«Записываем вас на диспансеризацию — назовите код из СМС»

Марина, Сочи

Получила звонок в конце рабочего дня. Мужчина обратился ко мне по имени отчеству, сказал, что он из поликлиники и хочет пригласить меня на диспансеризацию. По его словам, участковый врач уже назначил мне несколько обследований, и на них можно записаться прямо по телефону.

Я решила уточнить, можно ли в один день все пройти? Он что-то проверил и сказал, что есть окошки на пятницу и к терапевту, и на ЭКГ, и на флюорографию, и на кровь.

Мне нужно было еще и к офтальмологу. Но я совсем недавно пыталась записаться и в регистратуре узнала, что врач уволился. Думаю, вдруг уже нового взяли. Оказалось, и к нему можно! Чудесным образом нашелся один свободный талончик и как раз на пятницу.

Мужчина сообщил, что закрепил за мной места. Но чтобы подтвердить запись, нужно продиктовать код из СМС, который сейчас прислали. Начал торопить меня, чтобы талоны не перехватили.

Открыла сообщение и вот сюрприз — код вовсе не для записи в поликлинику, а для подтверждения входа на Госуслуги. Хорошо, что я прочитала, кто прислал код и для чего. Назвала бы на автомате и пришлось бы потрепать нервы с восстановлением доступа к своему аккаунту. Тогда уже вместо диспансеризации нужно было талоны к психотерапевту искать.

Совет эксперта по противодействию мошенничеству:

Мошенники используют в своих схемах темы здоровья и медицинской помощи, потому что они важны для многих людей. Обманщики представляются сотрудниками поликлиник, страховых компаний или даже несуществующих государственных организаций — скажем, «Единой медицинской службы».

Начало разговора может быть самым разнообразным. Они приглашают на плановые обследования или говорят, что появился шанс записаться к врачам узких специальностей. Иногда пугают якобы плохими анализами и предлагают срочно записаться на платную программу лечения. Или убеждают, что необходимо заменить бумажный полис ОМС на электронный.

Нередко аферисты знают не только фамилию, имя и отчество, но и другую информацию о человеке. К примеру, могут назвать настоящий диагноз, фамилии реальных врачей, адрес местной поликлиники или больницы. Такие сведения мошенники находят в открытых источниках или в базах данных, украденных из поликлиник или медицинских лабораторий.

Если преступникам удается втереться в доверие, они стараются выманить у человека секретные данные. Например, код из СМС, который открывает доступ к личному кабинету на Госуслугах. Там мошенники могут получить массу информации о своей жертве — номер паспорта, СНИЛС, сведения об имуществе. Эти данные могут использоваться в других схемах, к примеру, чтобы оформить на имя потерпевшего кредиты и займы или вымогать деньги у его родственников.

Иногда мошенники сразу просят оплатить какие-то услуги и человек просто теряет деньги. Либо убеждают установить на телефон приложение для записи к врачу, а по факту это программа-вирус, из-за которой человек теряет доступ к своему устройству. И под угрозой оказываются все приложения с персональными и платежными данными, в том числе банковские.

Нельзя говорить незнакомцам данные своих документов, коды из СМС, реквизиты банковской карты или раскрывать ответ на контрольный вопрос на портале Госуслуг. Ни в коем случае не переходите по ссылкам от незнакомцев и тем более не устанавливай по их просьбе приложения.

Всегда обращайте внимание, кто вам прислал уведомление на телефон и для чего именно оно нужно. Перепроверяйте любую информацию, особенно если она касается денег. Сами свяжитесь с организацией, из которой к вам обратились. Настоящие контакты можно найти на ее официальном сайте. Обычно поисковики отмечают проверенные ресурсы галочкой.