Департамент информационных технологий
города Москвы

# Социальная инженерия: как не попасть на удочку мошенников в мессенджерах?

[Играя на чувствах и слабостях жертвы, мошенники заставляют ее действовать в своих интересах]

# Оглавление

## 1. Основные методы социальной инженерии в мессенджерах

В настоящее время самыми популярными публичными мессенджерами в России являются WhatsApp, Telegram и Viber.

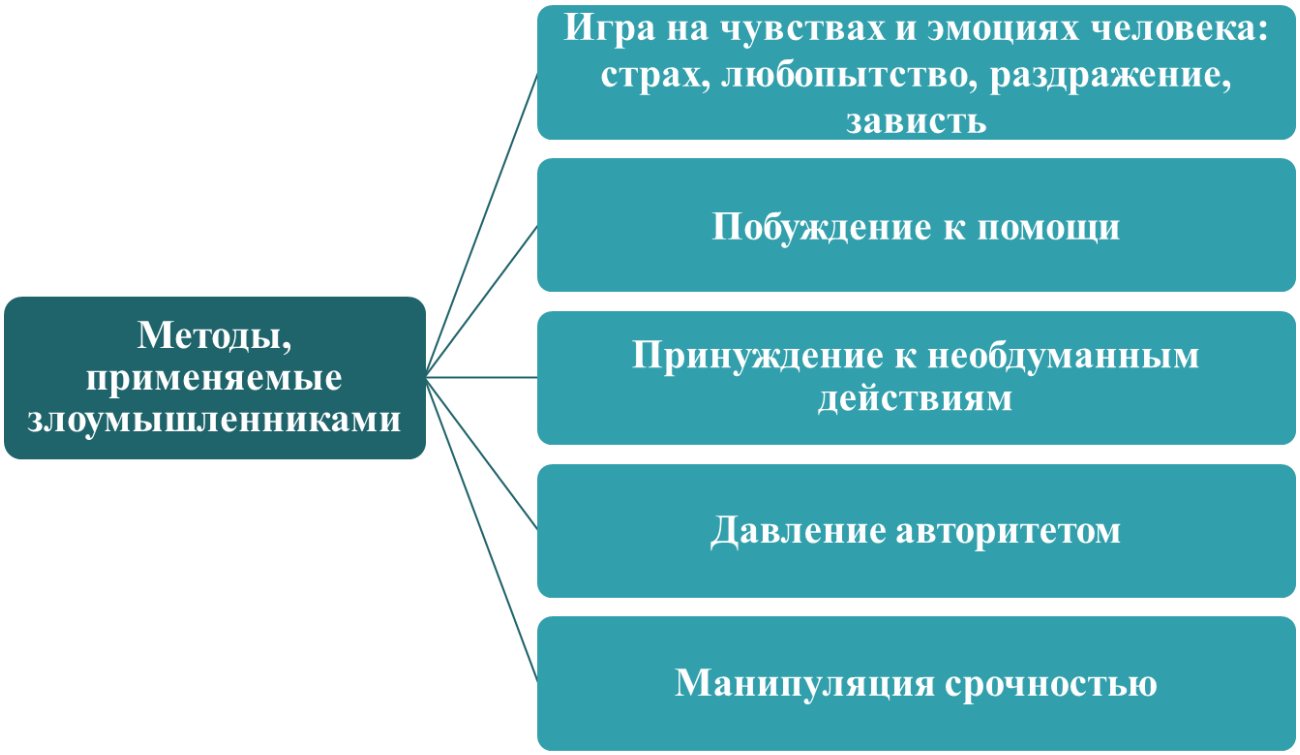
С ростом их популярности развивается и киберпреступность.

Самый распространенный метод социальной инженерии, которым пользуются мошенники – это фишинг.

**Способы фишинговых атак:**

1. Рассылка сообщений, содержащих вредоносную ссылку;
2. Рассылка сообщений с вложенными (вредоносными) файлами;
3. Сообщение от скомпрометированного пользователя из числа личных контактов (от лица коллеги, знакомого или близкого человека);
4. Рассылка сообщений от имени органа государственной власти (МВД России, ФСБ России, УФМС России и т.д.).

