Дистанционное мошенничество, то есть совершение хищения денежных средств с использованием телекоммуникаций – быстрый и лёгкий, но незаконный способ заработать деньги на доверчивых гражданах.

Мошенники пользуются любой ситуацией, сложившейся в обществе, чтобы обогатиться. Злоумышленники представляются сотрудниками банков, сотрудниками правоохранительных органов, покупателями (продавцами) товаров (услуг), родственниками, сотрудниками Госуслуг. При этом, для того, чтобы выманить деньги или сведения о банковских картах, сообщают, что родственник попал в беду, близкий человек болен и ему срочно требуется дорогостоящая медицинская помощь, что на деньги гражданина оформлен кредит, произошло снятие с его карты, взломан личный кабинет и т.д. Если ранее в мошеннических схемах чаще использовались поддельные Интернет-ресурсы, имитирующие официальные страницы известных сайтов, то теперь стали использоваться фейковые мобильные приложения, используется переписка в мессенджерах, телефонные звонки совершаются с помощью голосовых роботов (так называемый «автоматизированный обзвон»). Также предлагают получение всевозможных выплат: за трудовой стаж, за перенесённый коронавирус, за участие в акциях, компенсации за оказанные медицинские и иные услуги, начисление дивидендов, пособий, страховых выплат и т.д. Так, используя сложившуюся обстановку в государстве, мошенники изобретают и новые схемы завладения деньгами граждан. За определённую сумму денег предлагают приобрести карты Visa и Mastercard, предлагают открыть счёт в заграничном банке. Также предлагают товары по сниженным ценам, санкционные товары, обмен валюты и т.д. То есть злоумышленники пользуются уловками низкой цены, ограниченного предложения, доступности нужного товара или услуги. Для распространения информации мошенниками используются массовые почтовые рассылки, вбросы в тематических группах в мессенджерах и на форумах, привлекательные рекламные предложения. Если Вам звонят и предлагают сообщить персональные сведения, реквизиты, ПИН и CVV коды банковской карты, а также пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены, предлагают установить программы удаленного доступа, перевести денежные средства на «защищенный счет» - это мошенники.

Будьте внимательны, соблюдайте элементарные правила кибер-безопасности. Это снизит риск стать жертвой таких хищений.

Помощник межрайонного прокурора А.О. Рой