АКТУАЛЬНО!

«Вирусная» волна мошенничества

С подъемом заболеваемости COVID-19 в Кузбассе, как и по России в целом, активизировались мошенники. Они придумывают все новые способы отъема денег у доверчивых граждан и… добиваются своего. Можно ли не попасть на их удочку?

Традиции и новации

Наше издание уже сообщало о том, что жителям области стали звонить ушлые дельцы, предлагая купить «лекарство от коронавируса», пройти «платный экспресс-тест для выявления инфекции» или приобрести медицинские изделия, которые «помогут противостоять эпидемии».

В Москве, где эпидситуация хуже, чем в Кузбассе, а карантинные меры жестче, злоумышленники пошли дальше. С человеком связываются якобы сотрудники городской поликлиники и сообщают, что он «контактировал с зараженным COVID-19» и к нему уже едут медики для забора анализа, который нужно оплатить заранее – онлайн. Или присылают ему СМС-уведомление о штрафе за нарушение режима самоизоляции. Причем штраф требуют уплатить незамедлительно, переведя его на указанный номер мобильного телефона или же сообщив номера банковских карт, чтобы полиция могла сама снять деньги для оплаты штрафов…

В соцсетях теперь регулярно появляются посты о сборе средств на разработку вакцины против вируса, публикуемые «от имени» Всемирной организации здравоохранения.

ОКОНЧАНИЕ НА 2-Й СТР.

«Вирусная» волна мошенничества

ОКОНЧАНИЕ. НАЧАЛО НА 1-Й СТР.

А также сообщения об аттракционах невиданной щедрости – о том, например, что государство уже начало выплачивать всем желающим по 120 тысяч рублей, для получения этой суммы всего-то и надо, что указать номер своего СНИЛСа...

Чуть ли не ежедневно появляются все новые фишинговые сайты с упоминанием коронавируса в названии. Они изначально создаются для мошенничества и побуждают пользователя перейти по сомнительным ссылкам, цель которых – выманить его деньги. В «лучшем» случае человек просто оплатит онлайн покупку в несуществующем интернет-магазине. В худшем – запустит на своем устройстве установку вирусной программы, которая в дальнейшем передаст злоумышленникам пароли от всех его аккаунтов.

Все эти новые схемы действуют параллельно с традиционными уже разводами на тему «родственник попал в беду», «по вашей карте приостановлена подозрительная транзакция» и пр.

Только в конце прошлой недели пресс-служба ГУ МВД России по Кемеровской области сообщила о двух новых случаях крупных финансовых потерь у кузбассовцев. В Чебулинском районе местный житель обратился в полицию с заявлением о том, что неизвестные похитили у него 3,3 миллиона рублей. Мужчине позвонил некто, представившийся сотрудником брокерской компании, посулил ему высокий онлайн-заработок и убедил его установить на компьютер «программу для игры на бирже», а также зарегистрироваться «на площадке для торгов». В дальнейшем 61-летний пенсионер по требованию лжекосультанта вносил на разные счета крупные суммы денег, часть из которых он взял в кредит.

В Белове пенсионерке позвонил незнакомец, представившийся сотрудником службы безопасности банка, и сообщил ей о попытке несанкционированного списания средств с ее счета. Чтобы сохранить деньги, доброжелатель предложил женщине перевести сбережения на «безопасный счет», который он ей сообщит. В итоге она лишилась 750 тысяч рублей.

А в начале марта в подразделения полиции Кузбасса за один только день поступило одиннадцать заявлений о мошенничествах и три – о дистанционных кражах. Почему население продолжает упорно наступать на уже известные, многократно описанные в СМИ «грабли»? Почему охотно ведется на новые коронавирусные уловки? Что вообще происходит сегодня в обществе?

