**Ответственность за мошенничество в сфере компьютерной информации**

Под мошенничеством в сфере компьютерной информации понимается 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.

Наказанием за данное деяние предусмотрено ст. 159.6 УК РФ. Согласно санкции статьи, за совершение данного преступления может быть назначен штраф в размере до 120 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо ограничение свободы на срок до двух лет, либо принудительные работы на срок до двух лет, либо арест на срок до четырех месяцев.

В п. 20 Постановления Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» разъясняется, что по смыслу ст. 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Самыми распространёнными способами незаконного овладения чужими средствами или данными, являющимися собственностью правообладателя, являются:

- интернет-магазин, т.е. при осуществлении онлайн заказа с покупателя берут предоплату за товар и не выполняют своих обязательств либо по факту поставки товар существенно отличается от представленного в предложении на сайте (на сегодняшний день наиболее распространено мошенничество в интернет – магазине «Авито»);

  -фишинг, т.е. при помощи почтовых рассылок от лица банка, содержащих в себе ссылки на страницы, являющиеся точными копиями официальных сайтов, на которых предлагается ввести данные карты для возможности дальнейшего ее использования. Также все большую популярность обмана доверчивых граждан набирает голосовой фишинг, когда клиенту банка звонят от имени финансовой организации и под разными предлогами стараются узнать платежную информацию. Мошенники находят способы для блокировки облачных хранилищ с личными данными, устройств Apple в целях последующего шантажа;

- контент, содержащий вирусы, заключается в том, что включается в изменении процедуры доступа и выводе сообщения с требованием отправки СМС-сообщения или перевода средств для получения деблокирующего пароля. Стоимость короткого сообщения при его отправке существенно превышает указанный размер. Альтернативным является заражение компьютера "трояном", открывающим доступ к личным данным;

-«фейки» в социальных сетях, т.е. создается аккаунт вымышленного человека для общения с определенной категорией пользователей в части достижения собственных целей, например, получение личных фото и видео интимного характера для последующей демонстрации на страницах тематических ресурсов;

Для защиты от мошенников следует придерживаться некоторых правил.

- Никогда и никому, ни при каких обстоятельствах нельзя передавать такие конфиденциальные данные, как логин, пароль или реквизиты банковской карты;

- Выбирайте банкоматы, расположенные внутри офисов банков или в охраняемых точках, оборудованных системами видеонаблюдения.

- Если вы потеряли карту или у вас есть основания полагать, что третьи лица узнали ее реквизиты, обратитесь в банк и заблокируйте ее.

- Всегда с подозрением относитесь к сообщениям, в которых вас просят перейти по какой-то ссылке (проверьте, нет ли этой страницы в списке подозрительных).

- Помните, что даже если письмо или сообщение со ссылкой вы получили от лучшего друга, расслабляться нельзя - его тоже могли обмануть. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

- По возможности не заходите в онлайн-банки и другие подобные сервисы через открытые **Wi-Fi**-сети в кафе или на улице (за таким **Wi-Fi** могут стоять мошенники, подменяющие адрес сайта на уровне подключения и перенаправляющие вас на поддельную страницу).