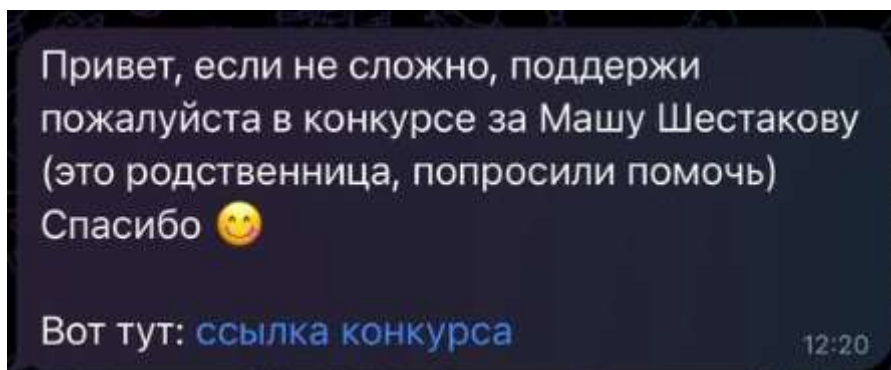


МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ: «Как обезопасить себя в мессенджере Telegram»

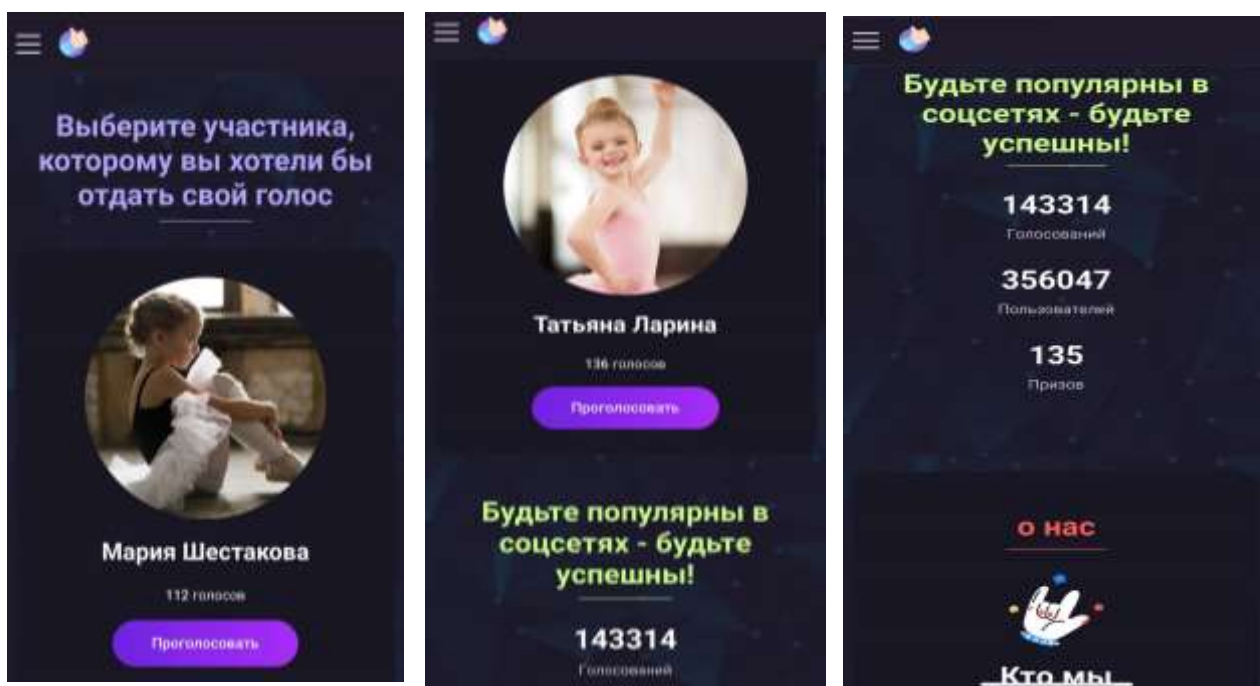
Мошенники используют новую схему кражи аккаунтов пользователей мессенджера «Telegram». Злоумышленники рассылают сообщения пользователям с просьбой «поддержать родственника (знакомого) в конкурсе».

В сообщении, пользователей просят перейти по ссылке «для голосования» (изображение 1).



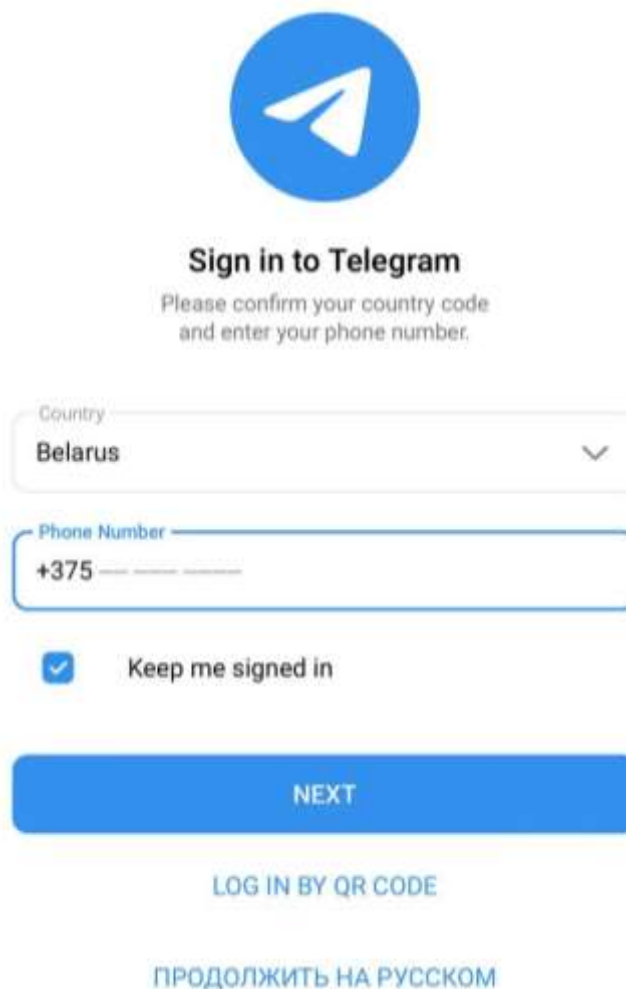
Изображение 1 (вид спам -рассылки) с фишинговой ссылкой

После перехода по ссылке, пользователь попадает на фишинговый ресурс с описанием сайта, краткой информацией о голосовании, участниках, призах, а также общей информации для голосования (изображение 2 - 4).



Изображение 2 – 4 Внешний вид фишингового ресурса

Далее, при голосовании за определенного участника фишинговый ресурс предлагает пользователю пройти авторизацию в мессенджере telegram для подтверждения якобы своей личности, где необходимо ввести свой абонентский номер, а также полученный код для авторизации (изображение 5).



Country
Belarus

Phone Number
+375

Keep me signed in

NEXT

LOG IN BY QR CODE

ПРОДОЛЖИТЬ НА РУССКОМ

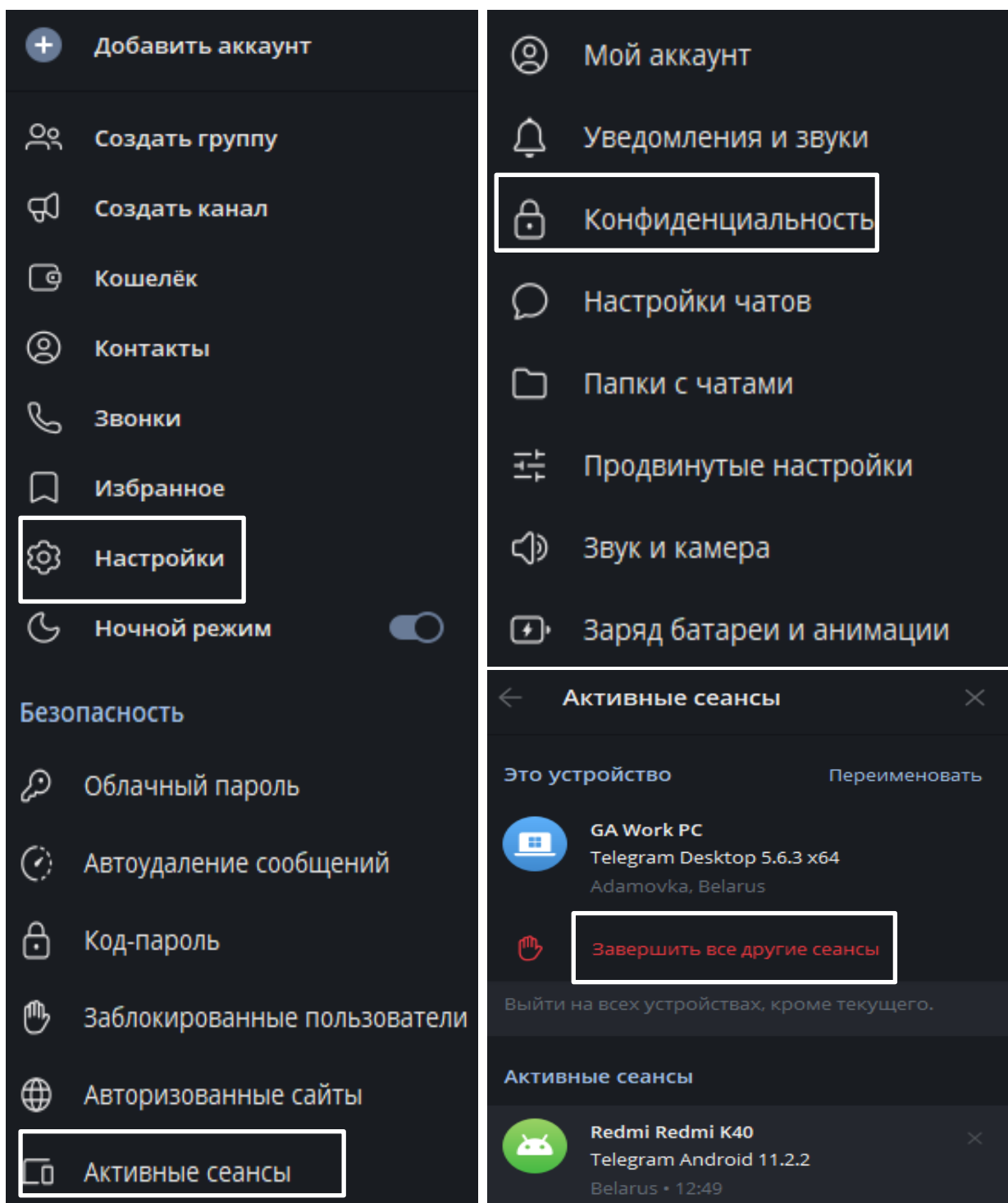
Изображение 5. Авторизация в мессенджере telegram.

Фактически, после предоставления указанных данных пользователь предоставляет доступ к своему мессенджеру, либо и вовсе теряет к нему доступ.

Основная цель злоумышленников – разослать максимальное количество таких сообщений, чтобы как можно больше людей осуществили переход по ссылкам, предоставляя таким образом доступ к своим учетным записям.

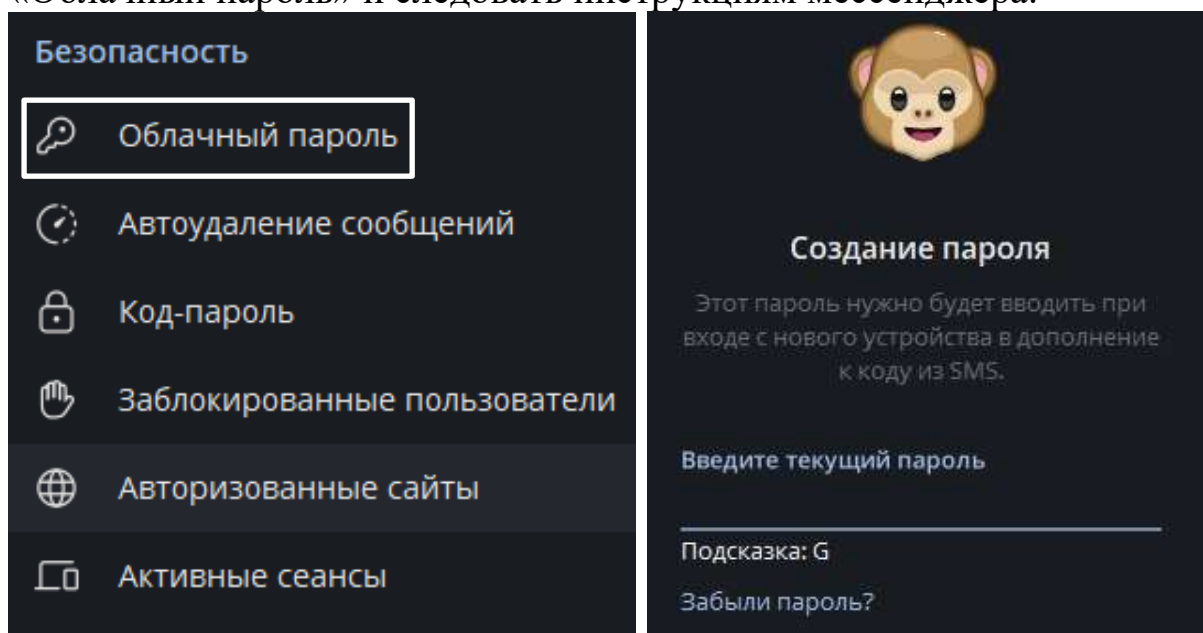
Как правило пользователь не может понять, что к его аккаунту был получен доступ, если только ему не сообщат об этом знакомые или родственники, которые получили от его имени сообщение с фишинговой ссылкой.

В случаях перехода по подобному рода ссылкам необходимо проверить о наличии доступа третьих лиц к вашему профилю. Для этого необходимо осуществить переход по следующему пути: «Настройки» – «Конфиденциальность» – «Активные сеансы» (здесь отображаются телефоны, компьютеры и браузеры, с которых входили в Ваш «telegram», а также их местоположение). После чего закрыть все подозрительные активные сеансы (изображение 6-9).



Изображение 6-9 Завершение других сеансов (сессий)

Далее необходимо установить (изменить) облачный пароль (изображение 10-11), а если его нет — задать. Для этого необходимо осуществить переход в раздел «Настройки» — «Конфиденциальность» — «Облачный пароль» и следовать инструкциям мессенджера.



Изображение 10-11. Установка облачного пароля

Если злоумышленники успели изменить пароль, необходимо произвести его сброс. Для этого необходимо осуществить переход в раздел «Облачный пароль» и кликнуть на «Забыли пароль?».

В тех случаях, когда Вами была указана электронная почта при установке пароля, то на неё адрес поступит письмо с инструкцией по восстановлению доступа (если электронную почту не указывали — пароль будет сброшен через семь дней, после чего вы сможете войти в мессенджер, закрыть чужие сеансы и поменять пароль).

Также можно связаться с технической поддержкой telegram по ссылке <https://telegram.org/support>, что позволит вернуть аккаунт в максимально короткий срок (изображение 12).

 The image shows a support form titled 'Поддержка' (Support). It has three input fields: 'Опишите свою проблему:' (Describe your problem), 'Ваш email:' (Your email) containing 'user@gmail.com', and 'Ваш номер телефона:' (Your phone number) containing '+12223334455'. Below the fields is a blue button labeled 'Отправить' (Send).

Изображение 12 Связь с технической поддержкой

Рекомендации по защите аккаунта в Telegram

Для обеспечения безопасности вашего аккаунта в Telegram, настоятельно рекомендуем выполнить следующие действия:

1. Установите облачный пароль.

Облачный пароль представляет собой надежную меру защиты, поскольку хранится в облаке, а не на вашем устройстве, что значительно затрудняет доступ к нему со стороны злоумышленников. Подробные инструкции по его установке приведены в предыдущем разделе. Обратите внимание на сложность пароля — он должен быть труднопредсказуемым.

Сохраните пароль в памяти или запишите его в безопасное место. Для удобства Telegram предложит вам ввести наводящее слово при создании пароля. При каждом входе в аккаунт с нового устройства, помимо кода, полученного по SMS, вам потребуется ввести облачный пароль.

2. Обеспечьте безопасность электронной почты.

Установите надежный пароль для доступа к электронной почте и активируйте двухфакторную аутентификацию. Это существенно снизит риск взлома вашей почты и получения доступа к кодам Telegram и другим личным данным.

3. Задайте код-пароль в Telegram.

Код представляет собой дополнительный уровень защиты вашего аккаунта в Telegram. Для его установки перейдите в раздел «Настройки» — «Конфиденциальность» — «Код-пароль» и выберите четырехзначный код.

4. Избегайте вредоносных ссылок.

Не кликайте по подозрительным ссылкам и не открывайте архивы в сообщениях от незнакомых аккаунтов — это может быть попытка завладеть вашими данными.

5. Контролируйте права доступа.

Если вы управляете Telegram-каналом, своевременно удаляйте администраторов, которые больше не работают с вами. Инструктируйте действующих администраторов о необходимости защиты своих аккаунтов, так как взлом любого из них может привести к несанкционированному доступу к управлению каналом.