Сохраним свои деньги от мошенников.

Самые распространенные схемы мошенничества

Схема 1. Мошенничества через сайты объявлений. Мошенник-продавец. Мошенник размещает на сайтах объявлении (Авито, Юла, Циан и тд.) 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. Мошенник-покупатель.

Мошенник звонит по объявлению потерпевшего, размещенному на сайте (Авито, Юла, Циан и тд.) и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения осуществляют перевод через онлайн сервисы или совершая покупку. Или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк, и в последующем похищая денежные средства.

Схема 3. Мошенничества со взломом страниц социальных сетей. Мошенник покупает в сети интернет взлом страницы социальной сети (ВКонтакте, Одноклассники, Инстаграмм и тд.) или осуществляет его самостоятельно. 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 тд.).

Схема 4. Мошенничества, совершенные с использованием Интернет-сайтов (Интернет-магазинов).

Мошенник создает (или покупает) интернет сайт по продаже товара различной тематики. Регистрирует несколько виртуальных номеров (8-800…,8-495…) у SIP-провайдера и указывает их на сайте в качестве контактов. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта.

Схема 5. Мошенничество, совершенное под предлогом заказа банкета (или связь с курьером).

Мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу банкета, заказу крупной партии товара или прочих услуг. Далее он сообщает адрес, где бы он хотел встретиться с представителем компании и спрашивает его телефон. В последующем он связывается с представителем и просит последнего по пути пополнить счет абонентского номера 9или банковской карты) на неопределенную сумму, которую он отдаст при встрече.

Схема 6. Мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств. Мошенник осуществляет рассылку SMS-сообщений с текстом о списании денежных средств или блокировке банковской карте. В данном сообщении указывает свой другой абонентский номер (иногда виртуальный 8-800..,8-

495..), который может проинформировать о произошедшем. Потерпевший звонит по данному номеру, после чего мошенник либо просит сообщить контрольные данные банковской карты, либо просит подойти к банкомату.

Схема 7. Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду.
На стационарный или абонентский номер потерпевшего звонит мошенник, который сообщает под видом родственника и сообщает, что попал в ДТП и сбил человека, с кем-то подрался и тд., а после передает трубку сотруднику полиции, который за отдельную плату предлагает решить вопрос об отказе в возбуждении уголовного дела.

Схема 8. Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы.
На стационарный или абонентский номер потерпевшего звонит мошенник, который, представляется сотрудником прокуратуры или следственного комитета. Он сообщает, что в настоящий момент задержана группа мошенников, продававших некачественные БАДы, и что потерпевшему положена компенсация или адвокат для участия в судебных разбирательствах. Однако для ее получения необходимо оплатить государственную пошлину, налоговый сбор или оплатить услуги адвоката.

Схема 9. 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? Ссылка: www.avito.o.ru/FriZksk)», или SMS-сообщение с текстом: «Смотри как мы здорово получились на этой фотографии. Ссылка www.bit.ly/ZreizEleaAa)». 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. В дальнейшем мошенник похищает деньги, путем направления сообщений на номер «900».