ВНИМАНИЕ! ПОЯВИЛИСЬ НОВЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ!

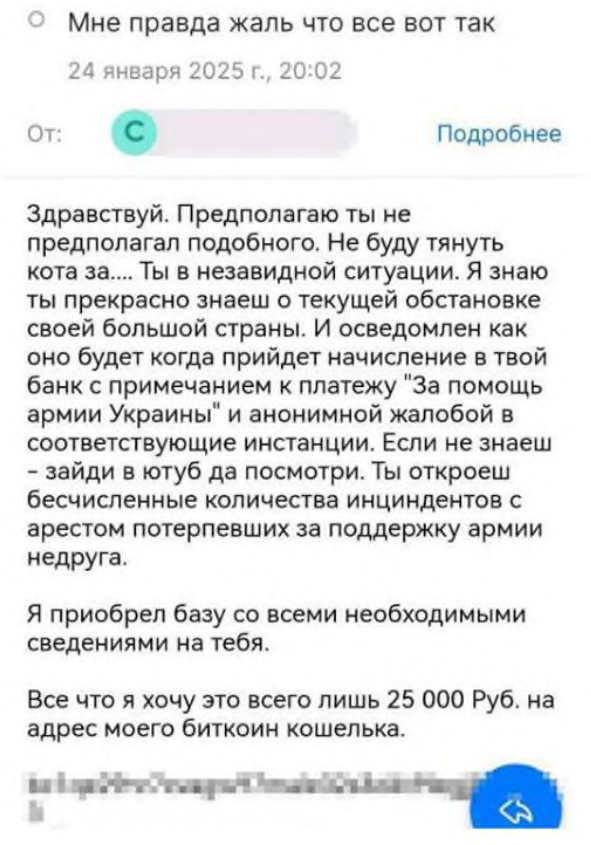
Пожалуйста! Будьте осторожны и предупредите близких!

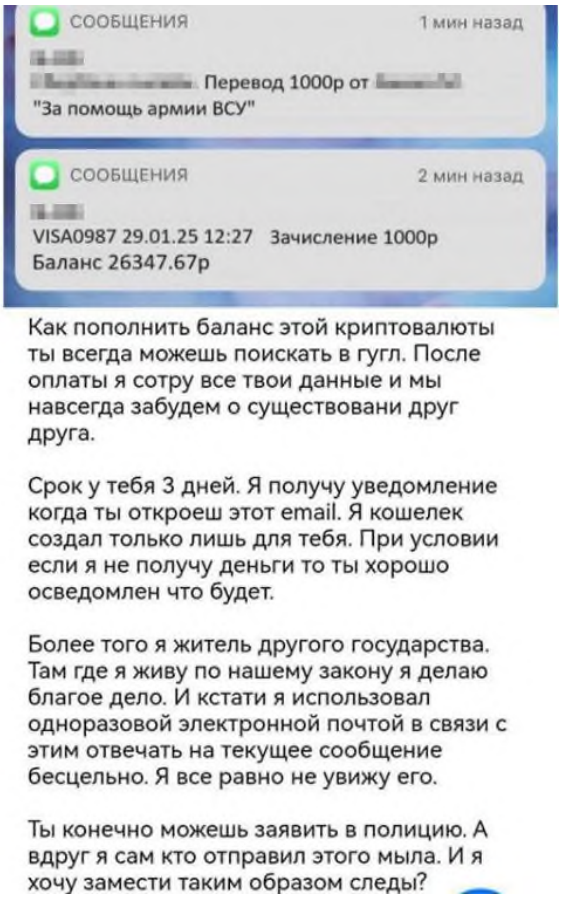
I. Угроза переводами с припиской «За помощь ВСУ»

Мошенники присылают на счет жертвы небольшую сумму денег, но с подписью «спасибо за помощь ВСУ», «за помощь ВСУ».

Затем начинают шантажировать жертву – угрожают отправить информацию о якобы помощи украинским боевикам в правоохранительные органы.

После этого злоумышленники предлагают передать им определенную сумму денег на специальный «безопасный» счет, угрожая в противном случае отправить скриншот платёжки в правоохранительные органы и обвинить в финансировании врага.





