Пандемию COVID-19 используют для массового обмана



24 апреля 2020, 08:26
Фото: Авилов Александр/Агентство «Москва»
Текст: Андрей Веселов

Эксперты по информационной безопасности и криминологи серьезно обеспокоены – в России на фоне пандемии COVID-19 возник бум интернет-мошенничества. Цифры поражают: 70% всех сайтов российского сегмента Всемирной паутины, посвященных коронавирусу, созданы преступниками. Кто и каким образом обманывает людей в интернете во время самоизоляции – в расследовании газеты ВЗГЛЯД.

«*У нас есть система, называется KSN – Kaspersky Security Network. С согласия наших клиентов нам поступают данные о киберугрозах. Это деперсонализированная статистика для анализа. Система функционирует очень давно, 10-15 лет, –* рассказывает Сергей Голованов, ведущий эксперт «Лаборатории Касперского». *– Она показывает, что уже несколько лет подряд количество атак постепенно идет на спад. Раньше шанс встретить вирус в интернете составлял примерно 70%, потом был спад, и угроза снизилась до 30%. Сейчас же, по статистике с начала марта, на волне ситуации с COVID-19 количество сообщений о том, что была встречена вредоносная программа, увеличилось на 15%*».

Что же касается случаев появления мошеннических ресурсов, то за время карантина, по данным «Лаборатории Касперского», их количество увеличилось в два раза. И ожидается дальнейший рост. Количество случаев мошенничества может «возрасти в разы». При этом, по оценкам «Лаборатории», всего в российском сегменте интернета около 70% сайтов, посвященных тематике коронавируса, являются мошенническими.

«*Коронавирус и связанные с ним общественные и экономические изменения – это предлог, которым пользуются злоумышленники. Они так делают всегда. Просто поводы были мельче*, – говорит генеральный директор компании «Интернет-розыск» Игорь Бедеров. – *Скажем, Новый год всегда провоцирует рост мошенничества со скидками. Но то, что происходит сейчас, отличается кардинально по масштабам. Мы фиксируем рост мошеннических сообщений в четыре раза, начиная с марта. Половина вообще всех мошенничеств за квартал – это кибермошенничества*».

«*Это настоящий шторм интернет-мошенничества*, – соглашается экс-сотрудник полиции и криминолог Валерий Юнусов, специализирующийся в области IT-преступности. – *Паника, неуверенность в завтрашнем дне, потеря денег: все это провоцирует даже очень адекватных людей на неадекватные поступки, и преступники этим успешно пользуются*».

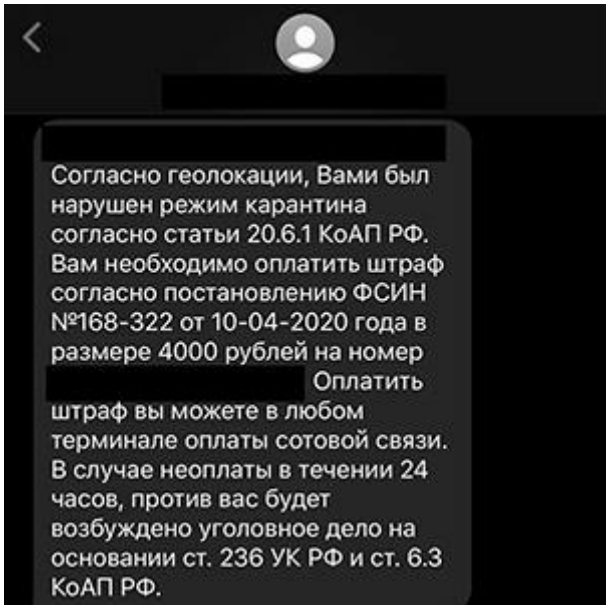
Опасения специалистов подтверждает официальная статистика МВД России. 20 апреля вышел доклад министерства о состоянии преступности в Российской Федерации за январь – март 2020 года. На общем фоне сокращения преступности (уличная преступность сократилась на 3,3%, преступность на транспорте – на 10,9%) число IT-преступлений возросло на 83,9%, мошенничеств – на 48,5%, мошенничеств с использованием электронных средств платежа – на 150,5%, преступлений с использованием или применением расчетных (пластиковых) карт – на рекордные 457,2%

«Письма для дурачков»

После того как в Москве и других регионах ввели систему самоизоляции, а следом пропускной режим, некоторым абонентам на телефоны стали поступать SMS-сообщения или сообщения в мессенджерах (чаще всего в WhatsApp или Viber) от мошенников. Неизвестные обращались к своим жертвам по фамилии и имени – а значит, имели доступ к некой базе или базам, в которых номер мобильного телефона был увязан с конкретным человеком. Время от времени такие базы «всплывают» на черном рынке.

