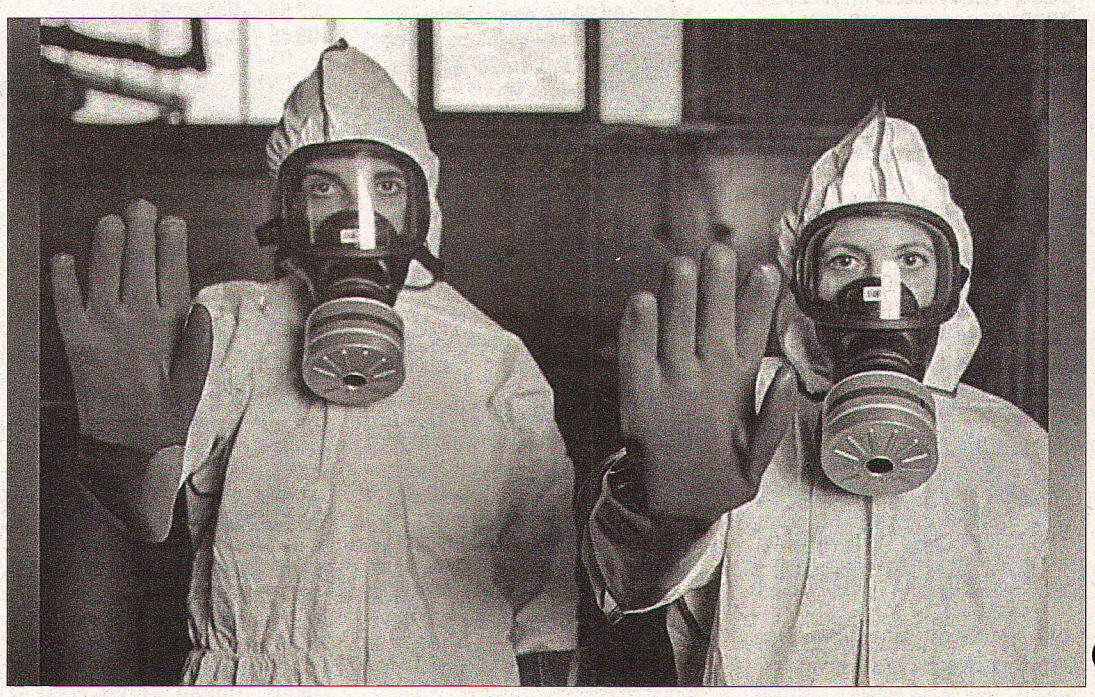
Мошенники взяли курс на коронавирус

ЛИЧНЫЕ ФИНАНСЫ

Коронавирусом решили воспользоваться злоумышленники и мошенники. По социальным сетям поползли страшилки. В одной из них рассказывается, что по домам ходят люди в костюмах химзащиты. «Говорят, что в вашем доме зафиксирован случай заражения коронавирусом, проходит дезинфекция квартир. Заходят в квартиру, усыпляют газом и выносят все из нее».



– В настоящее время в ряде мессенджеров распространяется информация о том, что в Ярославской области подобным образом действуют злоумышленники. Данная информация недостоверная и носит фейковый характер. Подобных фактов не зарегистрировано, – сообщили в региональном УМВД.

В то же время в полиции призывают граждан ориентироваться только на официальные источники информации, но при этом проявлять бдительность. Не впускать посторонних людей в квартиры и не открывать двери незнакомцам.

Свои рекомендации о том, как не стать жертвой мошенников, озвучил и Банк России. Специалисты по кибербезопасности сообщили, что злоумышленники активизируются в период каких-либо общественных волнений.

Каковы же основные крючки, на которые пытаются зацепить нас нечистые на руку люди? Об этом нам рассказал **специалист по кибербезопасности Ярославского отделения Банка России Андрей КОЦЕНКО**:

– Одна из популярных сейчас схем мошенничества основана на том, что многие люди отказались от своих поездок, путевок и сейчас ждут денежного возмещения от авиакомпаний. Преступник может позвонить, представившись сотрудником авиакомпании, и попросить сообщить данные банковской карты – якобы для возврата платы за отмененный рейс. Здесь важно понимать, что для возмещения денег перевозчикам не нужны данные карты или счета: средства вернутся на ту карту, с которой вы платили.

Банк России зафиксировал звонки мошенников и с обещаниями разного рода компенсаций, отсрочки по выплате кредитов или услуг по диагностике нового вируса. В этих случаях злоумышленники также пытаются выудить конфиденциальную информацию для хищения денег. Пожалуйста, помните: сообщать звонящим реквизиты банковской карты, CVV/CVC коды, пароли и пин-коды ни в коем случае нельзя – их всегда запрашивают только мошенники.

Но, пожалуй, самый популярный вид мошенничества в интернете – это фишинговые сайты. Сейчас они сменили тематику, адаптировались под актуальные вопросы. Злоумышленники рассылают письма с «рекомендациями защиты от вируса», призывают внести пожертвования на производство вакцины либо могут предлагать купить лекарства и дезинфицирующие или защитные средства. Такие письма содержат ссылку на поддельный, то есть фишинговый сайт.

При попытке произвести оплату на таком сайте жертва открывает доступ ко всем данным своей карты, что позволит злоумышленникам тут же опустошить счет. В некоторых случаях при посещении фишингового сайта на смартфон пользователя может быть установлена вредоносная программа, которая обеспечит мошенникам доступ к конфиденциальным данным – например, к паролю от онлайн-банка, а значит, к вашим деньгам.

Для того чтобы выманить у граждан данные банковских карт, убедить человека открыть вложение или перейти по ссылке на зараженный сайт, мошенники часто подделывают бренд и фирменный стиль авторитетных организаций (Министерство здравоохранения, Роспотребнадзор, Банк России, Всемирная организация здравоохранения и другие).

Не исключено, что тема вируса может быть использована злоумышленниками на всем протяжении пандемии, при этом возможно появление новых приемов введения граждан в заблуждение. Мошенники будут и дальше проверять нас на здравомыслие. Поэтому главный совет – не терять бдительность, не доверять подобным звонкам, письмам и предложениям, пользоваться только официальными источниками информации и проверенными интернет-магазинами. Кроме того, для онлайн-платежей стоит оформить отдельную карту и держать на ней не больше той суммы, которая нужна для конкретной покупки. И еще один крайне важный совет: установите и регулярно обновляйте на своих гаджетах антивирусную программу, которая включают защиту от спама и «фишинговых» писем.

СОВЕТЫ ОТ «СК ЯР»:

- **ПРАВИЛО 1.** Никогда не переводите свои деньги самостоятельно на чужой счет по указанию кого-либо. Заплатив таким образом якобы за товар, вы можете не увидеть ни денег, ни приобретаемой вещи.
- **ПРАВИЛО 2.** Никогда никому не сообщайте данные своей карты, свои персональные данные, коды из СМС-сообщений. Мошенник может запросить эти сведения по телефону якобы для перевода вам предоплаты. На самом деле, узнав эту информацию, он может получить доступ к вашим деньгам.
- **ПРАВИЛО 3.** Не переходите по ссылкам из электронных писем и СМС-сообщений о выгодных покупках. Поскольку один из популярных способов мошенничества – фишинговые сайты или, проще говоря, двойники официальных интернет-магазинов. Их адреса могут отличаться буквально на одну букву, поэтому обмануться легко. При этом липовый продавец крадет персональные данные посетителей или получает доступ к их деньгам на банковской карте.

Никому не сообщайте данные своих банковских карт!

Татьяна ЖДАНОВА.
Фото из архива