

Уважаемые обучающиеся!

С началом действия режима самоизоляции активизировались мошенники, которые используют введенные ограничения в своих целях.

После введения режима повышенной готовности мошенники быстро «переквалифицировались» и стали предлагать гражданам товары и услуги, «актуальные» в условиях распространения COVID-19.

Будьте внимательны и осторожны, если вы столкнулись со следующими обстоятельствами:

1. Предложения о продаже фиктивных товаров и услуг:

- Мошенники могут предлагать купить очиститель воздуха, удаляющий возбудителя вируса, маски с фильтром, отсеивающие вирус, или «чудо-средство» от COVID-19. Стоимость может быть сильно завышена, а эффективность не доказана. К этой же группе относятся предложения о покупке амулетов, оберегов и других магических предметов якобы охраняющих от вируса;

- Также злоумышленники предлагают купить у них лекарства, помогающие от коронавируса. Помните, что в настоящее время лекарства именно от COVID-19 не существует. Кроме того, любые лекарственные препараты необходимо принимать только по назначению врача и не заниматься самолечением;

- Настороженно относитесь к предложению приобрести индивидуальные средства защиты с обязательной предоплатой. Особенно если это неизвестный Вам продавец или интернет-магазин. Часто после получения денег товар не поставляется, сайт блокируется;

- Вам могут поступать звонки о якобы имевшем место контакте с подтвержденным носителем вируса, предложение сделать платный анализ на дому и просьбой заранее оплатить визит медиков;

- Под видом работников санитарно-эпидемиологических служб мошенники ходят по квартирам и заявляют о необходимости сдать бесплатный анализ на COVID-19 или провести дезинфекцию жилого помещения. Как правило, цель такого визита – квартирная кража.

2. Использование режима ограничения передвижения:

- В интернете начали появляться мошеннические сервисы, якобы позволяющие проверить, как далеко вам можно отходить от дома. При осуществлении такой «проверки» вас попросят ввести данные банковской карты;

- Мошенники предлагают купить пропуск на въезд и передвижение по Москве и другим городам. Помните, что продажа пропусков на 100% незаконна. Их оформлением занимаются только городские или региональные власти, информацию о способах их получения можно найти на официальных сайтах. Во всех случаях пропуска выдаются бесплатно на основании поданных Вами или Вашим работодателем сведений;

- 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 немедленно - по номеру телефона или карты, угрожая возбуждением уголовного дела или мотивируя тем, что завтра сумма штрафа удвоится. Не спешите отправлять деньги: знайте, что наложить на Вас штраф можно только по решению суда, а сумма штрафа всегда остается постоянной и прописана в законодательстве.

3. Новые уловки в интернете:

- Часто мошенники создают вирусные интернет-сайты, распространяющие вредоносное программное обеспечение для кражи личных данных или данных банковской карты. В условиях эпидемии COVID-19 такие сайты могут маскироваться под официальные порталы реальных организаций, например, Всемирной организации

здравоохранения или Минздрава России, благотворительных организаций, осуществляющих помощь и поддержку граждан;

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

- Возможно, что злоумышленники пригласят вас на осмотр в поликлинику — пройти обследование на коронавирус. Но сначала Вас попросят зарегистрироваться на неизвестном сайте или установить программу на компьютер или телефон.

- Мошенник создает (или покупает) интернет сайт по продаже товара различной тематики. Регистрирует несколько виртуальных номеров (8-800-..., 8495-... и др.) и указывает их на сайте в качестве контактов. В последующем принимает заявки от покупателей, получая от них денежные средства за покупку товара с сайта, но товар покупателю не предоставляется, сайт блокируется.

4. Обещания помощи с пособиями или долгами:

- Если неизвестные лица запрашивают Ваши конфиденциальные личные данные под предлогом помощи в оформлении государственных пособий и компенсаций ущерба от вируса, возврата денег за авиабилеты/страховой полис и т. п., то необходимо самостоятельно проверить достоверность такого рода сведений. Обо всех мерах государственной поддержки граждан и бизнеса можно узнать из средств массовой информации, а также на официальных сайтах соответствующих государственных учреждений и частных компаний;

- Одна из наиболее распространенных схем мошенничества - предложения по урегулированию взысканий, отсрочке по выплате кредитов или помощи в проведении упрощенной процедуры банкротства за комиссию. Получив предоплату, преступники скрываются. Другой механизм - предложение зайти по ссылке в личный кабинет банка и оставить заявку на получение отсрочки. При переходе открывается фишинговый (поддельный) сайт банка, на котором жертва вводит свои реальные логин и пароль от личного кабинета. Таким образом, эти данные отправляются мошенникам, и они получают к нему доступ.

5. Лжеблаготворительные акции:

- Множество злоумышленников пытаются спекулировать на добрых чувствах: они могут попросить принять участие в благотворительных акциях, например, пожертвовать деньги на помощь тем, кто заразился коронавирусом, пожилым людям или соотечественникам, оставшимся за рубежом. Переведенные Вами деньги вряд ли дойдут до тех, кто нуждается в помощи.