Как стало известно газете ВЗГЛЯД, такая рассылка осуществлялась как минимум в шести регионах – в Москве, Московской области, Санкт-Петербурге, Владимирской области, Тверской области и Красноярском крае. Но, скорее всего, география шире.

В сообщении говорилось, что «согласно геолокации» человек нарушил «режим карантина» и должен уплатить штраф в размере 4000 рублей. Штраф необходимо было перевести на указанный номер телефона «в любом терминале оплаты сотовой связи». При этом мошенники ссылались на статью 60.6.1 Кодекса об административных правонарушениях («Невыполнение правил поведения при чрезвычайной ситуации или угрозе ее возникновения») и выдуманное постановление Федеральной службы исполнения наказаний (ФСИН) № 168-322 от 10 апреля 2020 года. В случае же неоплаты в течение 24 часов мошенники угрожали возбуждением уголовного дела по статье 236 Уголовного кодекса («Нарушение санитарно-эпидемиологических правил»).



Предложение заплатить штраф по телефону вряд ли выглядит правдоподобно. «*Мы называем такие сообщения письмами для дурачков, пусть несколько грубовато, но это правда. ФСИН вообще не имеет никого отношения к штрафам, а занимается тюрьмами и колониями, а неуплата штрафа не ведет к возбуждению уголовного дела, тем более через сутки*», – говорит Валерий Юнусов.

«*В случае выявления административного правонарушения, например с помощью видеокамер, постановление по делу выносится без участия нарушителя. Однако экземпляр постановления направляется лицу, в отношении которого возбуждено дело об административном правонарушении, по почте заказным письмом. Других способов предъявления административных штрафов нет*», – объясняет адвокат, управляющий партнер AVG Legal Алексей Гавришев.

Фальшивые «Государственные услуги»

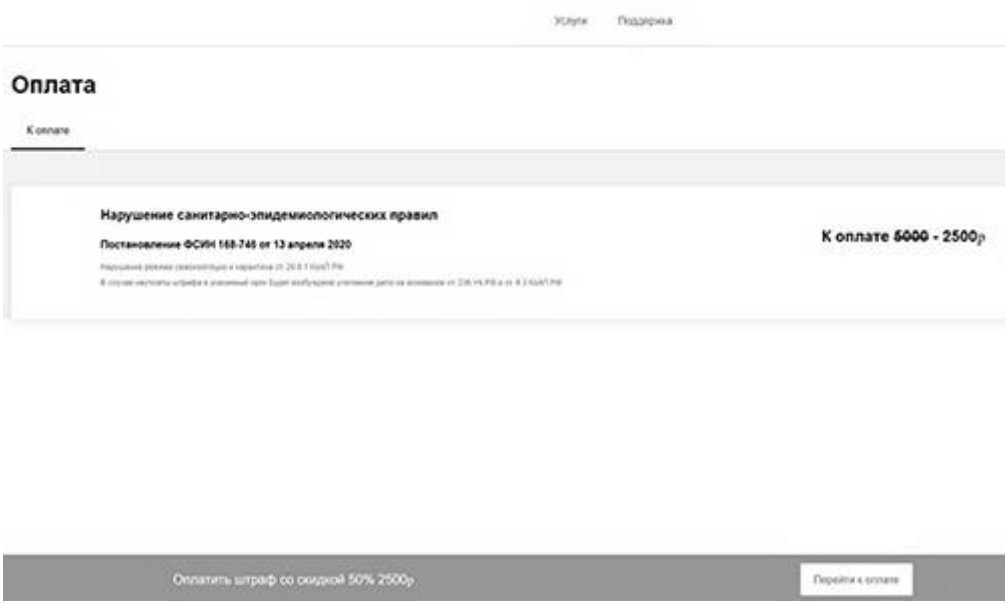
Низкий коэффициент полезного действия рассылок компенсируют масштабом. «*У обычных рассылок процент «успеха» – сотая процента. Если говорить о рассылке в социальных сетях от имени вашего друга, у которого украли логин и пароль, то это примерно один процент*, – рассказывает Сергей Голованов. – *Но низкие проценты компенсируются массовостью. Если сотая часть процента в электронных письмах приведет к необходимому результату, то злоумышленникам надо разослать десять миллионов писем, и в абсолютных цифрах это уже будет серьезный результат*».

