

Будьте осторожны!

УМВД России и банки фиксируют несколько новых схем мошенничества, связанных с коронавирусом, с помощью которых злоумышленникам удается похитить данные и деньги россиян.

Гражданам поступают СМС-сообщения о выявленных фактах нарушения ими режима самоизоляции и необходимости оплатить штраф за данные правонарушения.

Злоумышленники предлагают получить социальные выплаты и материальную помощь, тем самым собирая информацию о картах и персональные данные.

Мошенники звонят и сообщают гражданам, что те якобы контактировали с зараженным коронавирусом и сейчас приедут специалисты для проведения анализа. Стоимость процедуры 5 тысяч рублей.

Мошенники звонят от имени работников городских поликлиник, чтобы сообщить о серьёзных проблемах по результатам анализов. Жертвы, опасаясь за своё здоровье, соглашаются на покупку дорогостоящих лекарств, которые оказываются безвредными пищевыми добавками.

Злоумышленники адаптируются и к тому, что большинство россиян теперь работает из дома удаленно. С момента начала пандемии коронавируса было зарегистрировано 1,7 тысячи новых доменов, содержащих название сервиса популярной видеосвязи Zoom, при этом 25% из них были зарегистрированы только за последние семь дней.

Основные правила, которые помогут Вам избежать обмана:

1. Не спешите. Вам предлагают сделать что-то немедленно? Подождите пару дней, вполне возможно, что интернет-ресурс, на который вас вела ссылка, уже не будет существовать.
2. Не вводите конфиденциальные данные на неизвестных компьютерах или компьютерах без антивирусного программного обеспечения.
3. Будьте бдительны. Никогда не доверяйте даже знакомым людям в

сети, может оказаться, что с вами общаются злоумышленники, а не ваши знакомые.

4. Не доверяйте малознакомым лицам, которые пытаются связаться с вами от имени каких-либо финансовых, государственных и т.п. организаций с целью уточнения конфиденциальных данных.

5. По возможности любые финансовые вопросы обговаривайте при личной встрече.

6. Не переводите деньги на малозащищённые сервисы типа «ЯндексДеньги», работа которых не предполагает глубокой идентификации пользователей (кто в действительности получил ваши деньги, никто никогда не узнает).

7. Принцип «не уверен - не делай!». Если дизайн ранее знакомого вам сайта, его работа, адрес в строке браузера или размещённая реклама отличны от привычного вам вида, ни в коем случае не вводите конфиденциальные данные.

8. Для совершения покупок в сети Интернет заведите отдельную карту с минимальным количеством денежных средств.

9. Установите запрет отправки сообщений на короткие номера. Данная услуга доступна у всех операторов.