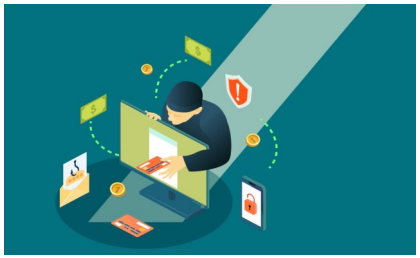
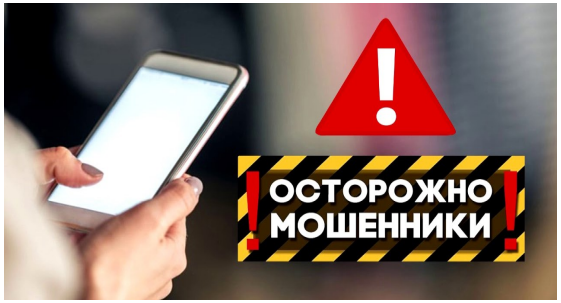
Преступления в сфере ИТТ разнообразны, прежде всего к ним относится, мошенничество, совершаемое посредством информационно-телекоммуникационной сети «Интернет», так и с помощью средств мобильной связи (ст. 159 УК РФ), преимущественно это хищения денежных средств с банковских счетов граждан. Также к таким преступлениям относятся, например, хищения, совершенные с использованием расчетных (пластиковых) карт (п. «г» ч. 3 ст. 158 УК РФ), создание, использование и распространение вредоносных программ (ст. 273 УК РФ), распространение противоправной информации (клеветы) посредством информационно-телекоммуникационной сети «Интернет» (ч. 2 ст. 128.1 УК РФ).



ЧТО ТАКОЕ ПРЕСТУПЛЕНИЯ В СФЕРЕ ИТТ?

Под преступлениями в сфере ИТТ понимаются такие уголовно запрещенные под угрозой наказания общественно опасные деяния, которые непосредственно совершены с использованием информационных технологий и информационно-телекоммуникационных сетей, в виртуальном мире.



Включают в себя:

⇒ интернет-мошенников;

⇒ телефонных мошенников.

Генеральная прокуратура Российской Федерации
Прокуратура Амурской области
Прокуратура Мазановского района

Профилактика преступлений, совершенных с использованием информационно-телекоммуникационных технологий

МЕРЫ ПРЕДОСТЕРЕЖЕНИЯ

⇒ не передавайте свои технические устройства незнакомым и малознакомым лицам, ни при каких обстоятельствах не сообщайте пароли и коды доступа к банковским картам и счетам ни один из представителей банка не запросит у клиента данную информацию;

⇒ сотрудники банков не звонят клиентам при сомнительных операциях, а сразу производят блокирование счета (карты);

⇒ знайте, что преступники используют специальные программы подмены номера, в результате которой Вашим техническим устройством связи поступающие от преступников звонки определяются как принадлежащие банку и идентичные указанному на обороте банковской карты;

⇒ при пользовании Интернет-ресурсами не переходите
на сомнительные сайты, так как преступники создают сайты-двойники, различие в наименовании может быть в одной точке и требует более внимательного использования, на постоянной основе знакомьтесь с общими рекомендациями по обеспечению безопасности работы в сети Интернет.

ВАЖНО!!!

При совершении преступлений преступники используют различные поводы, чтобы завладеть информацией или побудить человека самостоятельно передать денежные средства. Типичными фразами, предлогами для осуществления преступлений являются: «Ваш родственник, либо близкий попал в беду», «с Вашего банковского счета происходят операции по списанию», «Вам ошибочно переведены деньги», «Вы участвуете в акции и выиграли приз», «Положи мне на телефон деньги, не могу до тебя дозвониться», «Ваш почтовый ящик заблокирован, срочно перейдите по ссылке», «Вы можете предупредить преступление» и т.д.

В случае если Вы стали жертвой кибермошенников:

⇒ отключите устройство;

⇒ свяжитесь с банком, отозвать денежный перевод, заблокируйте расчетный счет

⇒ в течении одного дня напишите заявление в банк об отзыве платежа.

⇒ получите в банке детализацию с расчетного счета и обратиться в банк, в который ушли деньги по инициативе злоумышленника, с заявлением о приостановке исполнения платежа и возврате средств.

⇒ подайте заявление о факте хищения денежных средств в полицию.

Государство на законодательном уровне реагирует на сложившуюся обстановку.

Так, федеральным законом от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» усилено наказание за хищение денежных средств с банковского счета или электронных денежных средств до 6 лет лишения свободы. При этом уголовная ответственность наступает не только за совершение хищений с использованием банковских карт (их реквизитов и контрольной информации), но и иных электронных средств платежа («электронные кошельки», другие платежные сервисы).

Кроме того, главой 28 Уголовного кодекса РФ предусмотрена уголовная ответственность за совершение преступлений в сфере компьютерной информации (киберпреступлений).