Об основных видах мошенничества,
связанных с распространением коронавирусной инфекции.

Управление Роспотребнадзора по Красноярскому краю обращает внимание на основные виды мошенничества, связанные с распространением коронавирусной инфекции и введением ограничений передвижения.

Предложения о продаже несуществующих товаров, услуг, социальных льготах:

- Мошенники могут предлагать купить очиститель воздуха, удаляющий возбудителя вируса, или маски с фильтром, отсеивающие вирус. Стоимость может быть сильно завышена, хотя эффективности таких средств не доказана.
- Предложения о покупке лекарств, якобы помогающих от коронавируса.
- Предложение индивидуальных средств защиты известных и надежных производителей с обязательной предоплатой. После получения денег товар не поставляется.
- Многие государственные органы одновременно с началом распространения инфекции стали изготовлять и бесплатно распространять брошюры о коронавирусе. Мошенники могут просить за них деньги.
- Звонки с информацией о контакте с подтвержденным носителем вируса и о том, что придут специалисты для проведения платного анализа.
- Запросы конфиденциальных личных данных для предоставления мифической господдержки, компенсации ущерба от вируса и т.п.
- Фишинговые рассылки (просят пройти по ссылке и т.п. с целью кражи данных карты) – например, про то, как в квартире избавиться от возбудителя вируса с помощью фена.
- Мошенники могут предлагать провести на дому бесплатное тестирование или вакцинацию от коронавируса. Как правило, цель такого визита – квартирная кража.

Использование режима ограничения передвижения:

- В интернете начали появляться мошеннические сервисы, якобы позволяющие проверить, как далеко вам можно отходить от дома. Для этого нужно ввести данные банковской карты.
- В интернете начали активно продавать фальшивые пропуска на въезд и передвижение по Москве и другим городам. Стоит помнить, что оформлением таких пропусков занимаются городские или региональные власти, а информацию о методах их оформления можно найти на официальных сайтах.
- Мошенники могут рассылать фейковые СМС-сообщения о том, что вам выписан штраф за нарушение карантина или самоизоляции. Часто в таких случаях могут просить оплатить его сразу – по номеру телефона или карты, угрожая возбуждением уголовного дела.

Уловки в интернете:

- Мошенники создают вирусные интернет-сайты, распространяющие вредоносное программное обеспечение, для кражи личных данных или данных банковской карты. Часто такие сайты могут маскироваться под официальные порталы реальных организаций, например, ВОЗ или Минздрава.

- Кража личных данных также возможна через фишинговые рассылки, когда пользователя просят перейти по ссылке. Как правило, предлагают познакомиться со способами борьбы с возбудителем коронавируса, средствами защиты и т.д.

- Могут поступать звонки о якобы имевшем место контакте с подтвержденным носителем вируса и предложением сдать платный анализ, для которого специалисты приедут домой.

Обещания помощи с пособиями или долгами:

- Мошенники могут запрашивать конфиденциальные личные данные, чтобы помочь в оформлении пособий и компенсаций ущерба от вируса.

- Гражданам могут поступать предложения по урегулированию взысканий или помощи в проведении процедуры банкротства за комиссию. Получив предоплату, преступники скрываются.

Лжеблаготворительные акции:

- Мошенники могут попросить принять участие в благотворительных акциях, например, пожертвовать деньги на помощь пожилым людям или соотечественникам, оставшимся за рубежом. Переведенные в таком случае деньги, скорее всего, вернуть не удастся. Следует тщательно проверять такие обращения.

Ложные предложения о работе:

- Фейковые предложения об удаленной работе под прикрытие корпоративных рассылок. Такие сообщения могут иметь вид приглашения принять участие в Zoom-конференции. Таким образом, мошенники заставляют перейти по небезопасным ссылкам.

- Предложения по удаленной работе. Для того, чтобы к ней приступить, мошенники заявляют о необходимости предварительно купить методические материалы.