6. Ложные предложения о работе:

- Пользуясь ситуацией на рынке труда, Вам могут быть направлены фейковые предложения об удаленной работе под прикрытием корпоративных рассылок. Такие сообщения могут иметь вид приглашения принять участие в Zoom-конференции. Таким образом, мошенники заставляют перейти по небезопасным ссылкам;

- Если предложения по удаленной работе предусматривают предварительную покупку неких методических материалов, программ или инструментов, то скорее всего вы также имеете дело с мошенниками.

Несколько несложных советов, соблюдение которых поможет сохранить деньги и не стать жертвой мошенников:

- При необходимости покупки или продажи имущества через объявление в сети Интернет, постарайтесь не перечислять денежные средства в виде предоплаты, лично не убедившись о наличии данного имущества и необходимых на него документов, при этом по телефону ни в коем случае нельзя сообщать личные данные своей карты и одноразовые

пароли, в том числе совершать какие-либо операции через банкоматы «под диктовку» другого лица. Получив SMS-сообщение с незнакомого номера о том, что на Ваш счет поступил платеж, немедленно проверьте баланс.

- Не переходите по сомнительным ссылкам, которые поступают Вам в личных сообщениях в социальных сетях и не открывайте подозрительные вложения в письмах. Просто удалите их и заблокируйте отправителя;

- Обращайте особое внимание на абонентские номера, с которых приходят SMS-сообщения или телефонные звонки от лиц, представившихся работниками банка. Злоумышленники при этом используют стандартные 11-тизначные номера операторов сотовой связи, также имеют случаи использования злоумышленниками федеральных многоканальных номеров - 8-800-xxx-xx-xx;

- Мошенники часто делают ставку на общую нервозность ситуации и ждут от Вас стремительной покупки. Не верьте информации о том, что экспресс-тесты и новейшие лекарства от коронавируса можно купить в Интернете. Помните, что средств, излечивающих от нового коронавируса, пока не существует, а проходить тест необходимо при участии медицинского работника;

- Пользуйтесь только проверенными сайтами и онлайн-магазинами для покупки необходимых Вам товаров и услуг;

- Прежде чем открыть дверь незнакомцам в защитной одежде, которые представляются врачами или дезинфекторами от различных экстренных служб, уточните информацию о мероприятиях в вашем районе по номеру горячей линии штаба Рязанской области по коронавирусу:

Телефон горячей линии по номеру +7 (4912) 506-487 организован на базе больницы имени Н. Семашко и работает круглосуточно.

Также работают телефоны Роспотребнадзора: 92-98-50 и 928-930 с 9-00 до 18-00 в рабочие дни и в выходные с 9-00 до 15-00 по номеру – 92-98-07.

Кроме того, можно бесплатно воспользоваться номером 8-800-100-22-62 с 9-00 до 18-00 и в рабочие дни, и в выходные.

- Если в Вашу дверь стучатся якобы представители управляющей компании и предлагают оплатить за вас жилищно-коммунальные услуги в банковском отделении, не поддавайтесь на уговоры и сообщите о случившемся в правоохранительные органы;

- Если к Вам приходят или звонят по телефону от имени Пенсионного фонда Российской Федерации и запрашивают данные банковских карт для перевода выплат от ПФР, не разглашайте свои персональные данные третьим лицам во избежание мошеннических действий. Сообщите о случившемся в правоохранительные органы;

- Не верьте лицам, которые пытаются обвинять вас в нарушении режима самоизоляции и при этом требуют немедленно заплатить деньги. Установить факт нарушения режима могут только представители правоохранительных органов лично или с использованием специализированных систем;

- Рассылки о компенсациях за ущерб от вируса - афера. Не кликайте по ссылкам и тем более не регистрируйтесь. Сайты с приглашением на обследование - ловушка, а предлагаемая для скачивания программа - вирус. Поэтому не скачивайте и не устанавливайте подозрительные файлы с незнакомых источников;

- Если Вас призывают оказать материальную помощь пострадавшим от коронавируса или поучаствовать в другой благотворительной акции, подумайте, знаете ли Вы организацию от имени которой к вам обращаются. Если нет, то просто позвоните по официальным телефонам и уточните, проводится ли подобный сбор.

- При поступлении звонка от неизвестного лица на мобильный (стационарный) телефон о проблемах близких людей, не впадайте в панику, необходимо любым способом связаться с тем, о ком идет речь. Если с незнакомого номера с Вами начинает разговаривать родственник, но при этом у Вас есть сомнение, что звонивший действительно ваш друг или родственник, постарайтесь перезвонить на его настоящий

мобильный телефон. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

При выполнении указанных простых правил, Вы не станете жертвами преступлений, совершаемых злоумышленниками. Будьте бдительны. Проинструктируйте по рекомендациям, как не стать жертвой злоумышленников, пожилых родных, близких и друзей.

Если Вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 02 (102/112 - для мобильных операторов) или по телефону дежурной части УМВД России по Рязанской области (4912) 27-08-60.

Управление безопасности и контроля