Мошенники манипулируют человеком, играя на его чувствах и слабостях, пытаясь получить нужную им информацию или побудить сделать что-то в их интересах.



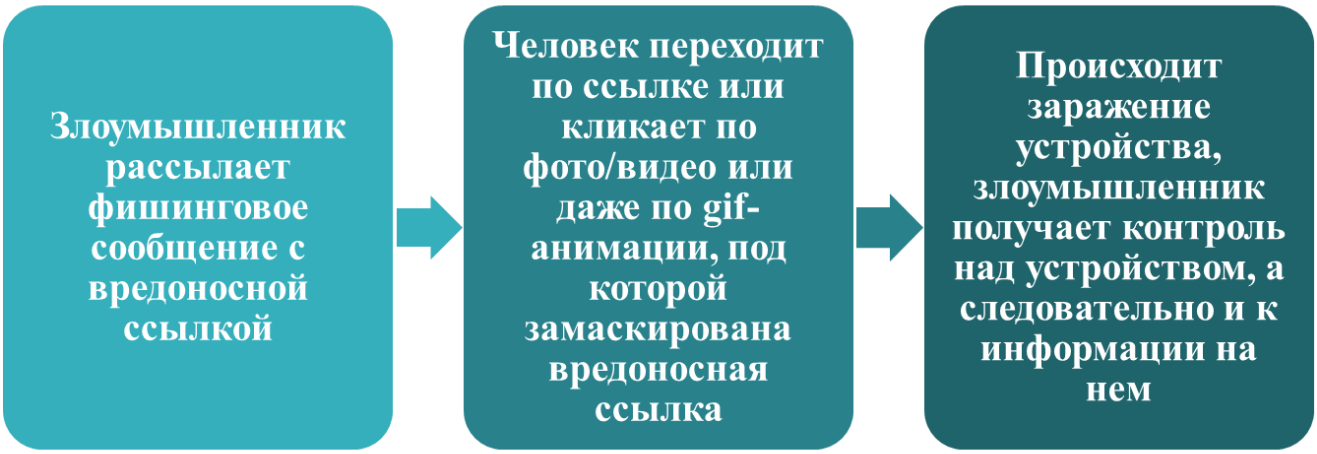

**Последствия фишинговых атак:**

- Кража личных данных (логина и пароля);
- Кража конфиденциальной информации;
- Финансовые потери;
- Подрыв репутации;
- «Потеря» контроля над устройством.

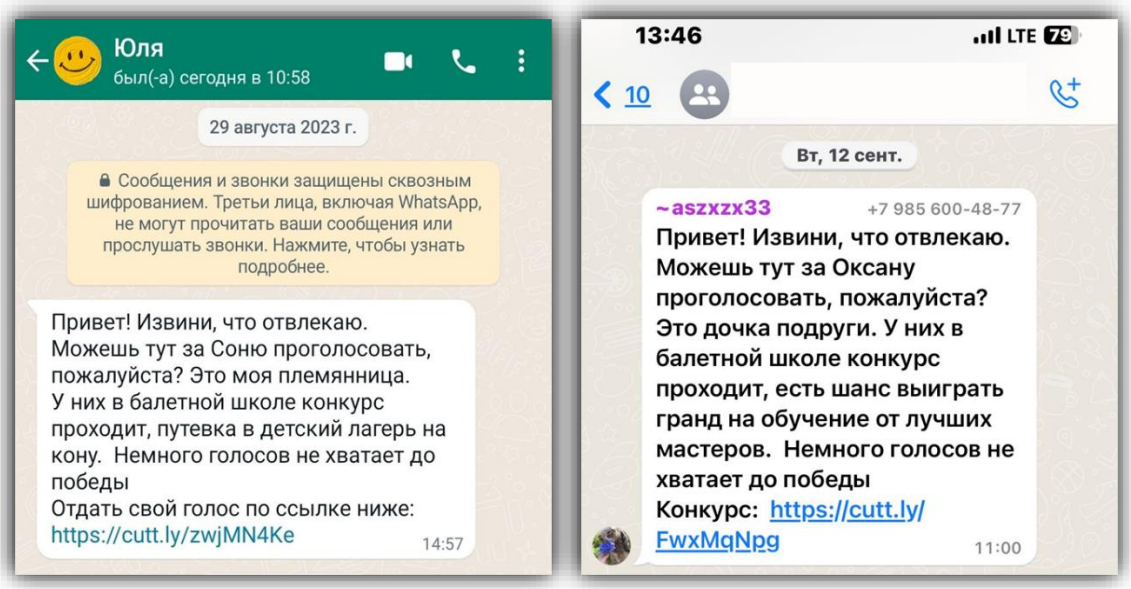
# 2. Способы фишинговых атак в мессенджерах

