Прокуратура Заднепровского района г. Смоленска информирует.

Способы защиты граждан от преступных посягательств в сфере информационных технологий.

На сегодняшний день информационно-телекоммуникационные технологии затрагивают все сферы жизни современного человека. Одновременно с этим происходит стремительный ростчисла преступлений, совершаемых с использованием данных технологий. Чаще всего схема совершения преступления выглядят следующим образом: злоумышленник звонит на сотовый телефон «жертвы», представляясь сотрудником отдела безопасности банка, в ходе телефонного разговора получает информацию о банковской карте потерпевшего (номер банковской карты, CVC/CVV-код). Далее происходит завладение злоумышленником денежных средств с карты «жертвы» и перевод средств на иные счета. Росту числа таких преступлений способствует большой материальный доход от такой деятельности, мобильность оборудования, способствующая сокрытию следов и уклонению от ответственности. А также низкое правовое просвещение граждан о способах защиты от преступных посягательств такого рода.

Уважаемые граждане!

Убеждайтесь в достоверности информации, полученной в ходе телефонного разговора и Интернет-переписки с неизвестными лицами. Ни при каких обстоятельствах не сообщайте свои личные данные и реквизиты банковских счетов и карт, тем более пароли от них.

Рекомендации гражданам:

1. Сотрудники безопасности банков не запрашивают Ваш номер мобильного телефона и другую дополнительную информацию через СМС-сообщения или телефонные звонки.
2. Никому не сообщайте ПИН-,CVC/CVV- коды банковской карты и одноразовые пароли.
3. В случае утраты банковской карты необходимо немедленно обратиться в банк с целью ее блокировки – это поможет сохранить Ваши денежные средства.
4. При вводе ПИН-кода необходимо прикрывать клавиатуру, вводить ПИН-код быстрыми, отработанными движениями, что предотвратит завладение данной информацией мошенниками в случае установки ими скрытых видеокамер.
5. Перед тем, как вставить карту в картоприемник, внимательно осмотреть банкомат на предмет наличия подозрительных устройств.
6. В торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты.

7. Если Ваш родственник звонит Вам с неизвестного номера или любое другое лицо сообщает, что он «в беде» и требует Ваши личные данные или данные карты, то в первую очередь необходимо позвонить этому родственнику. Не дозвонившись, сообщите о случившемся в полицию, а не поддавайтесь на уговоры злоумышленников, единственная цель которых – завладеть Вашими деньгами.
8. Если в социальных сетях Вам поступило сообщение с просьбой о переводе денежных средств под любым предлогом или перейти по неизвестной ссылке, в первую очередь свяжитесь с отправителем сообщения другим способом (по телефону или через другую социальную сеть).

Если Вы или Ваши близкие стали жертвами мошенников, либо Вы подозреваете, что в отношении Вас совершаются противоправные действия – незамедлительно обращайтесь в правоохранительные органы!