Памятка по мошенничествам.

Мошенники наживаются на всеобщем горе и распространяя всевозможные ложные сведения. При этом они создают различные сайты якобы о том, что для получения компенсации необходимо пройти по ссылкам, ввести свои анкетные данные, зарегистрироваться и ответить на вопросы. Цель мошенников получить анкетные данные граждан, номера телефонов, данные счетов и банковских карт. Сайты мошенников создаются по стилистике схожими с государственными, к ним прикрепляются ложные положительные отзывы пользователей, как они прочитав статью получили сотни тысяч рублей, совершенно бесплатно. Комментарии довольных людей, которые оплатили комиссию и получили деньги.

Виды мошенничеств:

- гражданам зарегистрированным на портале «Госуслуг», на эл.почту жертвы приходит письмо от отправителя по имени «Гос. Услуги». Где говорится, что выписан новый штраф и посмотреть детали штрафа и номер постановления вы можете, перейдя в раздел Штрафы ГИБДД. Даже прилагается своеобразная акция, предлагающая оплатить штраф как можно скорее с 50%-ой скидкой (на это даётся 20 дней). Перейдя по ссылке, жертва попадает в фейковый сайт, вводит свои логин с паролем и потеряет деньги. Фейковый сайт «Яндекс.Денег» обозначен в адресной строке как mail.yandex-9742.ru. У настоящего Яндекса никаких лишних цифр после имени нету, он выглядит так — mail.yandex.ru. В случае блокировки мошенники в любое время создают новые адрес: mail.yandex-9743.ru, mail.yandex-9744.ru, mail.yandex-9745.ru и т.д.

- могут прийти в жилище граждан под видом врачей и предложить провериться на наличие коронавируса с помощью тест-системы. Когда наивные люди пустят их к себе домой, преступники попросту «обчистят» квартиру.

- могут позвонить любому человеку по телефону и сообщить, что тот ехал в транспорте (самолете/поезде/автобусе) с зараженным гражданином. Пока от услышанной информации человек будет паниковать, воры постараются выведать реквизиты банковской карты.

- рассылают гражданам «письма счастья» от имени Всемирной организации здравоохранения (ВОЗ), Роспотребнадзора и других авторитетных источников злоумышленники, которые содержат вредоносные файлы и программы.

- создают специальные сайты с информацией о том, как избежать заражения COVID-19, при переходе в компьютер внедряется вирус, который крадет пароли и логины от почты, соцсетей и личных кабинетов в онлайн-банках.

- организовывают сбор народных лжепожертвований, которые якобы будут направлены на борьбу с коронавирусом. Злоумышленники обещают, что

денежные средства пойдут на разработку лекарств и вакцины от заболевания, а также помощь пострадавшим от пандемии.

Как обезопасить себя от «коронавирусных» мошенников:

- не открывайте дверь незнакомым людям, даже если они представляются медицинскими работниками;
- доверяйте только официальным источникам информации (сайты Правительства РФ, Роспотребнадзора, администрации регионов, Министерства здравоохранения);
- не переходите по сомнительным ссылкам, которые могут вести на сайты злоумышленников;
- не открывайте подозрительные письма приходящие на электронную почту, не скачивайте содержащихся в них файлы;
- установите на свой ПК и смартфон хорошую антивирусную программу, которая будет блокировать переход по сомнительным ссылкам;
- **никому и ни при каких обстоятельствах не сообщайте данные своих банковских карт**;
- не поддавайтесь панике и при необходимости обращайтесь за советами к родным и близким, которые могут отговорить вас от необдуманных действий.
- не обращайтесь к гадалкам и целителям, которые обещают вам гарантированную защиту и исцеление от коронавируса.
- не покупайте товары, которые позиционируются как лучшие средства защиты от COVID-19.

Запомните!!!

Основная цель мошенников заполучить от Вас сведения о банковских счетах, банковских картах, различных кодах необходимых при проведении ОН-лайн операции по перечислению средств. Если вы назвали данные сведения по телефону или сообщили кому-либо можете считать, что подарили свои накопленные средства мошенникам, либо получили для них кредит.