## 2.1. Спам-рассылка сообщений, содержащих ссылки на голосования, акции или щедрые подарки

**Принцип проведения фишинговой атаки:**



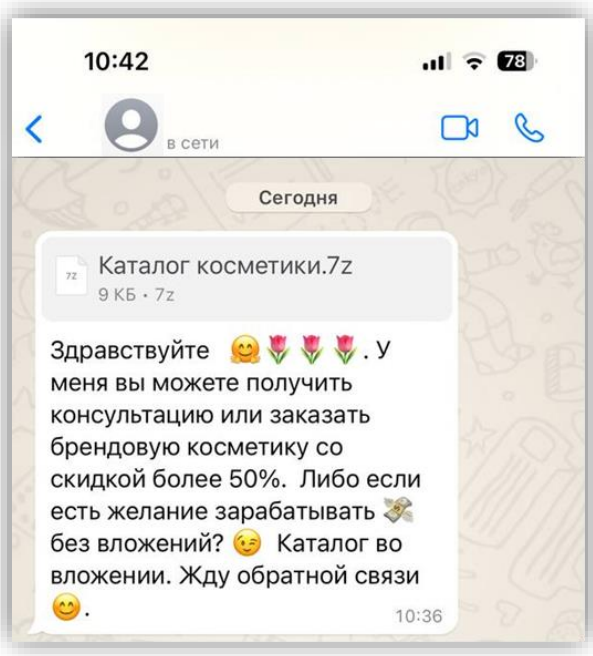

**Примеры:**

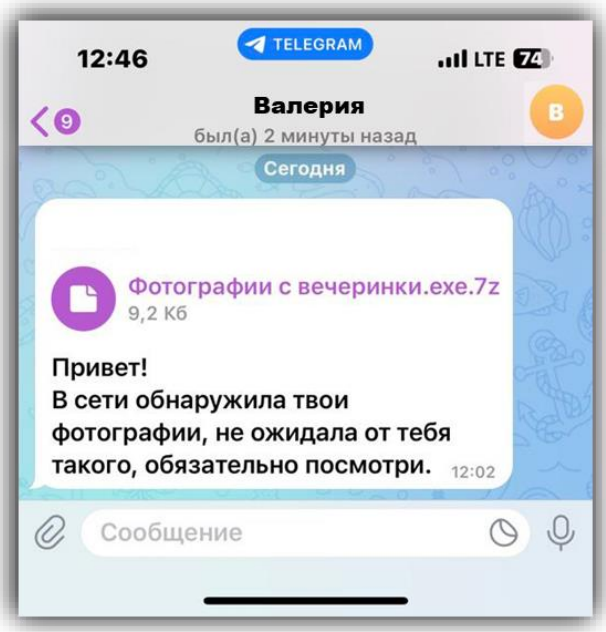


## 2.2. Спам-рассылка сообщений, содержащих вложенные вредоносные файлы

**Принцип проведения фишинговой атаки:**


**Примеры:**



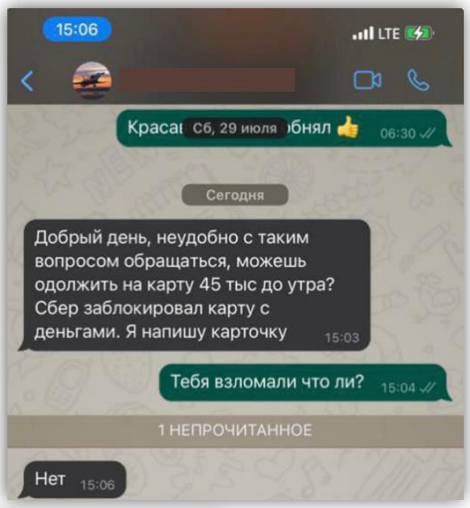
## 2.3. Отправка сообщений от скомпрометированного пользователя из числа Ваших личных контактов (от лица коллеги, знакомого или близкого человека)

**Сообщение:**

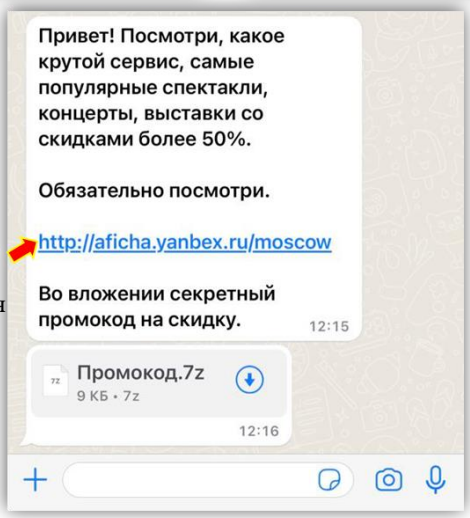
- с просьбой поучаствовать в опросе или проголосовать за него в конкурсе;
- с вложенным файлом;
- с фишинговой ссылкой на вредоносный сайт.

