памятка от StopPhish

ДИПФЕЙКИ: ЧТО ВАЖНО ЗНАТЬ КАЖДОМУ СОТРУДНИКУ

Дипфейки и их создание

Дипфейки — это видео, аудио или фото, подделанные с помощью нейросетей. Они могут заставить человека выглядеть так, будто он говорит или делает что-то, чего на самом деле не делал.

Как создаются:

- Сначала мошенник собирает материалы: видео, аудио, фото цели.
- Потом нейросеть «учится» повторять голос и движения лица.
- Полученный файл может быть почти неотличим от оригинала, особенно при коротких видео или аудиосообщениях.

Даже короткое видео или голосовое сообщение могут быть опасными.

Типовые сценарии атак

1. Финансовые мошенничества
Мошенники делают дипфейк видео или звонок с голосом директора, чтобы сотрудник перевёл деньги на фейковый счёт.

2. Социальная инженерия через мессенджеры
Фальшивое видео HR или IT-менеджера, где «даётся команда» скачать файл или перейти по ссылке.

3. Дезинформация и репутация
Поддельные видео с сотрудником могут появиться в соцсетях, чтобы дискредитировать его или компанию.

4. «Проверка доверчивости»
Мошенники могут прислать дипфейк, чтобы узнать, как сотрудник реагирует на необычные запросы, и использовать это в дальнейшем.

Реальные случаи:

WPP — попытка мошенничества

WPP — один из крупнейших глобальных рекламных холдингов. Мошенники клонировали голос и образ CEO Марка Рида. Создали WhatsApp-аккаунт с его фотографией и попытались организовать встречу в Microsoft Teams с другим топ-менеджером. Цель — выудить деньги или личные данные. Атака была пресечена благодаря внимательности сотрудников.

Arup — потеря $200 млн

Arup — крупная британская инженерная группа.

Сотрудник в Гонконге участвовал в видеоконференции с «топ-менеджерами компании» (включая CFO). Все, кроме жертвы, были дипфейками. По поручению «руководства» он совершил 15 переводов на разные банковские счета — всего $200 млн.

Статистика (Banking+):

Россия (2025, первые 3 мес.)
Обнаружено 67% дипфейков от годового объёма 2024 года.

41% россиян уже сталкивались с дипфейками.
Успешность таких атак ~20 %

Как распознать дипфейк без специальных программ

• Видео: движение губ и глаз не совпадает с голосом, мимика кажется странной или неестественной, «дерганые» движения рук и головы, неровные тени на лице и странные блики.

• Аудио: слишком ровная речь без эмоций, «плоский» голос, странные паузы.

• Контекст: сообщение требует срочного действия или противоречит обычной практике.

• Источник: проверяйте, кто прислал и через какой канал; мошенники часто подделывают адреса и имена.

На телефоне:
• Сравните голос с ранее записанными звонками или голосовыми сообщениями.
• Попросите собеседника записать короткое «живое» видео с конкретной фразой.

На компьютере:
• Замедлите видео — несинхронные движения сразу заметны.
• Проверьте метаданные файла (дата создания, программа).
• Если видео или аудио пришло с подозрительной ссылки, не открывайте — сначала уточните у отправителя другим способом.

Как защитить себя и данные

• Не выкладывайте в соцсети слишком много фото и видео лица — это материал для дипфейков.

• Используйте сложные пароли и двухфакторную аутентификацию.

• Проверяйте источники всех необычных сообщений и ссылок.

• Не спешите выполнять срочные просьбы, особенно касающиеся денег или данных.

Что делать, если сомневаетесь

• Свяжитесь с отправителем через другой канал (телефон, личная встреча).

• Не пересылайте подозрительные видео или аудио.

• Сообщите в ИБ-отдел — они проверят и при необходимости предупредят остальных сотрудников.

Полезные привычки для защиты компании

• Всегда проверяйте необычные запросы и ссылки.

• Разговаривайте с коллегами и делитесь подозрительными случаями.

• Будьте внимательны к корпоративной информации — даже короткие видео и аудио могут быть использованы против компании.

С пожеланиями безопасности, StopPhish