Более изощренный тип мошенничества предполагает использование фиктивных сайтов, имитирующих фирменный стиль и образ государственных интернет-ресурсов. Например, Федеральной налоговой службы (ФНС), Федеральной службы судебных приставов (ФССП) или MOS.RU – официального портала мэра и правительства Москвы.

В компании «Интернет-розыск» корреспонденту газеты ВЗГЛЯД рассказали о копии портала «Госуслуги» – мошенническом сайте, расположенном по адресу esla-gosuslugi.ru. Мошенническая рассылка о якобы штрафе за «нарушение карантина и режима самоизоляции» в SMS-сообщениях, мессенджерах и по электронной почте

содержала ссылку на этот ресурс. Таким образом, перечислить деньги вам предлагают уже не на какой-то сомнительный сотовый телефон, а «официально» – прямо на «госпортале». Это придает схеме дополнительную убедительность.

В качестве приманки на сайте могут предложить бонус – оплату только половины «штрафа» в случае оперативного перевода денег. Например, 2500 рублей вместо 5000.



«Старый и тупой» vs «новый и продвинутый»

С мошеннической рассылкой тесно связано традиционное телефонное мошенничество. Злоумышленники могут действовать по тем же самым рецептам. «*Звонок с неизвестного номера. Вас называют по имени, отчеству и фамилии, представляются участковым, майором Дмитрием Андреевичем Истоминым, например. Какая разница? Участковых никто не знает. Говорят, вы выходили из дома, мы об этом знаем, заплатите штраф, а штраф в условиях карантина заплатите на специальный телефон МВД*», – говорит Валерий Юнусов.

«*По нашим данным, число телефонных мошенничеств за последнее время увеличилось примерно на треть. Чаще всего этот рост связан с мошенническими схемами в сфере банковского обслуживания, когда злоумышленники представляются сотрудником службы безопасности банка*», – добавляет Сергей Голованов.

Дальше возможны два варианта – «старый и тупой» или «новый и продвинутый». Используют оба. «Старый и тупой» состоит в том, что вам сначала придет SMS-сообщение, где будет сказано «в связи с подозрительной активностью мошенников во время карантина ваш счет временно заблокирован», а дальнейшую информацию можно получить по телефону «службы безопасности» – телефон в сообщении прилагается. Если вы перезвоните, то сначала на другом конце провода заиграет классическая музыка или джаз, автоответчик женским голосом сообщит, что все операторы заняты и требуется подождать минуту.

Потом трубку снимет «оператор», он же «сотрудник службы финансового мониторинга банка», который скажет, что по карте «зафиксирована мошенническая

активность, но все деньги пока на месте, не переживайте». А чтобы они и дальше были на месте, вам надо сообщить оператору данные вашей кредитной карты, включая секретный код CVC/CVV на обратной стороне. Как только сообщите – прощайтесь с деньгами.

«Новый и продвинутый» способ выглядит так: клиенту сообщают, что распоясавшиеся в эпоху COVID-19 мошенники пытаются взломать мобильное банковское приложение. Реквизиты карты никто не спрашивает, пароль к онлайн-банку тоже – это усыпляет бдительность. Жертву просто просят скачать программу удаленного доступа, например, TeamViewer или AnyDesk на свой смартфон. Дальше пользователя просят назвать номер ID программы для того, чтобы «сотрудник безопасности» смог «уничтожить вирус». Делать этого нельзя. Как только сообщите ID, мошенники подключаются к вашему устройству удаленно. Снова – прощайтесь. Не только с деньгами, но и с личными данными, паролями, логинами, почтой.