**Принцип проведения фишинговой атаки:**


**Примеры:**


**Ссылка-обманка** (используются похожие символы)

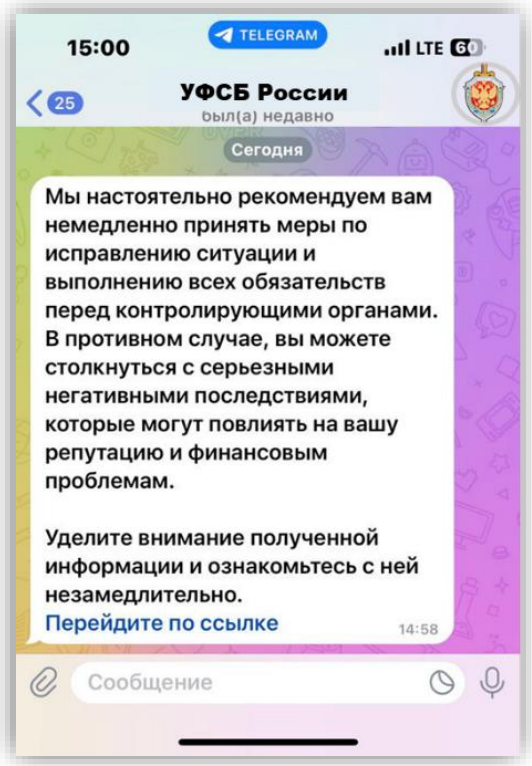


## 2.4. Спам-рассылка или персональное обращение от имени органа государственной власти (МВД России, ФСБ России, УФМС России и т.д.)

Злоумышленник пишет персональное сообщение человеку (обращается по имени и отчеству) или делает обезличенную рассылку от лица госоргана.

**Принцип проведения фишинговой атаки:**


**Пример:**



## 2.5 Сообщения от имени администрации мессенджера (Telegram, WhatsApp и т.д.)

Мошенники действуют под «маской» Telegram с целью кражи аккаунтов.

Жертвы мошенников получают сообщения якобы от Команды Телеграм, в которых предлагается перейти по ссылкам.

