



**Внимание!
Deepfake
мошенничество:
Как не стать жертвой?**

Deepfake (гунфейк)

– это созданные искусственным интеллектом голосовые и видеозвонки от якобы коллег, друзей и родственников.

**Как распознать
Deepfake?**

• **Неестественное освещение и тени:**

Обратите внимание на то, как свет падает на лицо и окружение.

• **Размытые контуры лица:**

Deepfake часто имеет нечеткие границы между лицом и телом.

• **Несинхронность губ:**

Сравните движения губ с произносимым текстом.

• **Механические движения:**

Обратите внимание на неестественные движения головы, глаз или мимики.

• **Несоответствия в голосе:**

Голос может звучать синтетически или не соответствовать лицу.

**Deepfake – это обман!
Будьте бдительны
и защитите свои
сбережения!**

**Прокуратура
Железнодорожного
района
г. Красноярск**



**почтовый адрес:
ул. Ладосовели, д. 18 "А"
г. Красноярск, 660001**

**телефон:
+ 7 (391) 299-16-00**

Защитите себя сейчас!

РЕКОМЕНДАЦИИ

- Ограничьте доступ к своим фотографиям и видео:

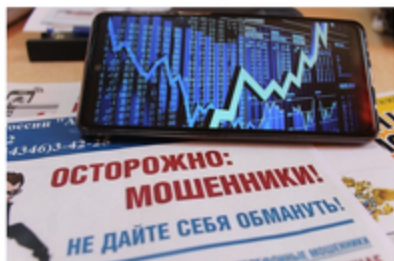
Настройте приватность в социальных сетях.

- Не публикуйте слишком много личной информации в Интернете

- Будьте осторожны с видеозвонками от незнакомых номеров

- Используйте двухфакторную аутентификацию для защиты своих аккаунтов

- Установите последние обновления безопасности на свои устройства



Что делать, если вы стали жертвой Deepfake мошенничества?



1. Немедленно прекратите все контакты с мошенниками!

Не переводите деньги, не сообщайте личные данные.

2. Сохраните все доказательства:

Сделайте скриншоты переписки, сохраните ссылки на видео/аудиозаписи.

3. Обратитесь в полицию!

Обратитесь в правоохранительные органы с заявлением о мошенничестве. Предоставьте всю имеющуюся информацию.

4. Сообщите в банк!

Чтобы заблокировать транзакцию.

5. Предупредите близких!

Расскажите им о случившемся, чтобы они не стали следующими жертвами.

Сценарии мошенничества с использованием Deepfake

"Родственник попал в беду":

Вы получаете видеозвонок от якобы вашего родственника, который плачет и просит срочно перевести деньги, потому что попал в аварию/его задержали/ему нужна операция.

"Компрометирующее видео":

Вам угрожают публикацией фальсифицированного видео, порочащего вашу репутацию, и требуют выкуп, чтобы его не распространили.

Поддельные инструкции от банка/госорганов:

Злоумышленники, используя Deepfake, выдают себя за сотрудников банка или госорганов и убеждают вас перевести деньги или предоставить личные данные.

"Инвестиции в прибыльный проект":

Поддельный эксперт убеждает вас вложить деньги в несуществующий проект.

Мошенники используют ваши эмоции – страх за близких, желание помочь. Не поддавайтесь панике!