**دیپ فیک (Deepfake) چیست؟**

دیپ فیک (Deepfake) به معنی جعل عمیق فیلم‌های صوتی و تصویری جعلی از افراد است که از آنها را به طور دروغی و غیرواقعی جلوه می­ دهد. “Deep” اشاره به فناوری «یادگیری عمیق» برای تولید رسانه‌ها و “Fake” به ماهیت دروغی آن ارتباط دارد.

بیشتر وقت­ ها چهره یک فرد بر روی بدن فرد دیگری قرار داده می­ شود و چهره واقعی آنها تغییر می­ کند و در ظاهر، کارها و گفتارهایی را انجام می­‌دهند که هرگز آنها را انجام نخواهند داد.

فناوری دیپ فیک Deepfake، شکل و حالات نقاط مختلف چهره انسان را از طریق دوربین ها کشف کرده و به طرز کاملا ً باورپذیری چهره همان انسان را جعل کرده و می‌تواند او را در حال حرکت، سخنرانی و هر حالتی که فکر کنید قرار دهد. یک عروسک خیمه شب بازی دیجیتالی که در محیط‌های دیگر، بازتولید می‌شود. هوش مصنوعی همانند سوختی است که توسعهDeepfake، را سرعت بخشیده، اما این فقط یک فناوری است، که باید از طریق قوانین و دستورالعمل‌هایی مربوط به اسکن تصاویر چهره کنترل گردد.

این اصطلاح در سال ۲۰۱۷ ایجاد شد و در آن یک کاربرReddit، ویدیوی جعلی از چهره برخی از افراد مشهور هالیوود را نشان می­داد، منتشر کرد.

**چگونه می‌توان دیپ فیک یا جعل عمیق را شناسایی کرد؟**

امروزه محققان و شرکت­‌ها در حال تحقیق در مورد چگونگی استفاده از هوش مصنوعی برای تشخیص و از بین بردن **دیپ فیک** (Deepfake) هستند. پیشرفت‌‌های جدیدی به وجود آمده است که به ما در شناسایی عکس‌ها و فایل­‌های ضبط شده واقعی و تقلبی کمک می‌ کنند.

با این حال، چنین کاری مانع از ایجاد، به اشتراک ­گذاری، مشاهده و شنیدن رسانه­‌های جعلی میلیون ­ها نفر از مردم، قبل از حذف آنها نمی‌ شود؛ و بدون تردید، پس از انتشار آن‌ها، با پیامدهای زیادی مواجه بوده و ترمیم آسیب­‌های ناشی از آن نیز بسیار دشوار خواهد شد.

**چگونه می­** **توانید از کسب و کار خود در برابر دیپ فیک محافظت کنید؟**

رقبا می­ توانند برای حذف شما از صنعت، به باج­ خواهی از طریق جعل عمیق روی بیاورند.

این که راه حل­ های تشخیص دیپ فیک و فناوری مناسب آن در دسترس باشد، مهم نیست. مهم این است که این راه حل­ها مانع به اشتراک گذاشتن رسانه­های جعلی و انتشار آن نمی­ شوند. بنابراین بهترین راه این است که به کارمندان خود، چگونگی تشخیص رسانه­ های جعلی را آموزش داده و در مورد آنچه که به نظر می­ رسد نوعی سوءتفاهم در سازمان است، تحقیق کنید.

1. **به کارمندان خود آموزش دهید.**

موضوع آموزش تشخیص دیپ فیک را می ­توان در آموزش **[امنیت سایبری](https://softyab.com/what-is-cyber-security/)**جستجو کرد. به عنوان مثال، اگر کارمندان یک تماس غیرمنتظره از مدیرعامل دریافت کنند که از آنها بخواهد 10 میلیون تومان به حساب بانکی واریز کنند می­‌توانند قبل از هر چیز سؤال کنند آیا شخصی که پشت خط تلفن است واقعاً همان مدیرعامل است؟ شاید بهتر باشد که چند سؤال امنیتی برای تأیید هویت فرد تماس گیرنده از وی پرسیده شود.

اگر قربانی دیپ فیک شده‌­اید، اطمینان حاصل کنید که اطرافیانتان از این حمله هدفمند آگاه هستند. این کار یعنی تلاش برای نادیده گرفتن آنچه اتفاق افتاده است یا این که مخاطبان به چیزی که دیده یا شنیده­اند اعتقادی نداشته باشند. بنابراین تلاش‌های شما باید مبتنی بر روابط عمومی و در حول این موضوع باشد که افراد در شرکت شما در مورد جعل عمیق، اطلاعات کافی داشته و ماهیت جعلی رسانه­های توزیع شده را فاش کنند.

 خطر وجود افراد ناآگاه همواره جدی بوده و نباید آن را دست­ کم گرفت. یک شایعه غیرمنتظره می­ تواند کسب و کار شما را نابود کند. بنابراین شما هم به عنوان یک فرد و هم به عنوان یک سازمان باید آمادگی ایستادگی در برابر این تهدیدها را داشته و هرگز اجازه ندهید که اطلاعات نادرست و جعلی، اعتماد عمومی به شما را از بین ببرد!

**معرفی برخی نرم‌افزارهای دیپ فیک**

اگر شما هم می‌خواهید فناوری دیپ فیک را امتحان کنید و ببینید که کارکرد آن چگونه است، ما در ادامه تعداد از برترین نرم‌افزارها و اپلیکیشن‌های دیپ فیک را به شما معرفی می‌کنیم. برخی از موارد این لیست صرفا جنبه سرگرمی دارند.

* وب سرویس [Deepfakes web β](https://deepfakesweb.com/)
* وب‌سایت [AvengeThem](https://avengethem.com/)
* اپلیکیشن [Doublicat](https://play.google.com/store/apps/details?id=video.reface.app)
* وب‌سایت [MachineTube](https://www.machine.tube/)
* نرم‌افزار [DeepFaceLab](https://github.com/iperov/DeepFaceLab)
* اپلیکیشن [Deep Art](https://play.google.com/store/apps/details?id=de.nextsol.deeparteffects.app&hl=en_IN)
* اپلیکیشن [Face Swap Live](https://play.google.com/store/apps/details?id=com.laan.labs.faceswaplive.beta&hl=en_IN)

منبع [theguardian](https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them)

لطفا جهت مشاوره در [انتخاب محصول امنیتی مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[**اجتماعی**](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**