Мошенничество во время пандемии коронавирусной инфекции

К сожалению, воспользовавшись непростой ситуацией с распространением коронавирусной инфекции, мошенники продолжают активно использовать незаконные и обманные схемы и методы для кражи денежных средств и персональных данных граждан. При этом злоумышленники постоянно изобретают новые способы. Они действуют изощренно, используя все новые схемы социальной инженерии и интернет.

Необходимо иметь представление о самых распространенных мошеннических методах, чтобы не стать жертвой злоумышленников.

- **«штраф за нарушение режима самоизоляции»**. На мобильный телефон гражданина приходит смс-сообщение якобы от государственных органов с требованием оплатить «штраф» за нарушения карантина или самоизоляции. К сообщению мошенники прилагают реквизиты, по которым нужно внести оплату. Иногда о «нарушении режима самоизоляции» обманщики сообщается по телефону. При этом уточняется, что суды из-за пандемии не работают, но у нарушителя есть шанс прекратить производство по делу, оплатив штраф удаленно. В противном случае - грозит уголовная ответственность.

- **«компенсация за режим самоизоляции, карантин и т.п.».** В социальных сетях рассылается или размещается фейковая информация о выплатах из-за режима самоизоляции в связи с распространением коронавирусной инфекции. К сообщению прилагают ссылки на сайты, где эти выплаты «оформляются». Тем, кто кликает на эту ссылку и заполняет там анкетные данные, приходит сообщение о якобы полагающейся компенсации. Но есть условие - для получения необходимо сначала оплатить комиссию, услуги по оформлению документов, создать ключ электронной подписи, пройти проверку безопасности транзакции.

Другой вариант – телефонный звонок гражданину на мобильный или домашний телефон с сообщением о перечислении «карантинной» выплаты, для получения которой необходимо сообщить данные банковской карты.

- **-«оформление отсрочки по кредитам, получение денежной помощи и др.»**. На электронную почту, мобильный телефон гражданам приходят письма (смс-сообщения) с фишинговыми ссылками, то есть такими, которые открывают доступ к личным паролям и логинам пользователя. По этим ссылкам сообщается о якобы отсрочке по кредитам, о праве на получение пособий, волонтерскую помощь и др. Человека пытаются заставить пройти по ссылке и оставить на фиктивном сайте - «близнеце» данные для доступа к платежным системам и банковским картам и другую личную информацию.

- **«сообщение о родственнике в больнице с коронавирусной инфекцией»**. На мобильный телефон гражданину поступает звонок от имени лже-врачей, лже-сотрудников Роспотребнадзора и других ведомств. Гражданам сообщают, что у их родственников или близких оказался положительный тест на коронавирусную инфекцию, их увезли в больницу или изолировали в обсерваторе. При этом предлагается перевести денежные средства на счет «медучреждения» для улучшения условий содержания больного и его лечения. Таким же образом могут также предлагаться медицинские препараты, якобы рекомендованные для лечения от COVID-19, или даже вакцина от него.

- **«рассылка писем от Всемирной организации здравоохранения»**, где ВОЗ «призывает ознакомиться с мерами безопасности против вируса». Пользователь нажимает на ссылку и переходит на фишинговый сайт, где нужно ввести персональные данные. В таком случае персональные данные гражданина могут стать достоянием общественности.

Специалисты по информационной безопасности рекомендуют установить антивирус на каждое устройство — смартфон, планшет, компьютер для исключения таких проблем.

- **«рассылки писем от Всемирного банка (ВБ) или Международного валютного фонда (МВФ)».** Граждан просят внести небольшое пожертвование на борьбу с коронавирусом, на восстановление мировой экономики и т.д. Опасность указанной схемы в том, что при переходе по ссылке и введении в специальном поле данные банковской карты, мошенники смогут получают доступ к Вашим денежным средствам.

- **«продажа средств индивидуальной защиты, антисептических средств, перчаток и т.д.».** Мошенники активно используют продажу дефицитных товаров (маски, антисептики, различные средства гигиены) как способ получить данные банковских карт граждан при оформлении покупки. Эксперты советуют заниматься онлайн-шопингом только на проверенных площадках, например официальных сайтах магазинов, при этом никогда не переводить за товар денежные средства заранее и не сохранять данные своей банковской карты.

- **«тест на коронавирусную инфекцию на дому».** На различных сайтах или в интернет-магазинах гражданам предлагают купить тесты на COVID-2019 для самостоятельного проведения. Это является мошенничеством: тесты проводятся в только медицинских учреждениях.

- **«исцеляющие коронавирусную инфекцию средства».** В сети Интернет появляются объявления о продаже магических средств защиты от коронавирусной инфекции - амулеты, обереги, подвески и проч. Покупателям гарантируется защита от COVID-19, что, безусловно, является мошенническими действиями.

- **«санобработка квартиры от инфекции и т.п.»**. Мошенники в специальной одежде - белых халатах или комбинезонах, масках и с дезинфекторами звонят в дверь квартиры. Если им открывают, сообщают о внеплановой санитарной

обработке жилья от коронавирусной инфекции. После их ухода граждане часто обнаруживают кражу денежных средств, вещей, ценностей и др.

Практические советы:

1. Никому не сообщайте реквизиты своих банковских счетов и карт, код с оборотной стороны пластиковой карты, а также СМС-коды и пароли, присылаемые банками.

2. Если вам звонят незнакомые граждане, кем бы они ни представлялись, прекратите разговор и положите трубку. Перезвоните своим близким или в названную звонившим компанию для уточнения информации.

3. Ни при каких обстоятельствах не перечисляйте деньги на счета и номера телефонов, которые сообщили вам злоумышленники.

4. Если вы стали жертвой или свидетелем мошенничества, немедленно сообщите в полицию.

5. Избегайте народных целителей, гадалок, колдунов, которые сейчас активно берутся спасать клиентов от коронавируса.

6. В сети Интернет и социальных сетях не стоит отвечать на сообщения от незнакомых людей, предлагающих помочь справиться с вирусом, а также переходить по неизвестным ссылкам. Как только Вы перейдете по ссылке, злоумышленники получат доступ к вашим данным, а может, и счетам.

7. Не открывайте дверь незнакомым людям, даже если они в белых халатах, масках и представляются сотрудниками какого-либо ведомства. Всегда требуйте документы. Если Вы находитесь на карантине, медицинские работники могут прийти к Вам только после предварительного звонка.

8. Не поддавайтесь панике. Соблюдая необходимые правила профилактики, Вы находитесь в безопасности.

Адреса:

УМВД России по Архангельской области
163000, г. Архангельск, ул. Воскресенская, д. 3
Дежурная часть: 8 **(**8182) 28-60-20, 21-66-18

Прокуратура Архангельской области
163002, г. Архангельск, просп. Новгородский, д. 15
Приемная: (8182) 41-02-04

Уполномоченный по правам человека в Архангельской области
163000, г. Архангельск, пл. Ленина, д. 1, каб. 210
8(8182) 20-72-96

Уполномоченный по правам человека в Российской Федерации
119121, г. Москва, Смоленский бульвар, д. 19, стр. 2
Телефон приемной: 8 (495) 870-41-77

Уполномоченный по правам человека в Архангельской области

Как обезопасить себя от мошенничества в период пандемии коронавирусной инфекции?

Архангельск,
2020