Медицинский «вездеход»

Еще одна схема – предложение оформить «безлимитный пропуск» на выход в город. «Распространенный тип мошенничества сейчас – якобы безлимитные пропуска. Такие пропуска предлагают по три-пять тысяч рублей. Например, медицинские работники могут передвигаться без преград и ограничений, мошенники представляются неким «Оператором Росгорздрава» и входят в доверие пользователей», – рассказывает Сергей Голованов.

При этом, отмечает эксперт, в этом случае не мошенники ищут жертв, а сами жертвы, обеспокоенные свободой перемещения, ищут себе «надежный» пропуск.

Такие «пропуска» предлагают по предоплате, но при этом с «бесплатной доставкой» оформить на сайте справка-короновирус.рф. Название и дизайн фейкового портала отчасти напоминают настоящий правительственный ресурс стопкоронавирус.рф.

Еще один портал расположен по адресу propuski-spravki.ru. В компании «Интернет-розыск» по просьбе газеты ВЗГЛЯД провели деанонимизацию указанного в объявлении номера. Он оказался через Skype оформленным на имя некого Виктора Ермакова, номер был зарегистрирован в Москве через оператора «Билайн». Другие данные по номеру также удалось установить. Впрочем, он мог быть оформлен по украденному паспорту.



«*Главная цель злоумышленников – кража денег под разными предлогами. Кто-то предлагает фальшивые QR-коды. Кто-то продает маски, которые никогда не будут доставлены*», – говорит Сергей Голованов.

Крупная ловля на жадность

Так называемые фишинговые сайты и фишинговые рассылки на разнообразные темы, связанные с COVID-19, множатся за последние дни буквально в геометрической прогрессии. Фишинг (от английского fishing – рыбная ловля) – это тип мошенничества, целью которого является доступ к персональным данным жертвы. Злоумышленники хотят получить несанкционированный доступ к вашим онлайн-сервисам (электронной почте, социальным сетям), а главное – к номерам банковских карт.

Несколько дней назад компания Google выпустила пресс-релиз, где рассказала, что за последнюю неделю ежедневно блокирует в своей почтовой системе Gmail около 18 миллионов фишинговых писем, связанных с COVID-19.

В таком письме может содержаться ссылка на сайт «Объединенного компенсационного фонда РФ». Дизайн и общее оформление похожи на сайт «Общероссийского народного фронта» (ОНФ). Здесь вам расскажут, что «каждому гражданину России полагается компенсация». Всего родное государство уже раздало… 39 309 144 рубля. Соответствующие поправки якобы только-только внесены в «действующее законодательство». Право на компенсацию нужно сначала «проверить», потом «рассчитать» ее размер, а потом – «по закону получить выплату на свою банковскую карту».

На портале «Фонда» у вас попросят ввести фамилию, имя и отчество, паспортные данные, адрес прописки, домашний и мобильный телефон, электронную почту. А потом – ура! виват! – вам сообщат, что вы имеете полное право на компенсацию. Мошенники уже выполнили свою первую задачу – заполучили полный набор ваших данных, на которые, например, можно оформить кредитный продукт в микрофинансовой организации. Некоторые похожие сайты для «подтверждения

личности» простят также прислать отсканированный или сфотографированный паспорт.

Теперь второй шаг – оформление «компенсации». Вы вводите данные банковской карты, на которую хотите получить эту самую «компенсацию» – мошенники получают доступ к вашему счету и уводят оттуда все, что успеют. Ваша карта привязана к телефону и требует подтверждения операций по SMS, это может притормозить аферистов, но не блокирует их. Другой возможный вариант – вам насчитают «компенсацию», но предварительно попросят заплатить «госпошлину» в размере 800 рублей.



Чуть больше доверия вызывает у жертвы двухступенчатая схема. Фишинговое письмо содержит ссылку не на сайт самого «Объединенного компенсационного фонда РФ», а на крупное медиа – например, на якобы сайт телеканала «Россия 24» (как вариант, это может быть блог известной медийной персоны). Там пересказывается вымышленный сюжет о том, что «в России запустили единую платформу выдачи денежной помощи населению во время пандемии коронавируса». В фейковой новостной статье или посте в блоге содержится ссылка на портал «Фонда». Жертва снова оказывается в ловушке. Сайт мошенников существует на нескольких десятках, а возможно и сотнях порталов-зеркал.



