

تهدید صرافی های رمزارزی از طرف هوش مصنوعی

مدیر ارشد امنیت بایننس هشدار داده که فناوری Deepfake که به دست کلاهبرداران رمزارزی برای دور زدن احراز هویت مشتری (KYC) در صرافی های رمزارزی مانند Binance استفاده می شود، پیشرفت زیادی کرده است.

به گزارش سایت خبری پرسون به نقل از کوین تلگراف، دیپ فیک ها با استفاده از ابزارهای هوش مصنوعی ساخته می شوند که از یادگیری ماشینی برای ایجاد صدا، تصاویر یا ویدیوهای شبیه به افراد استفاده می کنند.

جیمی سو، مدیر ارشد امنیت بایننس در گفت و گو با کوین تلگراف خبر داد که کلاهبرداری که از این فناوری برای دور زدن فرآیندهای احراز هویت در این صرافی استفاده می کنند، در حال افزایش اند.

سو گفت که این ابزارها به گونه ای پیشرفته شده اند که حتی می توانند به درستی به دستورات صوتی ای که برای بررسی انسان بودن متقاضی طراحی شده اند، به درستی پاسخ دهند و این کار را به صورت زنده انجام می دهند.

در فرآیند احراز هویت بعضی از اعتبارسنجی ها نیاز است که کاربر، به عنوان مثال، چشم چپ خود را بر هم بزند یا به سمت چپ یا راست یا به بالا یا پایین نگاه کند. دیپ فیک ها امروزه به قدری پیشرفته شده اند که در واقع این دستورات را اجرا می کنند.

با این حال، سو معتقد است که ویدیوهای تقلبی هنوز به حدی پیشرفت نکرده اند که بتوانند یک اپراتور انسان را فریب دهند.

سو در پاسخ به سؤالی درباره نحوه مبارزه با چنین حملاتی بیان داشت که، حل این مشکل بسیار دشوار است.

در آگوست ۲۰۲۲ نیز، پاتریک هیلمن، مدیر ارشد ارتباطات بایننس، هشدار داد که یک «تیم هک پیشرفته» از مصاحبه های خبری قبلی و حضورهای تلویزیونی او برای ایجاد نسخه ای «دیپ جعلی» استفاده کرده است.

منبع: رمزارز نیوز