

## Прокуратура Каргопольского района предупреждает о мошеннических действиях с использованием IT-технологий:

Один из таких способов это звонок по сотовому телефону, номер которого не известен человеку, представляются от имени близкого родственника (сын, дочь, супруг и т.п.), говорят что он(а) попал в аварию, полицию, тюрьму или что-то подобное, лежит в больнице и на операцию (врачам) нужны деньги, которые необходимо перевести на номер сотового телефона или названный им счет.

Второй способ представляет опасность для людей, кто каким-либо образом утратил свои документы (паспорт, права и т.п.), дал объявление в газете или сети интернет об их возврате за вознаграждение. Этим способом любят пользоваться люди, отбывающие наказание в местах лишения свободы. Они звонят по указанному номеру сотового телефона и заставляют доверчивых граждан переводить денежные средства путем внесения определенных денежных сумм на номер телефона, которые за считанные минуты переводятся на другие номера, счета или попросту тратятся.

Третий способ, для людей ищущих легкой наживы, так сказать «халявы» - на сайтах «Авито», «Автору» и ряде аналогичных, которые подыскивая различных интересующий их товар, в основном машины, трактора, снегоходы и мотоциклы, натываются на объявления о продаже интересующей их техники по бросовой цене либо с очень большими скидками. Созваниваются, проверяют данные, в том числе паспортные (мошенники отнюдь не дураки, они используют потерянный кем-то паспорт и представляют этими установочными данными, и даже могут вам скинуть копию паспорта), после чего вводят вас в заблуждение, заговаривая вас, предлагают скинуть предоплату от 30% до 100% стоимости на номер пластиковой банковской карты, который они Вам высылают. Здесь нужно смотреть и быть очень внимательным, поскольку при переводе высвечиваются данные владельца карты, например: «Сергей Петрович И.» и если они не совпадают с данными человека, с которым вы общаетесь и уж тем более паспортными данными, то спешить переводить денежные средства не стоит.

Четвертый способ, для наших сердобольных граждан, путем рассылки СМС-сообщений, в которых указывается о проводимой акции «добрых дел» каким-то «липовым» благотворительным фондом во спасение детей, животных или территории от загрязнения, где вам предлагается перевести определенную сумму денег, при этом не стоит забывать, что и за перевод также деньги будут сняты. Отмечу, что все настоящие акции добрых дел официально освещаются на федеральных каналах, у них есть свои официальные сайты в сети интернет, где подробнеем образом указана история детей или проблемный вопрос, на который идет сбор средств.

Пятый способ, легкие деньги или быстрый заработок, то есть заработать огромные деньги, потратив минимум времени и вложений, что возможно «благодаря» казино онлайн казино, букмекерским конторам, рынок «Форекс» и так далее, где вас введут в заблуждение, выманив у вас тем самым немалые денежные средства. Люди, кто умеет так зарабатывать, вряд ли поделятся с вами данными секретами, появившимися на вашем рабочем столе в «всплывающих окнах».

Шестой способ, так называемые телефонные лотереи, когда на ваш сотовый телефон поступают СМС-сообщения о том, что вы стали участником, финалистом лотереи, и выиграли автомобиль, крупную сумму денег или другой ценный приз, после чего вам предлагается либо продолжить участие в ней, чтобы выиграть более

крупную сумму (ценный приз), либо получить деньги, но для этого вам нужно перевести определенную сумму на их счет, например, под предлогом уплаты налогов за выигрыш. Вы переводите указанную сумму на указанный ими телефон или счет и все это продолжается до тех пор, пока у вас не заканчиваются деньги, а потом ....а потом все, и они куда-то пропадают...

Седьмой способ, набирающий популярность, это использование вашей личной странички в таких социальных сетях как «Вконтакте», «Одноклассники», «Фейсбук», «Твиттер» и т.п., когда мошенники делают полную копию вашей странички и уже от вашего имени рассылают под благовидным предлогом просьбы о переводе денежных средств - сумма варьируется от «важности» предлога, указывают данные карты, номер сотового телефона или электронный кошелек, куда необходимо перечислить денежные средства. Последствия, надеюсь, понятны.

Восьмой способ, высший пилотаж, это вредоносные (вирусные) программы, разрабатываемые профессиональными программистами - хакерами, которые могут оказаться на вашем телефоне, планшете, ноутбук, компьютере при выходе на сайт в сети интернет и скачивании какой-либо информации или программы, они скачиваются одновременно и дают возможность удаленно управлять вашими техническими средствами, соответственно становятся обладателями вашей личной информации, что влечет за собой нарушение неприкосновенности частной жизни (ст. 137 УК РФ), и утечку данных, в дальнейшем, с помощью которых мошенники получают доступ к вашим электронным банковским картам.

Девятый способ, когда вы заказываете какой-либо товар на сайте, с вами общается продавец и все чинно и пристойно, до тех пор, пока не приходит по Почте заказанный товар, но там не совсем то, что Вы ожидали: вместо куртки - ненужные тряпки и, банально, обычный песок.

Десятый способ, когда представляются сотрудниками одного из банков (сотрудниками службы безопасности банка), где у вас имеется электронная банковская карта, называют все ваши данные, номер карты и счета, при этом сообщают о совершении по вашему счету подозрительных операций, предлагают при этом либо назвать код, который придет вам по СМС, либо перевести все ваши деньги на новый «безопасный» специально приготовленный для вас счет. В дальнейшем, при выполнении указаний мошенников, ваши деньги исчезают со счета.

Поэтому ряд простых советов доверчивым гражданам во избежание печальных инцидентов: перестать искать «халявы», верить в чудо, Деда Мороза, быть более внимательными, при необходимости, созваниваться с близкими; не переводить крупные суммы денег, максимально проверять и уточнять данные продавца и покупаемого товара, запрашивать на них копии подтверждающих документов, получать которые лучше по факсу - стационарный телефон; просить знакомых (если это другой город) съездить и посмотреть товар; сопоставлять данные продавцов, паспортов и банковских карт (работа от имени друга или знакомого - продажа по его просьбе, должна вас насторожить); устанавливать на ваши девайсы (технические средства связи) сертифицированные программы защиты от вирусов.

Прокурор Каргопольского района  
старший советник юстиции Носков В.А.