Ложные бизнес-партнеры

Количество веерной спам-рассылки с вирусными программами также растет. Компания Microsoft говорит, что ежедневно блокирует 240 миллионов спам-писем с вирусами, в которых упоминается COVID-19. Но даже если такое письмо попадет к вам в почтовый ящик, чаще всего почтовая программа идентифицирует его, как ненадежное, и автоматически отправляет в корзины «спам» или «мусор».

Другое дело – не «холодная», а «горячая» рассылка, когда мошенники отправляют вирусы не всем подряд, а по специально составленным тематическим спискам. В совершенно отдельной зоне риска оказались компании, занимающиеся поставками, в том числе экспортно-импортными операциями. Это для людей границы закрыты, а для грузов – нет, хотя пандемия и вносит значительные изменения в работу мировой логистики.

На волне естественных сложностей и ежедневных накладок с поставками сотрудники фирм стали получать странные письма. «*В сообщениях злоумышленники говорят о проблемах с доставкой, вызванных пандемией, в расчете на то, что получатель попытается разобраться, а о какой доставке идет речь? В других случаях мошенники давят на необходимость немедленно обработать срочные заказы, поскольку их обычные поставщики уже сорвали все сроки*», – описывает ситуацию старший контент-аналитик «Лаборатории Касперского» Татьяна Щербакова.

Главная цель злодеев – заставить получателя открыть вложение с вирусом. Типовой пример – письмо, где утверждают, что из-за пандемии китайские подрядчики не могут выполнить взятые на себя обязательства в полном объеме. Поэтому, чтобы не подвести клиентов по чужой вине, ваши партнеры срочно перезаказывают товары и уточняют номенклатуру и сроки у компании, в которой работает получатель письма.

Мошенник, который пишет по-английски и представляется Galya, запрашивает цены и условия доставки по товарам, перечисленным в приложенном DOC-файле. Когда заказов много и всех не упомнишь, человек может рефлекторно открыть файл, чтобы понять, о чем вообще идет речь. Вот только если его открыть и скачать, то на вашем

компьютере будет установлена вредоносная программа Backdoor.MSIL.Androm, цель которой – удаленный доступ к зараженной системе. Ваши данные и ваш компьютер захвачены.


Galya [redacted]
URGENT PO
Кому [redacted]
Сообщение PO.doc (0 Кбайт)

Good day,

I'm Galya [redacted]
Could you please send your best price and delivery for
the attach order,our chinese suppliers have delayed supply
of this order due to Corona virus epidemic in their cities.

Please handle as urgent.

Thanks and Best regard
Galya [redacted]
Purchase

[redacted]

Please, notice our new invoice address:

[redacted]

Пока это схема больше применяется к компаниям, работающим с внешними рынками, но если она приживется, есть риск ее распространения и на внутрироссийских поставщиков и получателей поставок.

В логове «темных сил»

Затронула пандемия и теневой интернет, так называемый даркнет. Здесь анонимно (пользователей, объединенных сетью TOR, крайне сложно идентифицировать) совершаются криминальные сделки – торгуют оружием, детской порнографией, даже заказывают убийства. Но главным образом здесь торгуют наркотиками.

Если в «светлом» сегменте Паутины активность возросла, то в «ночном» наблюдается некоторое затишье. «*Крупнейшая наркоторговая площадка в даркнете Hydra (*площадка имеет российское происхождение, здесь зарегистрированы 2,5 миллиона аккаунтов, 393 тысячи из которых совершили хотя бы одну покупку – прим. ВЗГЛЯД*)*, *приостановила продажу наркотиков на время изоляции. Цена наркотиков в России после этого пойдет вверх, и это спровоцирует рост числа преступлений*», – предупреждает Игорь Бедеров.