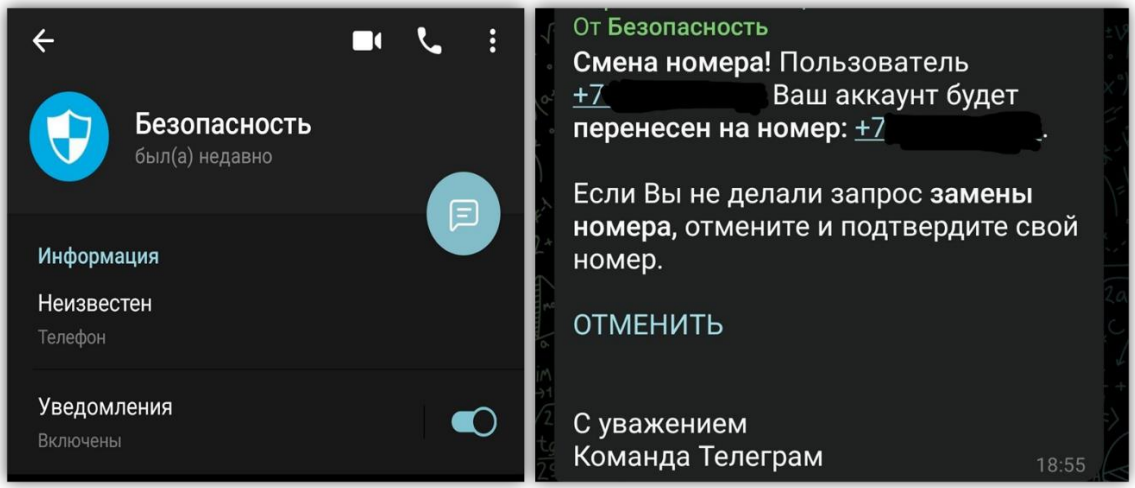
Сами ссылки спрятаны под текст: «Отменить», «Нажмите на сообщение» (под таким текстом скрываются подобные фишинговые ссылки: hxxps://telegramn[.]ru/MTgzNzU= или hxxps://telegramn[.]ru/MTg0MTI).

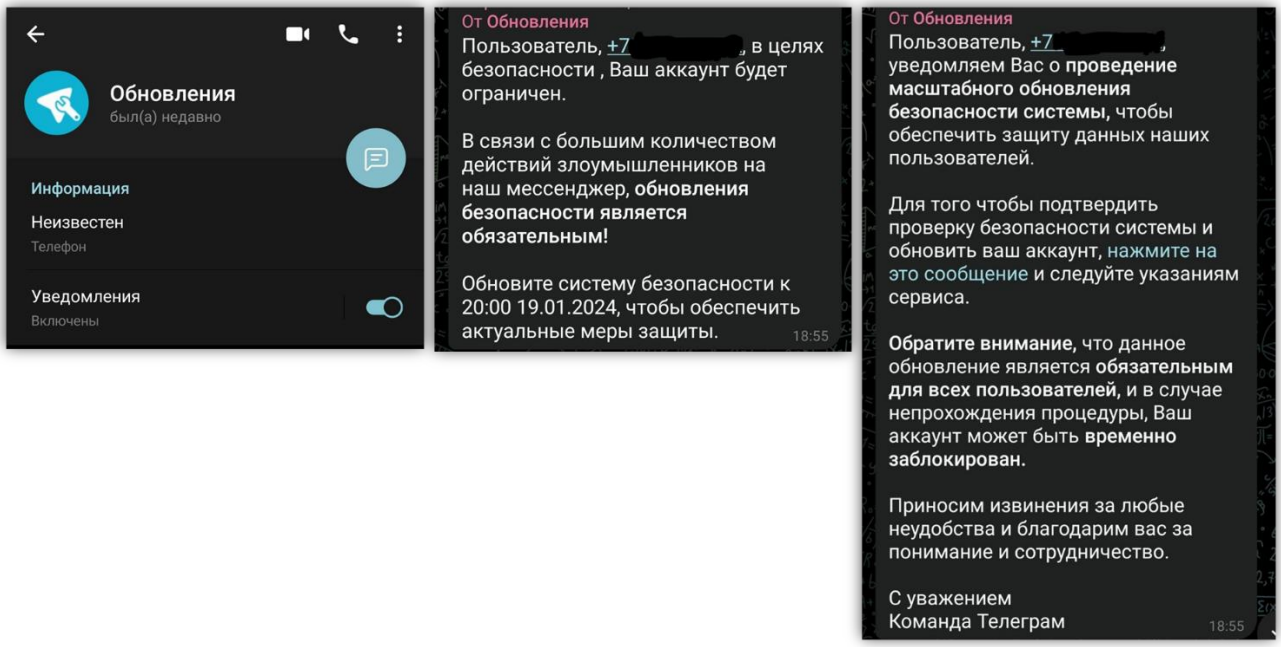
В сообщении побуждают:

- обновить систему безопасности;
- отменить привязку другого номера к аккаунту;
- обновить аккаунт и т.д.

Во всех таких сообщениях мошенники скрыто манипулируют человеком, побуждая к необдуманным действиям.

На рисунках ниже приведены примеры подобных сообщений в Telegram.



# 3. Общие рекомендации

1

**Ответьте себе на несколько вопросов:**

- **Насколько ожидаема тема или просьба, описанная в письме, нет ли в нем чего-то настораживающего?**
- **Насколько срочная просьба?**
- **Насколько непривычная ситуация описана в просьбе (например: заблокированная карта и т.д.)?**

2

- **При любом сомнении свяжитесь с этим человеком в другом мессенджере, по СМС или позвонив по телефону, чтобы уточнить действительно ли он отправлял это сообщение.**
- **Не следует продолжать переписку до получения ответа.**

3

**Дополнительно настройте безопасность своего профиля в мессенджере.**

**ВНИМАНИЕ!**

**Злоумышленники пытаются максимально расположить к себе собеседника, для этого:**

- **подменяют номер телефона на официальный** *(например, при входящем звонке отображается телефон ФСБ России и т.д.)*;
- **направляют фото якобы своего служебного удостоверения;**
- **используют официальную символику органов государственных власти** *(например, при входящем звонке отображается геральдический знак – эмблема ФСБ России и т.д.)*.
- **направляют от имени органа государственной власти якобы официальные обращения, заверенные подписью и печатью руководителя, в которых сообщают:**
  - о голосовом согласии в сотрудничестве с органами государственной власти;
  - о том, что вы являетесь подозреваемым (обвиняемым);
  - об установлении в отношении вас факта мошеннических действий;
  - о необходимости выполнения процедуры обновления единого лицевого счета;
  - о необходимости получения кредита и перевода денег на «безопасный счет» или передачи их курьеру и т.д.

**ВАЖНО ПОМНИТЬ!**

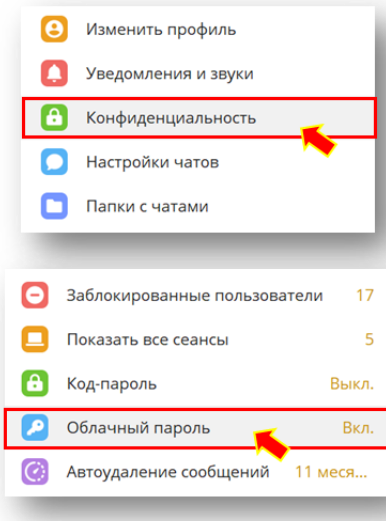
- ✓ **Уведомление гражданина органы государственной власти осуществляют лично ИСКЛЮЧИТЕЛЬНО В ПИСЬМЕННОМ ВИДЕ И ВРУЧАЮТ ЛИЧНО.**
- ✓ **Сотрудники органов государственной власти НИКОГДА НЕ ПРИСЫЛАЮТ гражданам копии своих служебных удостоверений.**
- ✓ **Органы государственной власти НЕ ИСПОЛЬЗУЮТ личные сбережения или кредитные средства граждан для оказания помощи оперативным подразделениям в предупреждении и раскрытии преступлений.**
- ✓ **Официальные телефоны органов государственной власти используются ИСКЛЮЧИТЕЛЬНО ДЛЯ ПРИЕМА ИНФОРМАЦИИ от граждан и организаций.**

