1. **Использование мессенджеров**

Общение в мессенджерах стало настолько привычным, поэтому мы зачатую без каких-либо сомнений делимся в чатах своими персональными данными и, возможно, даже реквизитами банковских карт. При этом остаются сомнения в том, насколько надёжно защищена переписка в мессенджерах. Что произойдёт, если доступ к ней получат посторонние лица?

1. **Настройка безопасности данных**

Критерии, по которым можно определить, насколько

безопасным является тот или иной мессенджер:

**2.1.** **Исчезающие сообщения.** Возможность отправлять сообщения, которые автоматически удаляются после их прочтения или по истечении заданного срока предусмотренав большинстве программ.

**2.2.** **Поддержка двухфакторной аутентификации.**

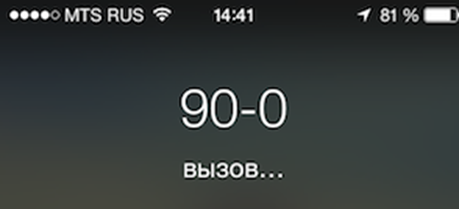
При активизации двухфакторной аутентификации требуется дополнительно вводить пароль или код из СМС-сообщения для получения доступа к приложению. На некоторых устройствах может быть доступна функция разблокировки при помощи биометрических данных (отпечатка пальца или распознавания лица).

1. **Угрозы, связанные с**

**использованием мессенджеров**

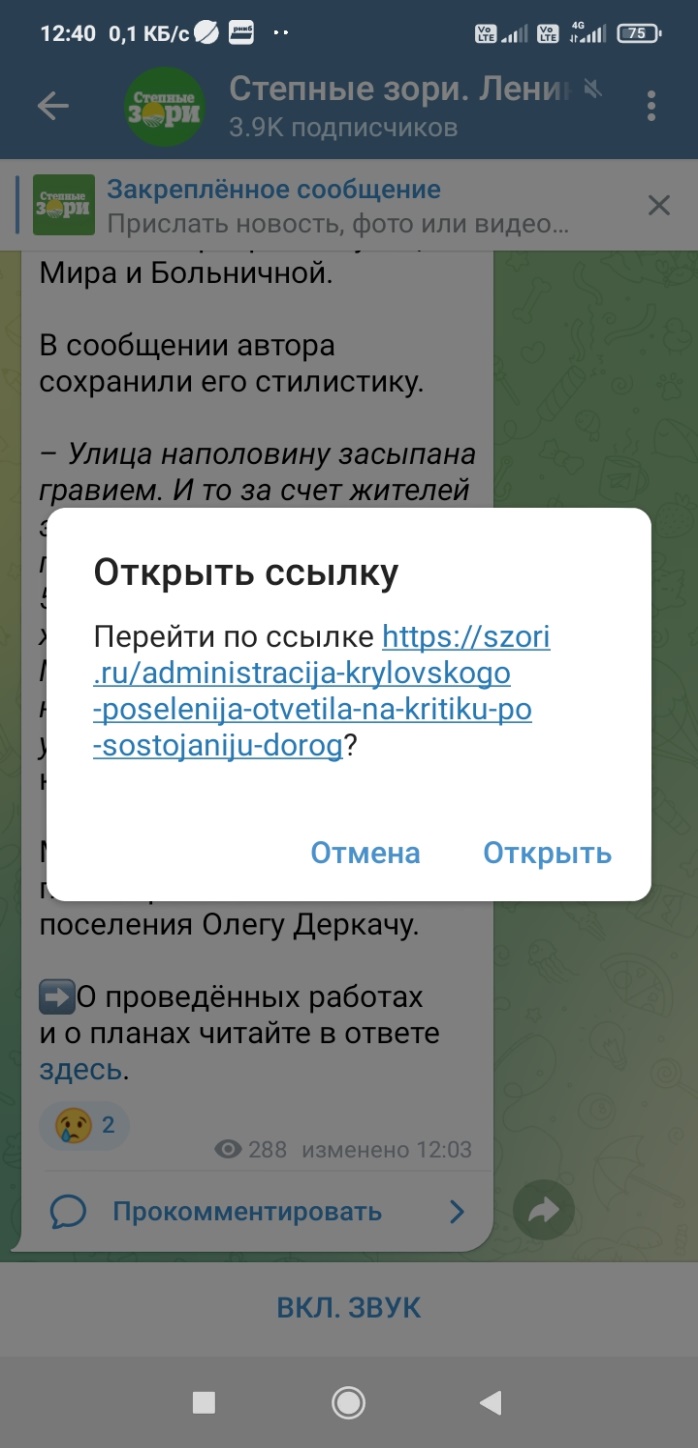
Приложения мессенджеров активно используют злоумышленники, чтобы похищать персональные данные, личную информацию и реквизиты банковских карт. Для этого они эксплуатируют уязвимости приложений, применяют методы социальной инженерии, рассылают фишинговые сообщения.

**3.1. Вредоносные ссылки и файлы**. Злоумышленники используют методы социальной инженерии, чтобы побудить жертву открыть файл или ссылку. Зачастую они представляются сотрудниками банка, подделывая на заставке названия и «аватарки». Например, Вам в мессенджер может поступить сообщение якобы от «Сбербанка» с номера 900, при этом вместо нулей будут использованы буквы **«О» – 9ОО** или номер записан с использованием знаков препинания



В сообщении будет сказано, что с Вашей банковской карты совершена покупка (перевод денег), а если Вы её не совершали, то для связи с банком необходимо позвонить по указанному в сообщении телефону. Если пользователь позвонит, то операторы-мошенники, используя методы социальной инженерии, постараются выведать у него реквизиты банковской карты.

**3.2. Предварительный просмотр ссылок.** При получении входящего сообщения, содержащего ссылку или файл, мессенджеры формируют небольшое окно предварительного просмотра с кратким описанием страницы или файла – так называемое «превью». Для того чтобы создать такое превью, программа автоматически открывает эту ссылку или загружает файл, что потенциально может привести к заражению устройства вредоносной программой.



Образец ссылки

1. **Рекомендации по использованию мессенджеров:**

4.1.Скачивайте приложения мессенджеров только с сайтов разработчиков и официальных магазинов приложений.

4.2.Запретите в настройках получение ссылок от незнакомых контактов.

4.3.С подозрением относитесь к полученным ссылкам и файлам, даже если они поступили от известного отправителя. Прежде чем переходить по ссылке или открывать файл, узнайте другим способом связи, действительно ли Ваш знакомый отправлял их.

4.4.Регулярно обновляйте все установленные программы и операционную систему своих устройств

Информацию подготовил специалист по социальной работе

организационно-методического отделения Резник С.А.

Информация актуальна на момент публикации

(февраль 2024 года)

**353740, ст. Ленинградская,**

**ул. Коммунальная, 42, каб. № 6а**

**8 (86145) 7 – 17 – 23**

**n.andriichenko@mtsr.krasnodar.ru**

[**www.leningradskiy-kcson.ru**](http://www.leningradskiy-kcson.ru)

**Государственное бюджетное учреждение**

**социального обслуживания**

**Краснодарского края**

**«Ленинградский комплексный центр**

**социального обслуживания населения»**

**Безопасное использование мессенджеров**

для граждан пожилого возраста и инвалидов,

проходящих обучение в компьютерном классе

**ст. Ленинградская**

**2024**