Как избежать мошеннических действий в интернете.



Интернет-мошенничество – вид мошенничества с использованием интернета. Оно может включать в себя скрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и наследства. Интернет-мошенничество не считается отдельным преступлением, а включает ряд незаконных действий, совершаемых в киберпространстве.

Каждый день появляются новые способы мошенничества в сети интернет, в том числе в интернет магазинах, социальных сетях (вконтакте, одноклассники, а также мессенджерах - whatsapp, viber).

Любое действие в интернете, особенно связанное с перечислением денежных средств, требует осмотрительности и тщательной проверки.

Примеры интернет-мошенничества:

Мошенничество при онлайн продаже товаров в интернет-магазинах, в социальных сетях или интернет-сервисах встречается в двух наиболее распространенных формах:

a)                Мошенники продавцы просят заранее перечислить денежные средства за товар, но в дальнейшем его не отправляют, перестают отвечать на сообщения и звонки. продаже товаров:

b)                Мошенники покупатели спрашивают реквизиты банковской карты для перевода денежных средств, а затем просят сообщить смс-код якобы для перевода, но фактически будет происходить списание денежных средств с Вашей карты.

Если Вы совершаете покупку/продажу через интернет:

·                   не сообщайте незнакомым лицам свои персональные данные и реквизиты банковских карт;

·                   не осуществляйте переводы, если Вас просят перевести денежные средства на электронные кошельки или пополнить баланс мобильного телефона;

·                   если вы сомневаетесь в надежности продавца, лучше откажитесь от покупки.

1.                Мошенничество на сайте знакомств.

Мошенник создает привлекательный профиль (страницу) на сайте знакомств и постепенно завоевывает доверие жертвы, оказывая знаки внимания и втираясь в доверие, при этом могут использоваться данные реально существующего человека, это может быть военнослужащий, успешный бизнесмен, киноактер.

Затем мошенник попросит перевести ему денежные средства для какой-либо цели и перестанет отвечать после совершения перевода.

Как избежать подобной ситуации:

·                   Не переводите денежные средства лицу, с которым общались только по телефону или переписке;

·                   Не переходите по направленным им ссылкам;

·                   Если перевели денежные средства мошеннику, то незамедлительно обратитесь в полицию.

3. Звонки из «службы безопасности» банка с просьбой перевести денежные средства на «резервный» счет.

Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка».

Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у Вас полные данные карты, CVV или СVC-код, одноразовый код из СМС.

Настоящий сотрудник банка никогда:

·                   Не попросит у клиента номер его карты, срок её действия, CVV-номер и одноразовый код из СМС;

·                   Не попросит перевести денежные средства на некий иной счет в кредитной организации;

·                   Не попросит оформить новый кредит для сохранения ваших денежных средств;

·                   Не попросит установить какое-либо приложение на телефон.

В случае хищения Ваших денежных средств или при подозрении совершения в отношении Вас мошеннических действий:

·                   Незамедлительно обратитесь в полицию;

·                   Позвоните в банк и сообщите о мошеннической операции и заблокируйте карту.