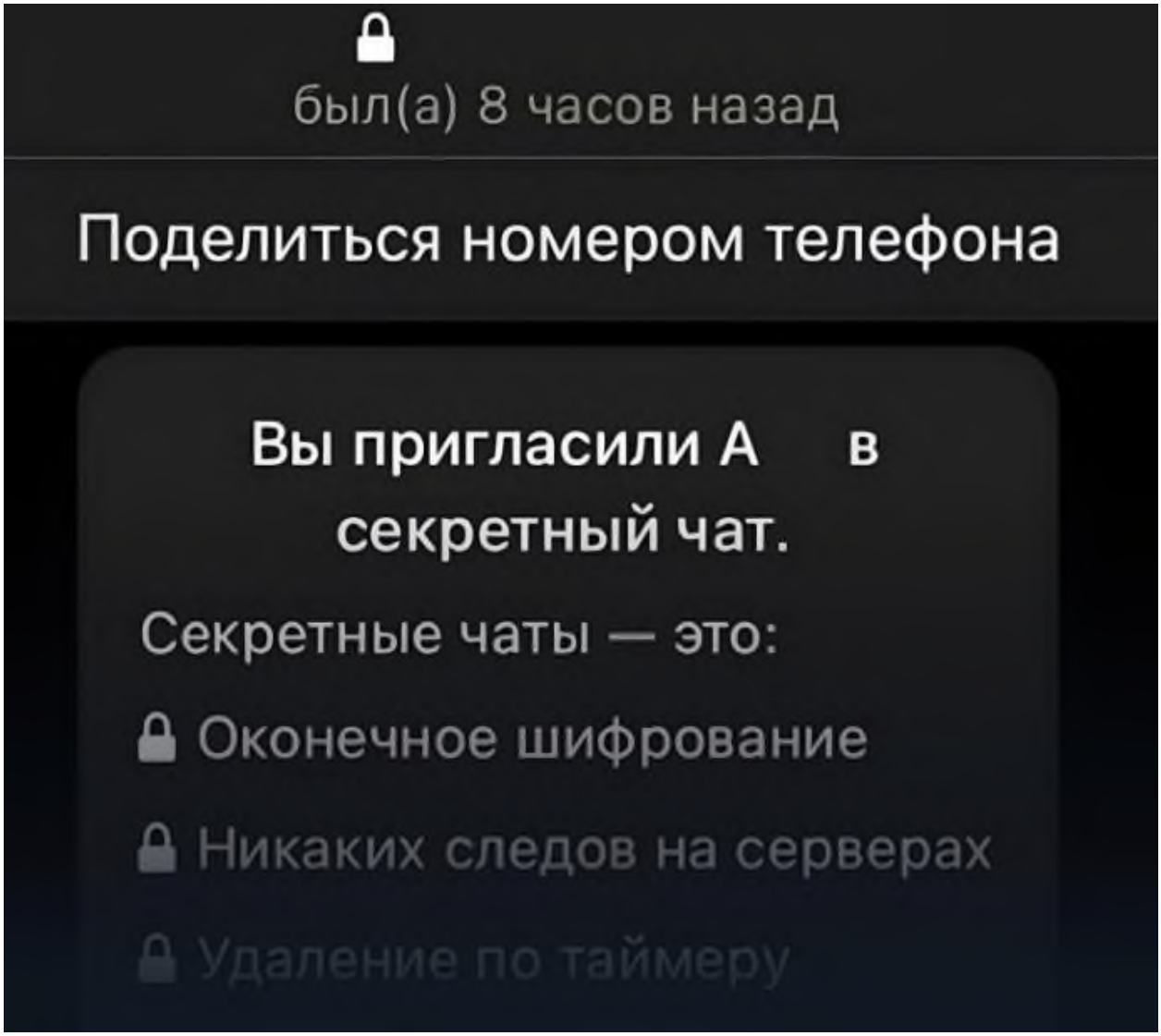
II. Новая схема кражи аккаунтов в Telegram через секретные чаты.

Мошенники якобы от лица поддержки мессенджера Telegram отправляют фишинговые ссылки в секретный чат и таким образом заполучают аккаунты жертв.

Они пишут жертвам с фейкового аккаунта «Поддержки» и сообщают о запросе на удаление профиля. Для отмены предлагают перейти по фишинговой ссылке.

После ввода логина и пароля аккаунт уходит к злоумышленникам.

P.S. Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (например, логинам, паролям).



III. Фальшивые домовые чаты

Мошенники стали активно использовать фальшивые домовые чаты как инструмент для обмана.

