«На «Госуслугах» сбой, вот резервная ссылка для оплаты коммуналки»

Ренат, Сочи

Моя мама обычно оплачивает счета за квартиру через сайт «Госуслуги». Считает, что это надежнее, чем через банк.

Недавно ей в мессенджер пришло уведомление якобы от «Госуслуг». На аватарке стоял их логотип, так что ее ничего не смутило. В сообщении было написано, что ей пришел счет за коммунальные услуги на сумму 5276 рублей. Там же сообщалось, что на портале сейчас технические проблемы и погасить задолженность можно по резервной ссылке. В качестве извинения за неудобства всем пользователям сделают скидку 30%, если оплатить квитанцию до конца дня.

Мама обрадовалась скидке, перешла по ссылке и ввела все данные карты. Как только она нажала «Оплатить», у нее зазвонил телефон. Мужчина представился сотрудником банка и сказал, что с ее карты сейчас проводится подозрительная операция – на номер счета, который в базе банка значится мошенническим. Чтобы отменить списание, нужно назвать код из СМС. Мама растерялась, увидела пришедший код и тут же озвучила его.

После этого мужчина положил трубку, а мама увидела еще одно СМС от банка: с карты сняли 20 000 рублей. Только тут она внимательнее прочитала первое сообщение с кодом – оказывается, там говорилось о подтверждении перевода денег, а не об отмене операции.

В этот момент мама позвонила мне. Я сказал ей срочно набрать номер горячей линии банка и разобраться, что случилось.

Она так и сделала. Менеджер по телефону подтвердил, что сумма действительно списалась, и предположил, что деньги ушли мошенникам. Он порекомендовал заблокировать мамину карту, чтобы преступники не обнулили ее счет полностью. Затем он посоветовал

подойти в ближайший офис банка, чтобы перевыпустить карту и подать заявление о незаконном переводе.

Совет эксперта по противодействию мошенничеству:

Злоумышленники проворачивают все более сложные схемы с помощью социальной инженерии. Маме Рената мошенники сначала написали от имени «Госуслуг» и перенаправили ее на фишинговую страницу с фальшивой формой оплаты. Когда женщина ввела данные карты, аферисты, вероятно, тут же вбили их на одном из сайтов для денежных переводов. Там понадобилось подтверждение операции – поэтому они под предлогом отмены подозрительной транзакции выманили у мамы Рената еще и код из СМС.

Мошенники могут повторно использовать реквизиты карты, чтобы воровать с нее деньги, поэтому банк совершенно правильно предложил заблокировать и перевыпустить ее.

При этом финансовые организации не обязаны возмещать потери человеку, который сам по неосторожности выдал аферистам секретную информацию. Но подать в банк заявление о незаконном переводе все же стоит. Финансовые организации отправляют такие жалобы в Банк России, который составляет единую базу данных мошеннических карт и счетов. У всех российских банков есть доступ к этой базе, и если они находят в ней реквизиты своего клиента, то блокируют ему все карты и останавливают его переводы. Чем больше заявлений от пострадавших, тем быстрее преступникам перекроют доступ к чужим деньгам.

Также маме Рената нужно обратиться в полицию с заявлением о мошенничестве. Необходимо подробно изложить все обстоятельства: с каких номеров злоумышленники выходили на связь, какую легенду использовали. По возможности приложить ссылку на мошеннический сайт и скриншоты.

Как обезопасить себя?

- Злоумышленники пользуются тем, что в мессенджерах сложно проверить, кто именно к вам обращается. Они ставят на аватарки логотипы «Госуслуг», банков или интернет-магазинов и под разными предлогами пытаются выманить деньги и реквизиты карт пользователей. Например, аферисты могут предлагать скидки на товары и услуги, обещать оформить денежные компенсации.

- Если кто-то выходит с вами на связь в мессенджере, соцсети, по электронной почте от имени какого-то ведомства, банка или магазина, лучше не поддерживайте разговор и не переходите по ссылкам из сообщений. Узнайте контакты организации на ее официальном сайте, самостоятельно свяжитесь с ней и уточните, действительно ли с вами общались ее сотрудники.

- С помощью фишинговых сайтов мошенники охотятся не только за реквизитами карт, но и за другой секретной информацией. Например, если вы по невнимательности введете логин и пароль от своего настоящего аккаунта на «Госуслугах» на поддельном сайте, то дадите доступ к своему профилю преступникам. А они могут оформить кредит на вас, используя номер вашего паспорта и другую персональную информацию.