ПАМЯТКА

для граждан в целях недопущения фактов «дистанционных хищений»

Количество «дистанционных хищений» к сожалению, растет с каждым годом.

Рост связан, прежде всего, с постепенным переходом населения на безналичный расчет, выпуском и начислением заработных плат, пенсий, пособий и других выплат на пластиковые карты, появлением большего количества интернет-магазинов, возможностью оплачивать услуги онлайн, интернет становиться более доступным, расширяются зоны покрытия сетей сотовой связи, как следствие все больше людей пользуются современными технологиями.

Какие основные способы хищений применяются мошенниками?

Схема 1. Мошенничества через сайты объявлений (продавец).

Мошенник размещает на сайтах объявлений (Авито, Дром, Юла, Циан, Доска.Якт и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг, за которые в *последующем получает предоплату, тем самым похищая деньги.*

Схема 2. Мошенничества через сайты объявлений (покупатель).

Мошенник звонит по объявлению потерпевшего, размещенному на сайте (Авито, Юла, Циан и др.) и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код и в последующем похищая денежные средства.

Схема 3. Мошенничества со взломом страниц социальных сетей.

Мошенники взламывают страницы социальной сети (В Контакте, Одноклассники, Друг вокруг и др.) и в последующем пишет всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.).

Схема 4. Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду.

На стационарный или абонентский номер потерпевшего звонит мошенник, который обращается под видом родственника (привет мама, привет бабушка и т.д.). Сообщает, что попал в ДТП и сбил человека, с кем- то подрался и т.д., а после передает трубку сотруднику полиции, который за отдельную плату предлагает решить вопрос об отказе в возбуждении уголовного дела.

Схема 5. Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы.

На стационарный или абонентский номер потерпевшего звонит мошенник, который, представляется сотрудником прокуратуры или правоохранительных органов. Он сообщает, что в настоящий момент задержана группа мошенников, продававших некачественные БАДы, и что потерпевшему положена компенсация. Однако для ее получения необходимо оплатить государственную пошлину или налоговый сбор.

Схема 6. Мошенничество, совершенное с использованием вредоносных программ на ОС «Android».

Потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом: «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? (приводится ссылка на сайт объявлений)». или SMS-сообщение с текстом: «Смотри как мы здорово получились на этой фотографии. (также приводится ссылка на интернет-ресурс)». Потерпевший проходит по данной ссылке, в результате чего загружает на свой телефон вирус (чаще всего используются вирусы под названием «Triada» и «Marcher»), предоставляющий злоумышленнику доступ к SMS-командам телефона потерпевшего. В дальнейшем мошенник похищает деньги, путем направления сообщений на номер «900».

Схема 7. Мошенничество, совершенное под предлогом несанкционированных списаний с банковской карты

Используя IP - телефонию звонит потенциальной жертве с виртуального номера (495…,8-800…и тд) и сообщает о том, что по его банковской карте либо по счету осуществляются несанкционированные списания денежных средств или происходит оформление кредита и для сохранения средств необходимо их перевести в безопасную ячейку. После чего, потерпевший, следуя инструкциям мошенника сообщает все реквизиты своих карт, CVV - коды и пароли, поступившие в смс – сообщение.

Какие рекомендации существуют, чтобы уберечься от таких преступлений и не стать жертвой злоумышленников?

- Так, в случае утраты сотового телефона или сим-карты, а также в случаях, когда вы решили сменить номер телефона, необходимо уведомить об этом банк, и путем подачи письменного заявления отвязать услугу «Мобильный банк» от старого номера.

- При поступлении на Ваш мобильный телефон разного рода рассылок необходимо быть бдительными и не отвечать на подобные сообщения, ни в коем случае не переходить по каким-либо указанным ссылкам.

- Необходимо помнить, что сотрудники банков никогда не запрашивают у клиента информацию о реквизитах карты, пин-коды и одноразовые пароли. Необходимо отметить, что злоумышленником могут быть люди с хорошей дикцией и приятным голосом.

- Не следует совершать покупки в непроверенных интернет-магазинах. Нередко такие магазины привлекают покупателей низкой ценой, качественным оформлением сайтов. Прежде чем совершать покупку не забывайте внимательно изучать отзывы покупателей, старайтесь узнать о магазине как можно больше. Не лишним будет связаться с представителями магазина, задать им несколько вопросов.

Необходимо помнить, что сотрудники правоохранительных органов никогда не потребуют с вас денежных средств за урегулирование проблемного вопроса. Свяжитесь с родными и близкими, попавшими в беду, напрямую, сообщите информацию о звонке, проверьте ее.

Какая ответственность предусмотрена законом для преступников?

В Уголовном кодексе Российской Федерации предусмотрена уголовная ответственность по статье – 159.6 «Мошенничество в сфере компьютерной информации».

Согласно данной норме мошенничество в сфере компьютерной информации это 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 штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

Кроме того, в указанной статье предусмотрены дополнительно следующие составы преступлений, которые влекут более строгое наказание:

- ч.2 ст. 159.6 УК РФ - Мошенничество в сфере компьютерной информации совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину.

-ч.3 ст. 159.6 УК РФ - деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) лицом с использованием своего служебного положения;

б) в крупном размере;

в) с банковского счета, а равно в отношении электронных денежных средств, -

- ч.4. ст. 159.6 УК РФ деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере.

Наиболее строгое наказание предусмотрено по ч.4 ст. 159.6 УК РФ - до 10 лет лишения свободы.

В целях обеспечения единообразного применения органами следствия, государственным обвинением и судами указанной статьи Пленумом Верховного Суда Российской Федерации дано разъяснения в постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

В частности разъяснено, что по смыслу статьи 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.

Если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, Интернет-магазинов, использование электронной почты), то такое мошенничество квалифицируется как общеуголовное по статье 159 УК РФ (Мошенничество), а не по статье 159.6 УК РФ.

Будьте бдительны! Не попадайтесь на уловки мошенников!

Прокурор города Волгореченска Д.В. Ивков