«Уважаемые магазины. В связи с вводимыми ограничениями в ряде субъектов вам необходимо временно снять с витрины клады, доступ к которым ограничен или будет ограничен в ближайшее время. Не создавайте дополнительных сложностей себе, покупателями и модераторам. После снятия ограничений выставите их обратно», – говорится в сообщении администрации Hydra.



При этом источник газеты ВЗГЛЯД в центральном аппарате МВД утверждает, что Hydra ситуацию с временной приостановкой наркоторговли использует для того, чтобы «закончить разработку сервисов для торговли наркотиками в Европе». «Ждем кучу запросов от Интерпола в Россию», – говорит источник.

Тем временем в европейском сегменте даркнета можно встретить объявления… о продаже крови переболевшего COVID-19 за 1000 долларов США. Плазму крови уже переболевших пациентов переливают зараженным. Однако эффективность такого экспериментального лечения еще предстоит подтвердить, клинические испытания терапии только начались. «*Сейчас люди готовы покупать все что угодно. А значит, и предложения будут самые бредовые. Все равно купят! Со временем кровь и в открытой Сети начнут продавать*», – полагает Игорь Бедеров.



Coronavirus – COVID-19

$1,000.00

I was infected with Coronavirus – COVID-19!!!

I sell my infected blood and saliva.

I do this to provide for my family financially.

Indicate how you prefer to get after purchase-Order notes (optional).

Несмотря на то, что наркотические сделки в даркнете прикрыты, здесь ведут работу по атакам на «светлый мир» – придумывают новые схемы и мошеннические рассылки.

«*Пандемия в топе, сейчас придумали попрошайничество от якобы лица ВОЗ, будут еще новации, ждите*», – заключает Бедеров.

***

Как обезопасить себя от IT-мошенников во время пандемии? По просьбе газеты ВЗГЛЯД эксперты в области информационной безопасности составили простые правила поведения. Вот они:

1. Сохраняйте общую разумность и рациональность, а также хладнокровие. Всегда перепроверяйте информацию по официальным источникам. Не стоит сломя голову оформлять себе «компенсацию за карантин», если никакой компенсации не существует в природе. Не паникуйте даже в сложной ситуации.

2. Не ищете обходных путей и «особенных» платных услуг.

3. Никогда и никому не называйте номер своей банковской карты целиком. Банковский служащий в крайнем случае спросит у вас последние четыре цифры. Решительно никогда и никому не называйте секретный трехзначный код CVV/CVC на обратной стороне карты. Если вам с подозрительным предложением позвонили якобы из вашего банка – положите трубку и позвоните в банк на «горячую линию». Ничего не настраивайте и не скачивайте на свой телефон или компьютер по «совету» неизвестных позвонивших. Всегда сами перезванивайте по проверенному номеру – в банк, онлайн-магазин.

4. Соблюдайте информационную гигиену. Не открывайте подозрительные письма и ссылки. Не переходите по ссылкам от незнакомцев. Не переходите по коротким ссылкам вида bit.ly или goo.gl (их часто используют мошенники), даже если такие ссылки приходят от друзей и коллег – созвонитесь или напишите, все уточните.

5. Будьте придирчивы и аккуратны. Обращайте внимание на адреса сайтов перед тем, как вводить свои данные. Фальшивые сайты могут выглядеть один в один как настоящие, но подделку можно распознать, если обратить внимание на адрес сайта в строке браузера. Мошенники часто регистрируют похожие имена. Например, вместо «online.sberbank.ru» можно увидеть «online.sbrbank.ru».

6. Используйте проверочные сервисы. Подозрительные сайты стоит проверять через сервис WHOIS, который раскрывает их истинных владельцев. Если по результатам проверки они оказываются скрыты, то полученной информации не стоит доверять. Также проверяйте фактическое существование электронной почты, с которой вы получили то или иное письмо. Это можно сделать, например, здесь или здесь. В идеале – проверяйте каждую подозрительную гиперссылку на наличие вредоносного содержимого.

7. Лучше используйте бразуеры Chrome, Safari или Firefox, которые уже имеют встроенную защиту от фишинга.

8. Установите на компьютер антивирусную программу и регулярно ее обновляйте. Используйте сервис «Безопасные платежи» в антивирусном пакете.

Подпишитесь на ВЗГЛЯД в Яндекс-Новостях