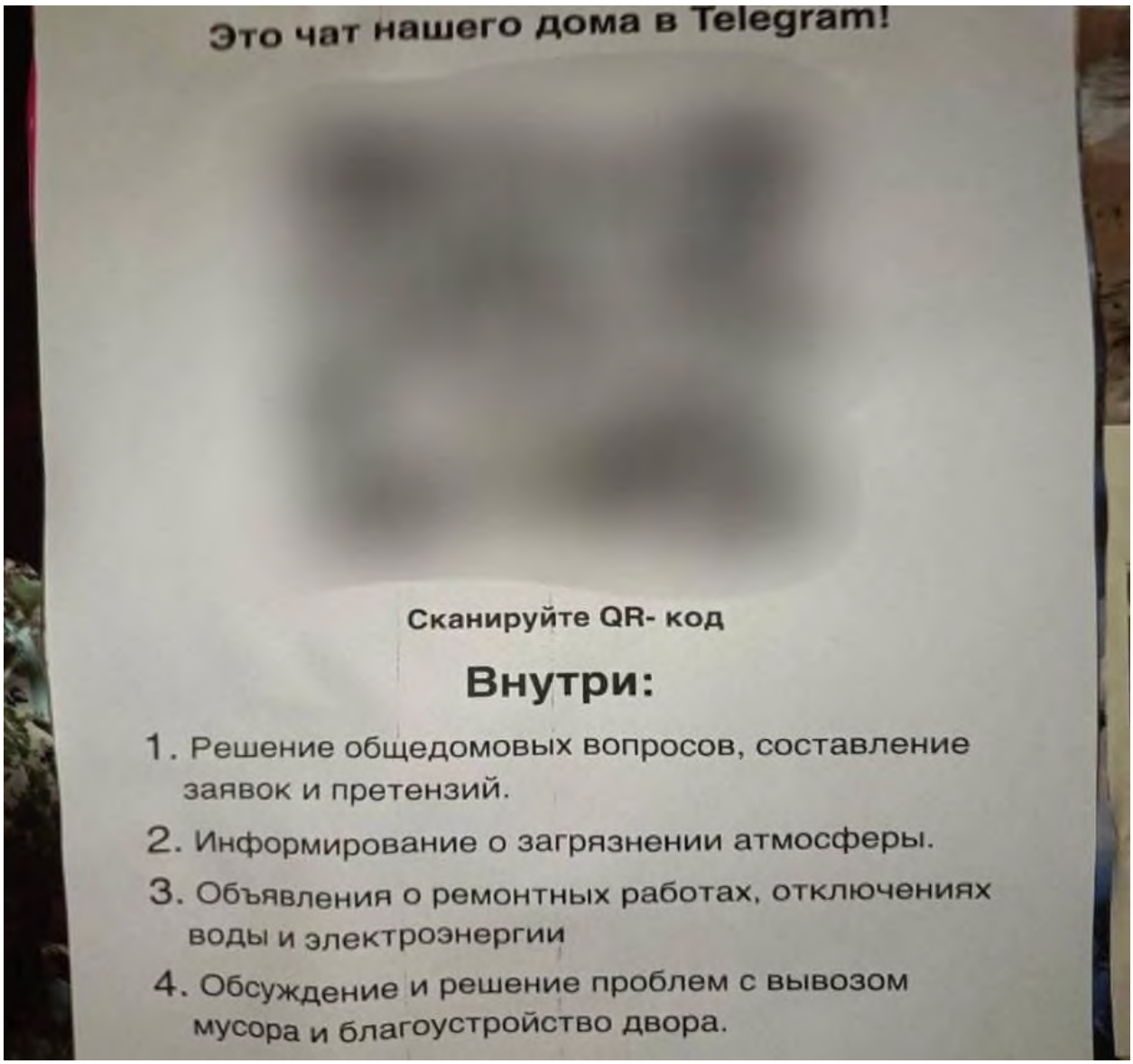
Мошенники размещают на досках объявлений в многоквартирных домах QR-коды с якобы ссылкой присоединиться в домовой чат.

На фальшивом сайте предлагается ввести личные данные, например логин и пароль от аккаунта в мессенджере либо банковскую информацию.

Основная проблема таких объявлений – их правдоподобие: люди не думают о подвохе в своем подъезде. Чтобы избежать подобных ситуаций, необходимо придерживаться нескольких правил.

Во-первых, не переходить по таким QR-кодам, если на них не указана ссылка. Не забывайте, что ссылка должна быть официальной.

Во-вторых, если вы увидели подобное объявление в своем подъезде, срочно свяжитесь с управляющей компанией или со старшим по дому, чтобы они предупредили остальных жильцов дома.

