

Ваш полис ОМС заблокирован!

Мошенничество. Как не стать жертвой телефонных аферистов

Н. Петрова, начальник отдела ООМС Новокузнецкого филиала ТФОМС Кемеровской области – Кузбасса

В последнее время в России наблюдается рост мошенничества, связанного с полисами обязательного медицинского страхования. Злоумышленники используют различные уловки и придумывают все новые схемы обмана граждан.

Они звонят по телефону и представляются сотрудниками страховых медицинских организаций или территориальных фондов ОМС, работниками регионального минздрава, специалистами портала «Госуслуги».

Уверенный голос, поставленная речь и уровень осведомленности звонящих располагают граждан к доверию. Но будьте бдительны! Это могут быть преступники, цель которых – завладеть вашими личными данными и сбережениями.

Для всех схем характерны несколько общих принципов построения диалога между мошенником и гражданином.

В начале разговора гражданам чаще всего предлагают прийти лично в страховую медицинскую организацию или поликлинику, называют адрес и режим работы учреждения, умело создавая ощущение достоверности. А затем «заботливо» предлагают облегчить процедуру и решить все вопросы дистанционно по телефону. Мошенники используют в разговоре реквизиты несуществующих законов

и нормативных актов, ссылаются на мнимые приказы Правительства Российской Федерации и администрации области, чтобы подчеркнуть официальность происходящего. Умышленно создают ситуацию срочности, подталкивая граждан к незамедлительным действиям. Человек жмет на указанные кнопки, не вникая в детали.

Распространенные схемы

«Срок действия вашего полиса ОМС истек». Для продления полиса ОМС собеседник может предложить перейти по присланной ссылке, чтобы установить на телефон приложение, например, регионального минздрава. На самом деле это вирус, который откроет доступ к мобильным банкам и личным счетам гражданина.

«Ваш новый полис ОМС готов». Гражданину сообщают о готовности нового полиса ОМС и уточняют, где застрахованному лицу удобно его получить: в поликлинике или доставить по месту работы или месту жительства. Затем просят сообщить из присланного СМС номер заказа, якобы необходимый для получения полиса ОМС. На самом деле эти цифры – код доступа к вашему личному кабинету на портале «Госуслуги». Ни в коем случае никому не сообщайте его!

«Электронный талон на обследование или прием к врачу». Мошенники предлагают гражданам записаться

на рентген, флюорографию или диспансеризацию. Подбирают удобные дату и время и отправляют гражданину СМС-код или талон о записи на мессенджер WhatsApp с просьбой подтвердить запись. После подтверждения записи преступники получают доступ к устройству гражданина и ко всем приложениям на нем.

Кроме «традиционных» кодов из СМС и переходов по ссылке, злоумышленники могут попросить сообщить девичью фамилию матери, предоставить доступ к экрану, оплатить услугу с выгодной скидкой перечислением на присланные реквизиты или номер телефона и т. д.

Перезвоните в контакт-центр

Чтобы уберечься от мошенников, запомните:

— полисы ОМС россиянам оформляются бесплатно и бессрочно, они не требуют продления;

— с декабря 2022 года оформляются цифровые полисы ОМС со штрих-кодом;

— полисы на бумажном носителе или в виде пластиковой карточки продолжают действовать и замене не подлежат;

— записаться на прием к врачу или обследование можно лично, обратившись в регистратуру поликлиники или позвонив в call-центр медицинской организации или на единый номер 122, или дистанционно – через порталы «Госуслуги» и ВРАЧ42.

Специалисты страховых медицинских организаций действительно могут позвонить с информацией о необходимости актуализировать данные полиса или пригласить на диспансеризацию, но они никогда не присылают СМС с кодами, не спрашивают ваши персональные данные, не присылают талоны на запись, не просят перейти по ссылке и перевести деньги.

Если вам поступил подозрительный звонок, прервите разговор и перезвоните в контакт-центр Территориального фонда ОМС по бесплатному круглосуточному номеру 8-800-200-6068 или в свою страховую медицинскую организацию, телефон которой указан на оборотной стороне полиса ОМС, в личном кабинете на портале «Госуслуги», на сайте ТФОМС (раздел «Страховые компании»), на сайте страховой медицинской компании. Контакт-центры страховых компаний работают круглосуточно.

IT-преступления

Хотел заработать

1,5 млн рублей потерял житель Калтана, решив попытать удачу на бирже.