# 4. Настройка безопасности личного профиля в мессенджере

## 4.1. Настройка двухфакторной аутентификации в Telegram

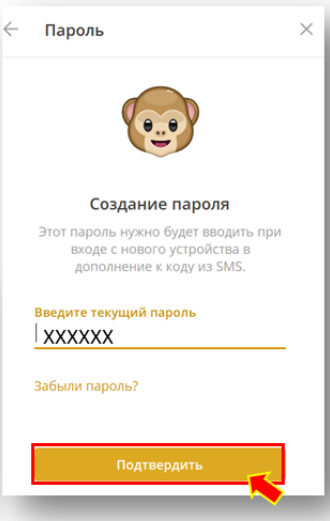
Перейдите в Настройки, выберите раздел Конфиденциальность и там кликните на пункт Облачный пароль

1



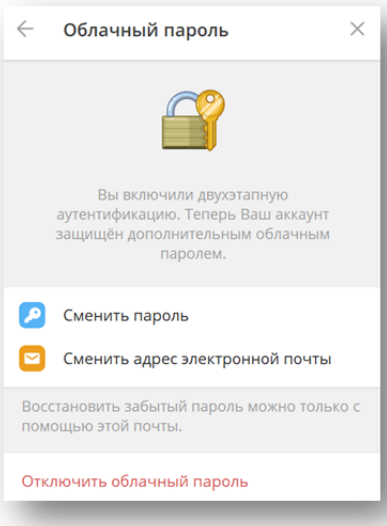

Сгенерируйте безопасный пароль и нажмите Подтвердить

2




Двухэтапная аутентификация включена

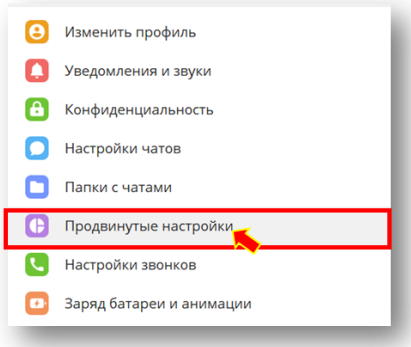
3




## 4.2. Отключение автоматической загрузки медиа файлов в Telegram

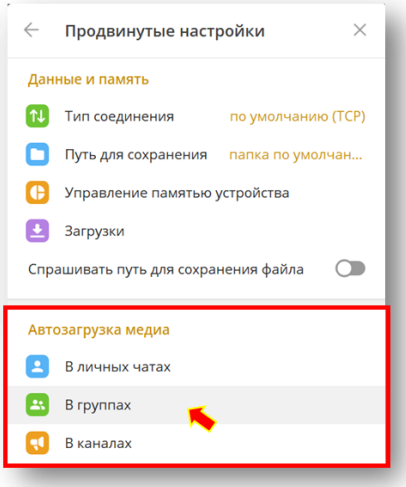
Перейдите в Настройки и выберите раздел «Продвинутые настройки»

1



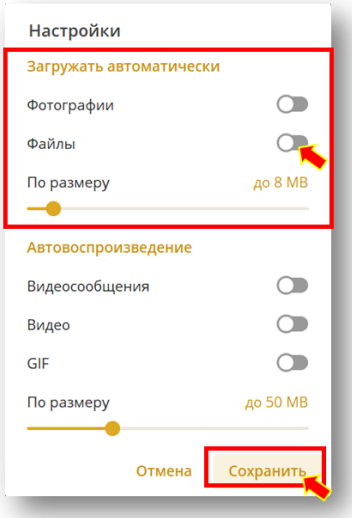

Выберите один из пунктов в разделе «Автозагрузка медиа»

2




Настройте автозагрузку в подразделе, переведя бегунок в левое положение. Нажмите кнопку «Сохранить»

3



## 4.3. Настройка конфиденциальности в Telegram