DEEPFAKE

Los “**Deepfake**” son vídeos manipulados usando técnicas de inteligencia artificial. El resultado es extremadamente realista.

Comenzaron siendo vídeos porno a los que un usuario de la red Reddit añadía caras de actrices famosas. Este hacker utilizaba el alias ***Deepfake***, un término que proviene de las palabras **fake (falso)** y **Deep learning** (aprendizaje profundo, una técnica de aprendizaje automático usando **inteligencia artificial)**.

La inteligencia artificial es capaz de recrear las **formas de la cara** de **cualquier** persona así como su **voz**.

Los Deepfakes son una amenaza que pueden agravar **las fake news**. Además de **videos falsos** de políticos y famosos, paulatinamente los videos usarán los **rostros** de personas más cercanas, como colegas, compañeros o familiares.

Se plantea un escenario que ***en un futuro no muy lejano***, algunos de nosotros no ***confiaremos en nada*****,** por más que los sentidos vean algo con contenido verdadero.

El gran problema de las Deepfakes es que su uso es para **manipular la información** y crear **consecuencias graves** para los involucrados, los peligros de los vídeos falsos son más grandes que los de las **“fake news”**, ya que un vídeo tiene un impacto mayor ante la sociedad.

¿Cómo se verifica un Deepfake?

1. Verificar la fuente, **¿Quién lo grabo**?, ¿Quién lo público?, **¿Y dónde se compartió por primera vez?**
2. Existen **programas** para ralentizar la grabación y descubrir **manipulaciones**.
3. **Interpretar, entender e investigar,** son hábitos para no creer cualquier cosa que se encuentra en internet.

JUICE JACKING

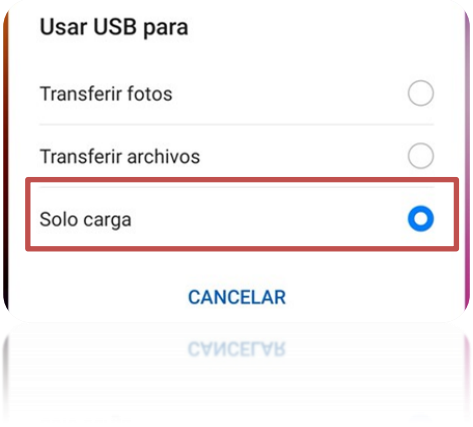
La dependencia del móvil ha provocado que a menudo las personas se encuentren en esa temida situación en la que el móvil está a punto de quedarse sin batería.

Para aliviar este problema muchos lugares públicos como restaurantes o aeropuertos ofrecen puertos de **carga USB;** pero **cuidado**, porque usarlos sin tomar algunas precauciones previas pueden ser muy mala idea.

Cuando los puertos hacen algo más que cargar.

El problema está en que esos puertos públicos están accesibles a todo el mundo, y eso hace que **cibercriminales** puedan aprovechar ese acceso libre para **modificarlos** y convertirlos en puertos capaces de **instalar malware**, mientras se carga el dispositivo.

Esta técnica se conoce como **juice-jacking,** este permite que un ciberatacante instale malware en los dispositivos, y pueda copiar ***información confidencial.***



No es recomendable utilizar estos puertos para recargar el dispositivo.

Pero si no se tiene alternativa deberemos asegurarnos de que cuando se conecte el celular **no se active** la ***opción de transferencia de datos*** del dispositivo. Se debe tener en solo **"carga".**