Прокуратура Смоленского района Смоленской области разъясняет.

Преступления в сфере информационных технологий включают как распространение [вредоносных программ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81), взлом [паролей](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C), кражу номеров [банковских карт](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D0%BB%D0%B0%D1%82%D1%91%D0%B6%D0%BD%D0%B0%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0) и других банковских реквизитов, [фишинг](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3), так и распространение противоправной информации через [Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Вместе с тем, к самым распространенным видам преступлений в обозначенной сфере относится телефонное мошенничество.

Так, номер банковской карты состоит из 16 цифр, распределенных на 4 группы по 4 цифры в каждой группе и формируемых по специальному алгоритму: первая цифра обозначает принадлежность банковской карты к определенной платежной системе; следующие пять цифр позволяют определить банк, выпустивший карту (цифры с 1-й по 6-ю также называют банковским идентификатором); цифры с 7-й по 8-ю несут в себе информацию о программе банковской организации, выпустившей карту; цифры с 9-й по 15-ю являются собственно номером банковской карты, заключительная 16-я цифра - это проверочное число; на оборотной стороне банковской карты есть CVV-код, состоящий из трех цифр (иногда из четырех), который может запрашиваться при проведении финансовой транзакции с использованием банковской карты.

Все вышеуказанные числа необходимы не только для идентификации, они формируют первую линию защиты от мошенника - именно эта информация будет целью, которую он тщательно будет пытаться узнать.

Например, Вам звонят или присылают СМС-сообщение с предложением под разными предлогами сообщить номер, PIN-код, CVV-код и другие реквизиты Вашей банковской карты. Это может быть платеж, совершенный якобы ошибочно на Вашу карту, или сообщение о блокировке Вашей карты. Может также поступить звонок о необходимости экстренного платежа Вашему родственнику или другу, попавшему в затруднительное положение. Данные о реквизитах вашей банковской карты позволят мошеннику произвести с нее списания денежных средств.

Чтобы не попасться на удочку мошенников, **не передавайте** информацию о Вашей банковской карте другим лицам, даже сотрудникам банка, и не перезванивайте по телефонам, указанным в СМС-сообщениях.

В связи с этим рекомендуется следующее: Вам надлежит точно удостовериться в надежности получателя средств, а также в необходимости оказания такой помощи конкретным лицам и только потом совершать какие-либо платежи. Старайтесь не вовлекаться в игру мошенников, постарайтесь закончить разговор в тот момент, когда только возникает подозрение, что Вами пытаются манипулировать. Обязательно сами перезвоните в банк, чтобы рассеять все сомнения.