**В связи с необходимостью борьбы с киберпреступностью в российское уголовное законодательство введено мошенничество в сфере компьютерной информации.**

**Киберпреступления** - деяния, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребление такими системами, сетями и данными

**Статья 159.6. Мошенничество в сфере компьютерной информации** (введена Федеральным законом от 29.11.2012 N 207-ФЗ)

Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -

**наказывается**

**Предмет преступного посягательства.** Завладение имуществом связано с проникновением в виртуальную среду, в которой осуществляются информационные операции, последствия которых состоят в приобретении участниками оборота имущества в виде наличных денег, безналичных денежных средств, иных имущественных прав (например, зафиксированных в реестре прав владельцев ценных бумаг).

**Орудиями преступления**, предусмотренного ст. 159.6 УК РФ, признаются информация, средства хранения, передачи и обработки компьютерной информации, повлекшие негативные последствия.

**Объективная сторона** мошенничества, предусмотренного ст. 159.6 УК РФ, заключается в хищении чужого имущества или приобретении права на чужое имущество

преступное деяние условно подразделяется на два этапа:

- получение доступа к компьютерной системе;

- ввод, удаление, модификация или блокирование компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей

**Субъектом** неправомерного доступа к компьютерной информации признается физическое вменяемое лицо, достигшее шестнадцатилетнего возраста.

**Субъективная сторона** характеризуется прямым умыслом и корыстной целью.

**Правила, которые помогут Вам не стать жертвой киберпреступлений:**

- храните номер карточки и ПИН–коды в тайне;

- не используйте один пароль для всех интернет-ресурсов;

- регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;

- поставьте лимит на сумму списаний или перевода в личном кабинете банка;

- не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;

- не переводите денежные средства на счета незнакомых лиц;

- не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;

- будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно;

- не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;

- не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;

- насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;

- не размещайте в открытом доступе и не передавайте информацию личного характера.