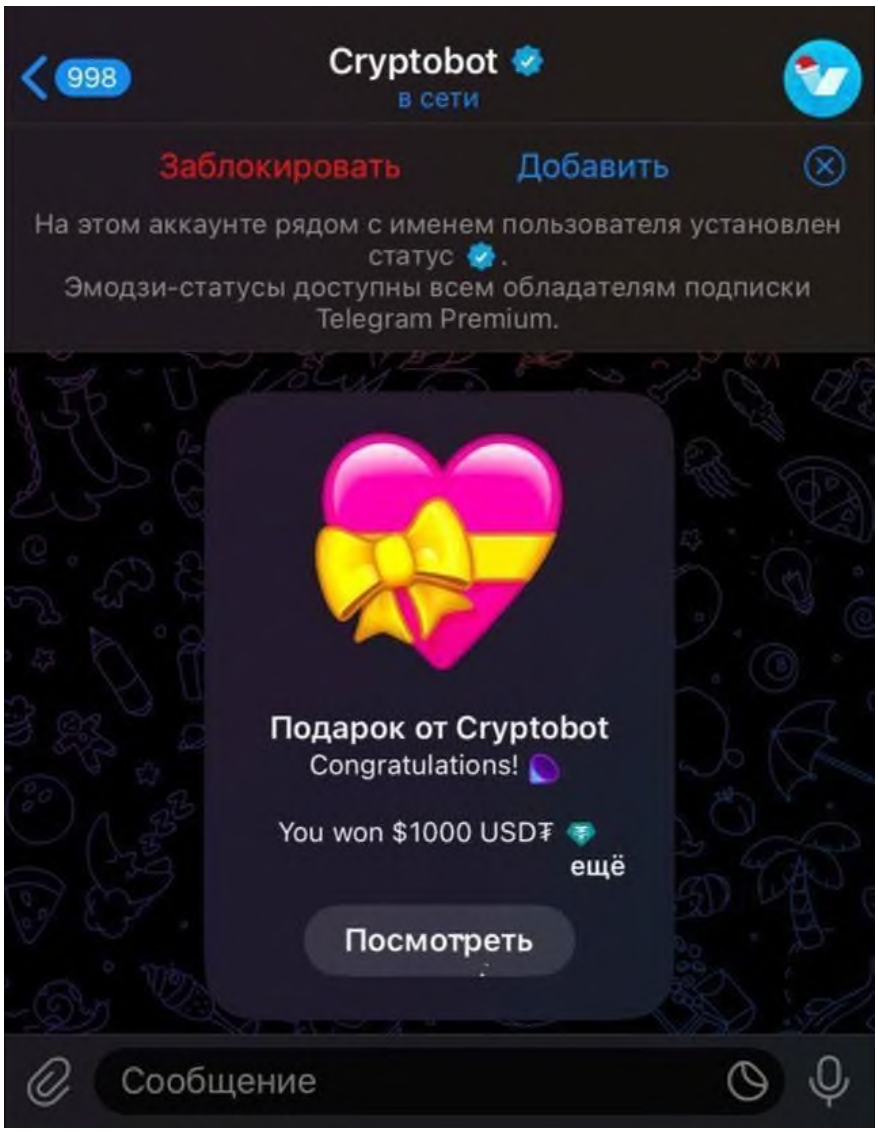


IV. Мошеннические схемы с подарочными ботами подписки Premium в Telegram

Мошенники стали массово красть Telegram-аккаунты пользователей с помощью подарков.

Под видом официальных ботов они рассылают жертвам подарки с деньгами. Забрать приз можно только после перехода по ссылке.

Однако после перехода по такой ссылке мошенники **крадут** доступ к аккаунту в Telegram, а потом и средства со счетов.



V. Опасные гифки (gif-изображения)

Мошенники используют гифки или же gif-изображения в мессенджерах – при их открытии на телефон попадает вредоносный код и собирает ваши данные.

P.S. *Гифки (gif-изображения)* –это постоянно прокручивающиеся ролики длительностью в несколько секунд.

Чтобы не стать жертвой мошенников, необходимо перепроверять «нестандартные» сообщения даже от знакомых, поскольку их могут взломать.

VI. Поддельные квитанции на оплату услуг ЖКХ

Мошенники начали рассылать поддельные квитанции на оплату ЖКХ. Такие поддельные документы стали находить в почтовых ящиках жители России.

На фальшивом бланке может быть QR-код с ссылкой на загрузку вредоносной программы. С помощью этого злоумышленники получают удаленный доступ к банковским приложениям и аккаунту на «Госуслугах» жертвы.

Человек может потерять и деньги, которые он переводит якобы за оплату ЖКХ, и все сбережения.

Мошенники кладут в почтовые ящики квитанции, которые по внешнему виду не отличить от настоящих. Одним из главных отличий таких квитанций является QR-код.

Пожалуйста! Будьте осторожны и предупредите близких!