всё актуальнее становятся вопросы предупреждения правонарушений, связанных с хищением, совершенном с использованием современных информационно-коммуникационных технологий. Данный вид хищения является общественно опасным деянием, причиняющий имущественный вред гражданам и разрушающий нравственные устои общества.

На территории Орловской области имеют значительный рост преступления, связанные с хищением денежных средств у физических и юридических лиц из банков и иных кредитных организаций, совершаемых с использованием информационно-коммуникационных технологий в сети «Интернет», с помощью средств сотовой связи.

Мошенники используют разные способы обмана людей в интернете от спама до создания сайтов-двойников. Цель злоумышленников - получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных об их банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками.

Анализ способов совершения преступлений с использованием информационно-телекоммуникационных технологий показал, что в основном распространенно используются 3 схемы:

- схема - злоумышленник звонит или отправляет СМС-сообщение на телефоны, сообщая, что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника;
- схема - поступает звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет злоумышленника;
- схема - потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ.

С целью пресечения совершения преступления, необходимо критически относиться к таким сообщениям и не выполнять просьбы.

При возникновении подобной ситуации необходимо самостоятельно связаться с оператором банка, сотовой связи и узнать о совершении блокировки карты, номера телефона, отключении услуг и т.д. Данные действия поспособствуют незамедлительному установлению злоумышленника и пресечению совершения преступления.

Помните, что ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код!

Признаки потенциально опасных Интернет-магазинов или объявлений:

- Требование предоплаты. Помните, что большей части случает при переводе денег в счет предоплаты, покупатель лишается гарантий их возврата или получения товара. Если же всё же решили совершить покупку по предоплате, то проверьте сначала рейтинг продавца в платежных системах;
- Отсутствие контактной информации и сведений о продавце. Если на сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и

мобильным телефоном то, такой магазин может представлять опасность. Если на сайте указан адрес магазина, проверьте, действительно ли магазин существует. Очень часто злоумышленники указывают несуществующие адреса, либо по данным адресам располагаются совсем иные организации;

- Излишняя настойчивость продавцов. Если в процессе совершения покупки менеджер магазина начинает торопить совершить заказом и оплатить его, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи — это явный признак мошенничества, поскольку злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все условия сделки.

Так, отсутствие возможности курьерской доставки и самовывоза товара, низкая цена товара, отсутствие у магазина «истории», а также подтверждение личности продавца путем направления отсканированного изображения паспорта, также свидетельствуют о подозрительности продавца, магазина.

При совершении телефонного мошенничества потерпевшему в соответствии со ст. 141 УПК РФ следует незамедлительно обратиться в отделение полиции и написать заявление о свершившемся противоправном деянии.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью.