О необходимости повышения бдительности при использовании мессенджеров

В последнее время участились случаи мошенничества и похищения аккаунтов пользователей в распространенных мессенджерах (Telegram, WhatsApp и др) с применением методов социальной инженерии.

Социальная инженерия - способ получения злоумышленником нужной информации или управления действиями человека без использования технических средств применяя только психологические методы воздействия на людей, убеждение, внушение доверие и хитрость.

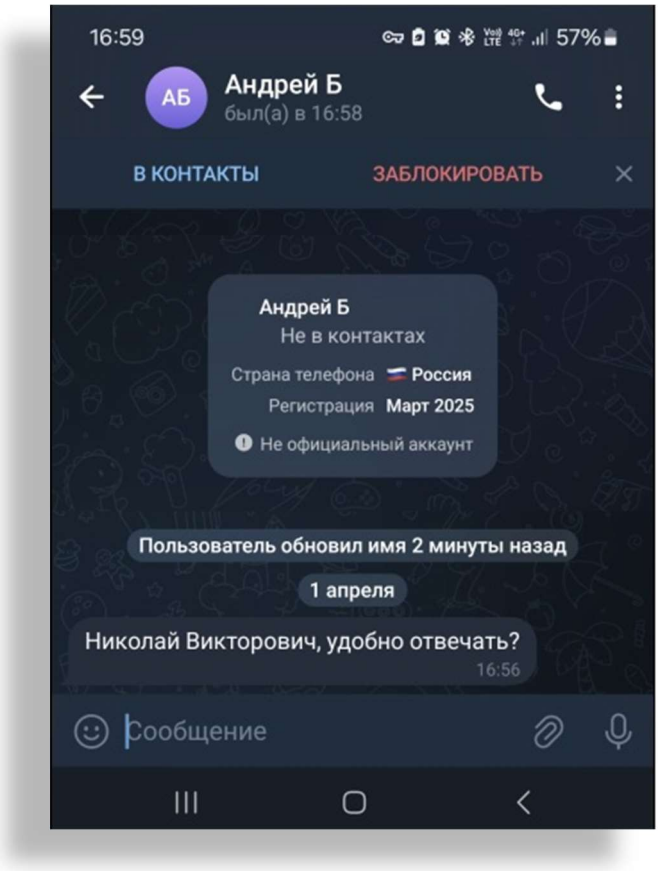
Типичные схемы атак:

Сообщения от имени «Поддельного руководителя»

Злоумышленник:

- через поддельный или взломанный аккаунт работника Общества, создает чат в мессенджере маскирующийся под чат АО «СО ЕЭС»;
- добавляет жертв в мошеннический чат, участниками которого могут быть поддельные или взломанные аккаунты;
- пишет в группе сообщение, в котором будет идти речь о проводимой проверке, в ходе которой именно вами заинтересовались соответствующие органы власти, либо обращается к Вам с заданием, к примеру, необходимо пройти процедуры — «оцифровки» и/или «актуализации персональных данных» работников, при этом подчеркивается важность задачи.

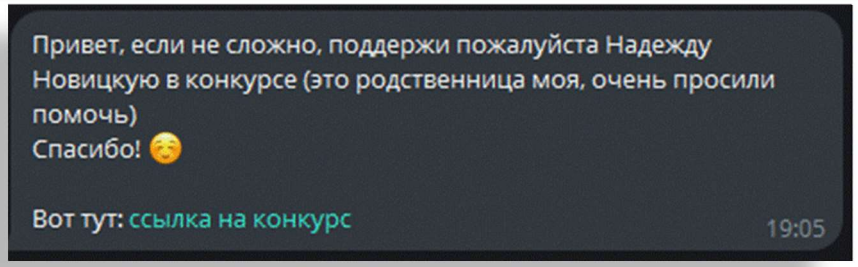
После получения информации от вас, она будет использована в различных противоправных целях. В иных случаях, может поступить звонок на мобильный телефон с попыткой получения дополнительной информации и/или угрозами и вымогательством денежных средств.

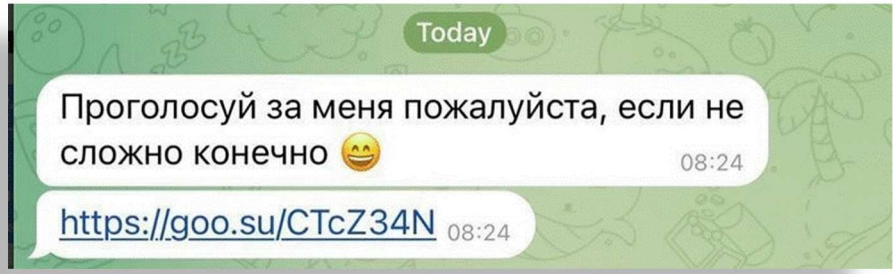


Прими участие в голосовании

Всё начинается с того, что пользователю приходит сообщение от уже взломанного знакомого. В нём он просит помочь его племяннице, проголосовав за неё на детском конкурсе рисунков. Ниже приводится ссылка на голосование.

Ссылка ведёт вас на фейковый сайт конкурса. При попытке проголосовать ресурс запрашивает у вас номер телефона и код, якобы для голосования. Если пользователь выполняет инструкцию, мошенники получают возможность войти в его учетную запись и перехватить управление.

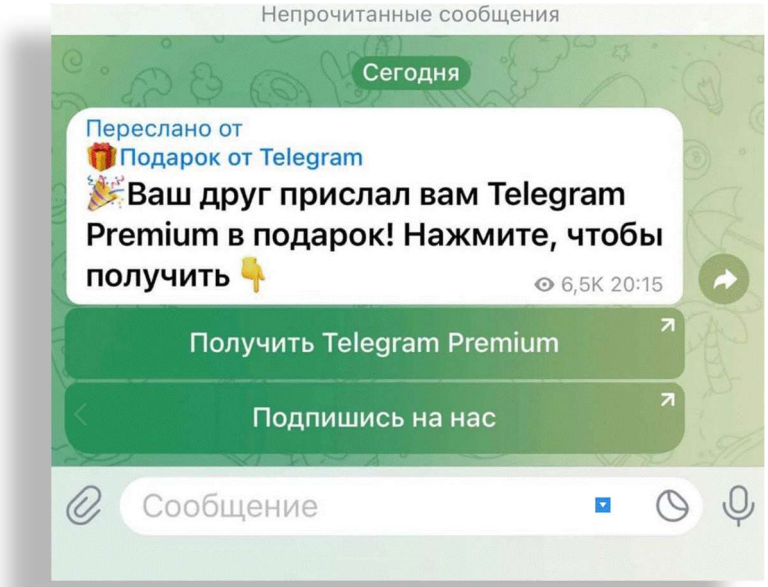




Вам прислали Telegram-Премиум в подарок

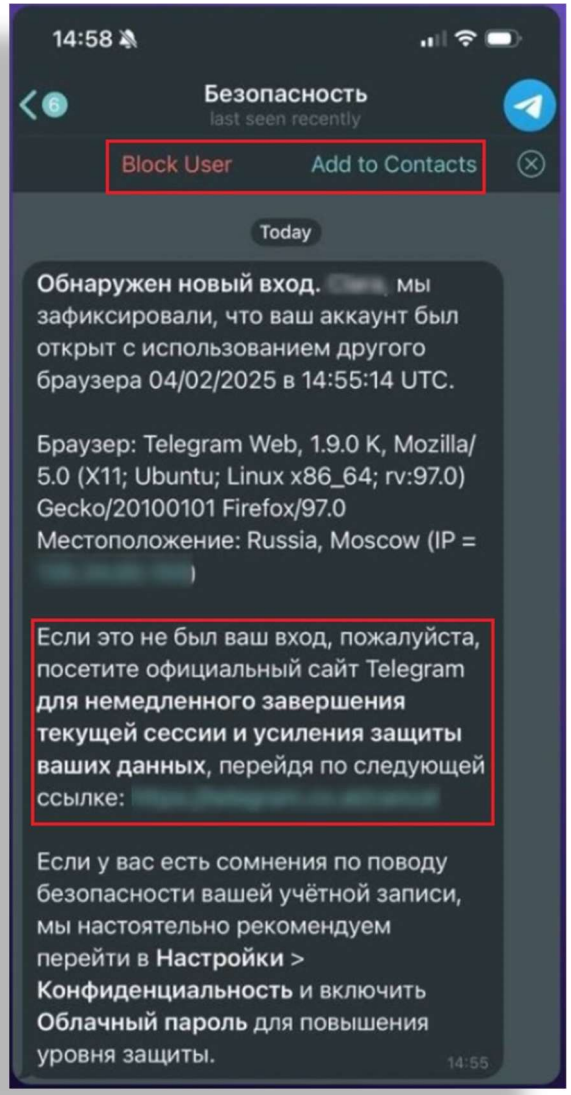
Вам в мессенджер приходит сообщение от человека, находящегося в вашем телефонном списке контактов с таким текстом «Ваш друг прислал вам в подарок Telegram Premium», сопроводив сообщение ссылкой на сторонний сайт.

Далее, происходит перенаправление на фейковый сайт с полем для ввода телефона и сообщением о том, что для получения подарка необходимо аутентифицироваться, и экран для ввода кода подтверждения, которые администрация сайта якобы выслали вам в Telegram. Если пользователь выполняет инструкцию, мошенники получают возможность войти в его учетную запись и перехватить управление.



Сообщения от пользователя «Безопасность»
Пользователи получают сообщение от пользователя с ником «Безопасность» и иконкой мессенджера Telegram или WhatsApp на аватарке. Таким образом, мошенники маскируются под системный аккаунт.

Сообщение сопровождается ссылкой, по которой необходимо перейти якобы для усиления защиты данных. При переходе по ней открывается фишинговый ресурс для авторизации в Telegram или WhatsApp с помощью QR-кода, либо через форму для ввода кода подтверждения. Если пользователь выполняет инструкцию, мошенники получают возможность войти в его учетную запись и перехватить управление.



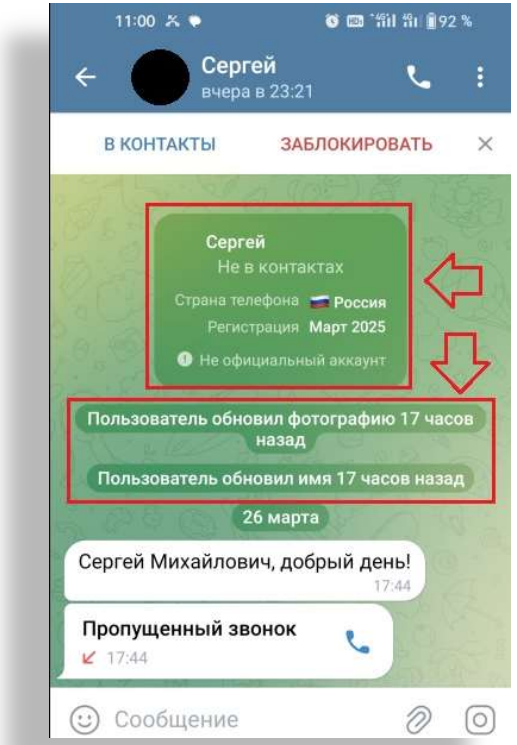
Даже если сообщения приходят якобы от знакомого человека или сервисного канала Telegram (WhatsApp и д.р.), будьте бдительны:

- не переходите по сторонним ссылкам;
- не сообщайте и не вводите на подозрительных ресурсах коды из СМС и push-уведомлений.

В актуальной версии мессенджера Telegram появилась функция, позволяющая увидеть детальную информацию об отправителе, если пользователю пишет незнакомый человек.

В чате можно увидеть:

- информацию о том, находится ли отправитель сообщения в списке контактов;
- страну регистрации телефона пользователя;
- дату регистрации;
- данные об общих группах;
- информацию о верификации (или ее отсутствии).



Памятка по настройке безопасности в мессенджерах доступны для скачивания по ссылке из QR-кода или на сайте: https://www.so-ups.ru/about/info-safe/

Способы обезопасить свой аккаунт:

- включите все инструменты безопасности в мессенджерах, в том числе двухфакторную аутентификацию и виртуальный пароль;
- не сообщайте свои данные и данные о месте вашей работы в ходе переписки, либо телефонных разговоров;
- не переходите по подозрительным ссылкам, в т.ч. и на мобильных устройствах;
- если вам написала родственница или коллега с просьбой проголосовать или поучаствовать в конкурсе — уточните по другим каналам связи так ли это;
- не сообщайте и не вводите на подозрительных ресурсах коды из СМС и push-уведомлений;
- если ваш аккаунт был взломан, первым делом предупредите об этом коллег, друзей и близких, чтобы они не стали следующим звеном в схеме злоумышленников. Далее попытайтесь вернуть контроль над аккаунтом: если аккаунт в мессенджере разлогинился, попробуйте снова войти, но, если это не получается — оперативно связывайтесь с техподдержкой мессенджера! Если все же получилось войти в свою учетную запись, то незамедлительно завершите чужие сессии и поменяйте облачный пароль.

О том, как можно настроить конфиденциальность личной информации и безопасность в популярных мессенджерах вы можете узнать в «Памятке по настройке безопасности в мессенджерах».