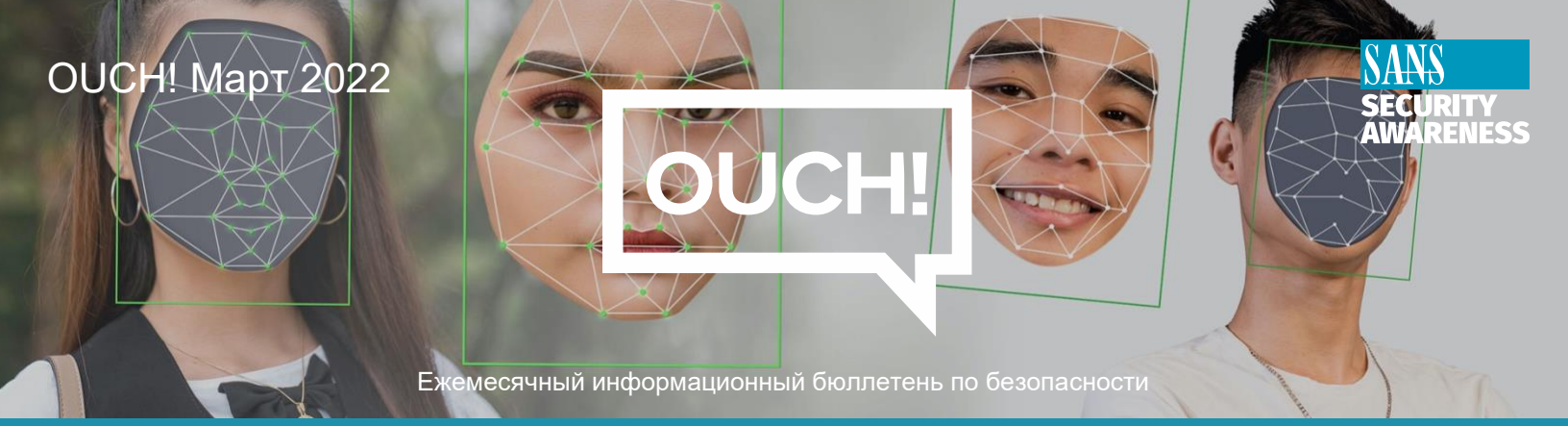
OUCH! Март 2022



Изучите новый навык: обнаружение дипфейков

Что такое дипфейки?

Слово «дипфейк» представляет собой комбинацию «глубокого обучения» и «подделка». Дипфейки — это фальсифицированные изображения, видео или аудиозаписи. Иногда люди в них представляют собой сгенерированные компьютером поддельные личности, которые выглядят и звучат так, как будто они настоящие люди. Иногда люди реальны, но их образами и голосами манипулируют, заставляя делать и говорить то, чего они не делали и не говорили. Например, дипфейковое видео может быть использовано для воссоздания того, как знаменитость или политик говорит то, чего никогда не говорил. Используя эти очень реалистичные фейки, злоумышленники могут раскрутить альтернативную реальность, где не всегда можно доверять своим глазам и ушам.

У некоторых дипфейков есть законные цели, например, фильмы, в которых умерших актеров возвращают к жизни, чтобы воссоздать известного персонажа. Но кибер-злоумышленники начинают использовать потенциал дипфейков. Они используют их, чтобы обмануть ваши чувства, чтобы украсть ваши деньги, беспокоить людей, манипулировать избирателями, политическими взглядами или создавать фальшивые новости. В некоторых случаях они даже создали фиктивные компании, состоящие из поддельных сотрудников. В свете этих атак, вы должны стать еще более осторожными в том, во что вы верите при чтении новостей или социальных сетей.

ФБР предупреждает, что в будущем дипфейки будут иметь «более серьезные и широкомасштабные последствия из-за уровня сложности используемых синтетических носителей». Научитесь определять признаки дипфейка, чтобы защитить себя от этих очень правдоподобных симуляций. Каждая форма дипфейка — неподвижное изображение, видео и аудио — имеет свой собственный набор недостатков, которые могут его выдать.