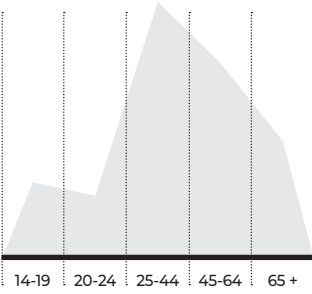
48-летний гражданин вел переписку в соцсетях с женщиной, которая рассказала, что играет на бирже и зарабатывает на этом хорошие деньги. Мужчина тоже решил увеличить свой капитал. По указанию «наставников» он скачал приложение на смартфон и под их руководством провел несколько сделок, однако вывести денежные средства не смог. По видеосвязи ему пояснили, что «необходимо совершить синхронизацию всех своих счетов по всем банкам, так как деньги будут выводиться с территории зарубежных стран». Потерпевший взял в кредит 1 300 000 рублей и стал отправлять деньги на номера неизвестных ему граждан, 200 000 рублей он перевел из личных сбережений. Возбуждено уголовное дело по ч. 4 ст. 159 УК РФ «Мошенничество».

Статистика

На 10 сентября в Калтанском городском округе зарегистрировано 84 преступления, совершенных с использованием IT-технологий. Материальный ущерб – 15 863 000 рублей.

По информации штаба ОМВД России по г. Калтану

Как обманывают мошенники

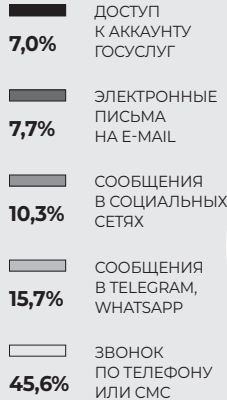


Возраст пострадавших.

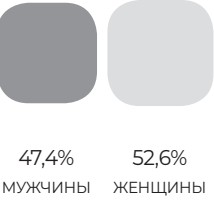
Наибольший интерес для мошенников представляют люди в возрасте от 25 до 64 лет, т. к. именно эта категория граждан часто пользуется банковскими сервисами.

Способы связи.

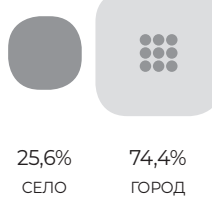
Среди способов связи с жертвами у мошенников преобладают телефонные звонки и СМС-сообщения на телефон.



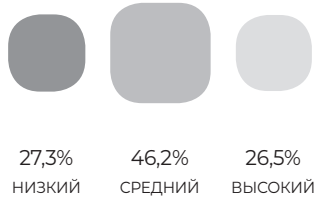
Жертвы по полу



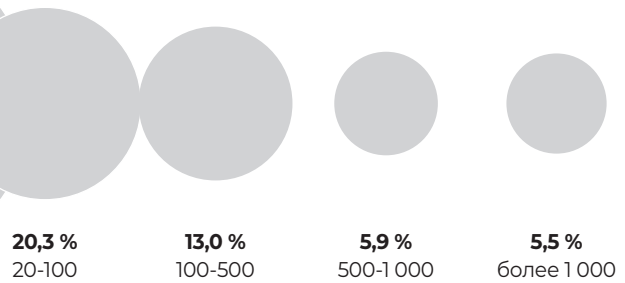
... по месту



... по уровню достатка



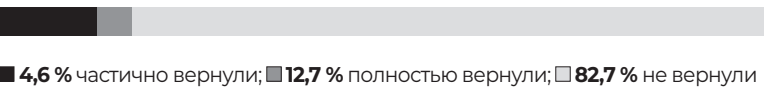
Какие суммы теряют пострадавшие (в тысячах рублей)



- 18,9 % ▶ переходили по присланной ссылке
- 15,6 % ▶ сами переводили деньги мошенникам
- 11,2 % ▶ сообщали коды из СМС от «Госуслуг»
- 10,8 % ▶ сообщали коды из пуш-уведомлений банков
- 7,6 % ▶ вводили данные банковской карты на сайте

- 6,7 % ▶ устанавливали вредоносное приложение
- 6,6 % ▶ сообщали паспортные данные
- 6,2 % ▶ вводили данные паспорта, СНИЛС на сайте
- 5,0 % ▶ сообщали данные банковской карты
- 3,8 % ▶ набирали комбинацию цифр на телефоне

Как банки возвращали похищенные деньги пострадавшим *



* Банк отправителя должен будет вернуть полную сумму украденных средств в течение 30 дней после получения соответствующего заявления от клиента-физлица в следующих случаях: если банк допустил перевод средств на мошеннический счет, который находится в специальной базе Банка России; если кредитная организация не направила гражданину уведомление о совершении перевода без согласия клиента; если банковская карта была потеряна или ею воспользовались без согласия владельца и он уведомил банк об этих фактах. Источник: Федеральный закон от 24 июля 2023 года № 369-ФЗ «О внесении изменений в Федеральный закон „О национальной платежной системе“».