Атака на доверие

На самом деле – ничего неожиданного, мошенники всегда активизируются в смутные времена. В 1990-х годах в России поднялась первая волна финансовых пирамид. В 2008-м, когда грянул мировой экономический кризис, пошла вторая. В 2014-м – третья. В марте 2020-го, после вхождения России в пандемию COVID-19, начала нарастать четвертая. Ситуация с активным выманиванием средств у граждан также укладывается в схему «волн». Об этом журналистам из региональных СМИ напомнили эксперты вебинара «Защита прав потребителей финансовых услуг». Он проводился на прошлой неделе при поддержке Минфина и Союза журналистов России.

«Мошенники – талантливые психологи, применяющие в своей деятельности методы социальной инженерии, – прокомментировал ситуацию Тимур Аитов, заместитель комиссии по цифровым финансовым технологиям Торгово-промышленной палаты РФ. – Социальная инженерия основана на естественной склонности человека доверять другому человеку. И мошенники в данном случае эксплуатируют не глупость или необразованность жертвы, а то, что она проявляет избыточную, неуместную степень доверия».

Все атаки происходят по общей схеме. На первом этапе злоумышленник выбирает жертву, используя различные базы персональных данных, «гулящие» по черному рынку, или же действуя наугад (звонок по схеме «родственник в беде», например). Затем он входит в контакт, обращаясь к потенциальной жертве напрямую или через различные «технические прокладки» – СМС-сообщения, электронные письма и прочее. Третий этап – самый творческий: преступнику нужно так эмоционально воздействовать на незнакомого человека, чтобы тот сам перевел ему деньги либо сообщил конфиденциальную информацию о своей банковской карте и коды для подтверждения операции. Как только преступник получает деньги, он исчезает практически бесследно, ведь всё происходит на расстоянии.

В 2019 году, по данным Банка России, было зафиксировано 577 тысяч несанкционированных операций с использованием электронного сервиса платежей. В результате со счетов юридических и физических лиц было украдено 6,4 миллиарда рублей. Причем более 90% хищений со счетов физлиц совершили «социальные инженеры», сумевшие уговорить жертву совершить платеж в своих корыстных целях.

Эта новость – не только со знаком «минус», но и, как ни странно, со знаком «плюс». Ведь когда у человека в темной подворотне требуют кошелек, угрожая ему ножом, выбора, в общем-то, не остается. А дистанционные мошенники жизни не угрожают. Статистика реальных хищений не отражает статистику попыток похитить средства граждан. Их наверняка больше. Но далеко не все объекты воздействия становятся жертвами.

«Главное – взять паузу в разговоре»

В этом уверена старший психолог центра кризисных состояний города Кемерово Галина Говорова:

«В нестабильные времена стремление человека к стабильности проявляется особенно сильно. И мошенники используют эту его потребность, цепляя потенциальную жертву за живое, предлагая ей некие мифические гарантии безопасности – медицинской, социальной, финансовой... В такой ситуации человека захлестывают эмоции, разум выключается, и он начинает действовать импульсивно. Остановить его может, как ни странно, тоже иррациональное чувство – интуиция, которая всегда срабатывает автоматически.

В какой-то момент общения с манипулятором потенциальная жертва почти наверняка начинает испытывать дискомфорт – от того, что на нее слишком «давят», или с ней до приторности вежливы, или просто «что-то не так». Мошенники знают об этом и пытаются отвлечь внимание человека от странного чувства, «уболтать» его. Самый надежный и эффективный способ противостоять им – быстро завершить разговор со словами: «Хорошо, я подумаю и перезвоню».

Как только вы отключитесь от настойчивого собеседника и действительно заострите внимание на своем негативном чувстве, пытаясь понять, после каких слов оно возникло, вы тем самым включите разум. А это сразу приглушит эмоции, способные привести к необдуманным, финансово затратным поступкам».

Совет о паузе применим и в случае с предложениями из интернета. В обычной жизни мы уже научились тщательно соблюдать гигиену. В цифровом мире тоже необходим карантин. Как минимум, спросите себя: «Я слышал об этом интернет-магазине раньше? Мне попадались новости в официальных источниках о том, что каждый россиянин получит от государства по 120 тысяч рублей?» Если нет, переходить по сомнительным ссылкам и сообщать неизвестным свои персональные данные точно не стоит.

Валентина АКИМОВА.