Фотографии

Чаще всего вы можете увидеть дипфейк — фальшивую фотографию профиля в социальной сети. На изображении ниже пример дипфейка с сайта этогочеловеканесуществует.com. Под изображением пять разных признаков того, что это может быть дипфейк. Вы заметите, что эти подсказки нелегко обнаружить и их может быть трудно идентифицировать:

1. Фон: фон часто бывает размытым или искривленным, а также может иметь непостоянное освещение, например ярко выраженные тени, направленные в разные стороны.
2. Очки: внимательно посмотрите на соединение между оправой и дужками возле виска. Дипфейки часто имеют несоответствующие соединения с немного разными размерами или формами.
3. Глаза: на дипфейковых фотографиях, которые в настоящее время используются для фальшивых изображений профиля, кажется, что их глаза находятся в одном и том же месте в кадре, что приводит к тому, что некоторые называют «дипфальшивым взглядом».
4. Ювелирные изделия: Серьги могут быть аморфными или причудливо прикрепленными. Ожерелья могут быть встроены в кожу.
5. Воротники и плечи: плечи могут быть деформированными или несоответствующими. Воротники могут быть разными с каждой стороны.

Видео

Исследователи из Массачусетского технологического института (MIT), разработали список вопросов, чтобы помочь вам выяснить, является ли видео реальным, отметив, что дипфейки часто не могут «полностью представить естественную физику» сцены или освещения.

1. Щеки и лоб: Кожа кажется слишком гладкой или слишком морщинистой? Возраст кожи подобен возрасту волос и глаз?
2. Глаза и брови: Появляются ли тени в ожидаемых местах?
3. Очки: есть ли блики? Слишком много бликов? Меняется ли угол бликов при движении человека?
4. Волосы на лице: волосы на лице выглядят настоящими? Дипфейки могут добавлять или удалять усы, бакенбарды или бороду.
5. Родинки на лице: выглядит ли родинка настоящей?
6. Мигание: моргает ли человек достаточно или слишком много?
7. Размер и цвет губ: Соответствуют ли размер и цвет остальной части лица человека?

Аудио/голос

Исследователи говорят, что такие технологии, как спектрограммы, могут показать, когда записи голоса являются поддельными. Но у большинства из нас нет такого оборудования, как анализатор голоса, когда звонит злоумышленник. Прислушайтесь к монотонной речи, странному тону или эмоциям и отсутствию фонового шума. Подделки голоса бывает трудно обнаружить. Если вы получили странный звонок от законной организации, вы можете проверить, является ли звонок реальным, сначала повесив трубку, а затем перезвонив в организацию. Обязательно используйте доверенный номер телефона, например номер телефона, который уже есть в вашем списке контактов, указанный в счете или выписке из организации, или номер на официальном веб-сайте организации.

Вывод

Имейте в виду, что злоумышленники активно используют дипфейки. Они могут создавать поддельные учетные записи в социальных сетях, чтобы общаться, или создавать поддельные видео, чтобы влиять на общественное мнение. Некоторые даже продают свои услуги в даркнете, чтобы другие злоумышленники могли делать то же самое. Мы не ожидаем, что вы станете экспертом по дипфейкам, но если вы вооружитесь основами выявления подделок, вы будете намного лучше защищены. Если вы подозреваете, что обнаружили дипфейк, сообщите об этом веб-сайту или источнику, на котором размещен контент.

Приглашенный редактор

Керри Томлинсон (@KerryTNews) является репортером киберновостей в Ampere News и сертифицированным специалистом по безопасности SANS. Ее миссия состоит в том, чтобы переводить то, что происходит в цифровом мире, для людей с любым уровнем знаний с помощью убедительных, проницательных новостей и презентаций.

Ресурсы

Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Сможете отличить подделку? (Новости Ампера): https://www.amperesec.com/news/can-you-spot-the-fake
Тест обнаружения дипфейков Массачусетского технологического института (MIT):
https://detectfakes.media.mit.edu/
Найди дипфейк: https://www.spotdeepfakes.org/en-US

Роман Полаков