

## ساخت ایستگاه‌های معلق 5G توسط ژاپن



فناوری جدید ژاپن که توسط صنعت مخابرات این کشور توسعه داده شده HAPS نام داشته و در سال ۲۰۲۵ به صورت ایستگاه‌های هوایی شبکه 5G راه‌اندازی خواهد شد. این فناوری با کمک وسایل نقلیه بدون سرنشین در استراتوسفر زمین قرار گرفته و می‌تواند شبکه 5G را به صورت گسترده در اختیار کاربران قرار دهد.

طبق گزارش‌های منتشر شده توسط رسانه Nikkei Asia این فناوری همانند استارلینک می‌تواند با استفاده از پهپاد‌های خورشیدی قرار گرفته در ارتفاعات ۱۸ الی ۲۵ کیلومتری خدمات شبکه را به کاربران ارائه کند. احتمالا یکی از این مازول‌ها تنها می‌تواند حدود ۲۰۰ کیلومتر را پوشش دهد. علاوه بر آن فرکانس‌های ۷۷ گیگاهرتزی، ۲ گیگاهرتزی و ۲/۶ گیگاهرتزی نیز در این فناوری استفاده خواهد شد. همچنین برای بهبود خدمات تلفن همراه در مناطقی از آسیا، اروپا، آمریکا و آفریقا باند ۷۰ تا ۹۰ مگاهرتزی نیز استفاده می‌شود.

از سال‌های گذشته تاکنون بسیاری از کشورها به دنبال راه‌اندازی شبکه‌های 5G بودند. در این بین کشور چین با داشتن بیش از سه میلیون ایستگاه زمینی توانسته است علاوه‌بر ارائه سریع‌ترین اتصال بی‌سیم رکورد بیشترین تعداد ایستگاه را از آن خود ثبت کند.

## راه حل جدید

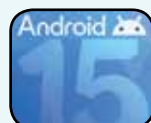
### کاهش ریسک هوش مصنوعی



شرکت OpenAI، سازنده چت‌بات هوش مصنوعی ChatGPT، از مجموعه‌ای از دستورالعمل‌ها و ابزارهای تازه موسوم به «چهارچوب آمادگی» برای نظارت بر هوش مصنوعی و خطرات آن رونمایی کرد. این کار از طریق یک گروه مشورتی برای تضمین ایمنی انجام خواهد شد که حتی حق وتوی نظرات «سم آلتمن» را خواهد داشت.

طبق این چهارچوب، مدل‌هایی که در دست توسعه قرار دارد، توسط تیم «ایمنی سیستم‌ها» ارزیابی خواهد شد. مدل‌های پیشگام OpenAI نیز تحت نظارت تیم «آمادگی» قرار می‌گیرد تا ریسک‌های احتمالی پیش از عرضه مدل‌ها، شناسایی و ارزیابی شود.

## اندروید ۱۵ با قابلیت نمایش سلامت باتری!



گوگل قصد دارد قابلیت جدیدی را در اندروید ۱۵ برای کاربران رونمایی کند که از طریق آن بتوان میزان سلامت باتری گوشی‌ها را مشاهده کرد. همچنین با کمک این قابلیت، کاربران نسبت به تعویض باتری نیز اطلاعاتی کسب خواهند کرد. این قابلیت جدید در اندروید ۱۵ پشتیبانی خواهد شد.

## ویندوز

### رونمایی از کلید هوش مصنوعی ویندوز



شرکت مایکروسافت دکمه‌ای به صفحه کلید ویندوز برای فعال کردن سرویس هوش مصنوعی کوپایلوت (AI Copilot) خود اضافه می‌کند و نخستین دستگاه‌ها با این دکمه جدید، ماه جاری عرضه می‌شوند.

کلید Copilot که در سمت راست دکمه اسپیس قرار می‌گیرد، اولین تغییر در چیدمان صفحه کلید ویندوز از زمانی است که مایکروسافت کلید ویندوز/استارت (Windows/Start) را در سال ۱۹۹۴ اضافه کرد. این تغییر، منعکس کننده تعهد این شرکت به هوش مصنوعی است و شرکای سخت افزاری مایکروسافت در روزهای آینده، در نمایشگاه فناوری CES، رایانه‌های ویندوز ۱۱ با دکمه Copilot را رونمایی خواهند کرد و به مرور زمان، این دکمه، به یک ویژگی ضروری تبدیل خواهد شد.

یوسف مهدی، مدیر ارشد بازاریابی مصرف کننده مایکروسافت، در وبلاگی با اعلام این تغییر گفت: این شرکت، سال ۲۰۲۴ را «سال رایانه‌های شخصی هوش مصنوعی» می‌بیند که منعکس کننده روند نوظهور مشابه در میان سازندگان گوشی‌های هوشمند برای معرفی مدل‌های خود به عنوان «تلفن‌های هوش مصنوعی» هستند. این عناوین، به خودی خود وزن زیادی ندارند، اما مایکروسافت سال گذشته را صرف بازسازی بزرگ‌ترین محصولات خود در زمینه فناوری هوش مصنوعی کرده است که می‌تواند محتوای جدیدی را از مجموعه عظیم داده‌ها، تولید کند. این فهرست اکنون شامل ویندوز، آفیس، موتور جست‌وجوی بینگ، نرم افزارهای امنیتی و محصولات مشتری و مالی است. این کار متکی به فناوری GPT-۴ شرکت OpenAI که مایکروسافت ۱۳ میلیارد دلار در آن سرمایه‌گذاری کرده است.

بر اساس گزارش بلومبرگ، ورود مایکروسافت به عرصه خدمات هوش مصنوعی، هنوز به افزایش فروش سازندگان دستگاه تبدیل نشده است، زیرا ویژگی‌های جدید Copilot به طور یکسان برای دستگاه‌های جدید و موجود عرضه می‌شود.

## فناوری جدید ذهن خوانی با هوش مصنوعی

در این فناوری که مبتنی بر هوش مصنوعی است برای نخستین بار از هیچگونه ایملنتی استفاده نشده و تنها فرد باید کلاه خاصی را روی سر بگذارد. امواج مغزی از طریق نوار مغزی ضبط و سپس با کمک هوش مصنوعی برای تبدیل به متن رمزگشایی خواهد شد. به گفته محققان فناوری DeWave تاکنون تنها ۴۰ درصد دقت داشته و نسبت به استاندارد قبلی برای ترجمه افکار بهبود ۳ درصدی را تجربه کرده است. محققان قصد دارند این دقت را تا ۹۰ درصد بهبود بخشند تا بتوانند از آن همانند روش‌های مرسوم ترجمه زبان با استفاده از نرم افزارهای تشخیص گفتار استفاده کنند. همچنین در این روش به کاشت الکتروود با دستگاه‌های بزرگ و گران قیمت ام آر آی برای ترجمه سیگنال‌های مغزی نیاز نخواهد بود. به گفته این محققان هنوز این فناوری با مشکلاتی در تشخیص کلمات مواجه بوده و ممکن است برخی از آنها را با یکدیگر اشتباه بگیرد. مقاله منتشر شده در این باره، این فناوری می‌تواند امواج خام را به طور مستقیم به کلام ترجمه کرده و برای بیماران فلج مغزی مورد استفاده قرار بگیرد.



## به روز

## خدا حافظی با جاعلان امضا!

در حالی که تصاویر جعلی روز به روز متقاعد کننده‌تر و گسترده‌تر می‌شود، سازندگان دوربین‌ها با فناوری جدیدی که می‌تواند صحت عکس‌ها را تأیید کند، با این مشکل مقابله می‌کنند. نیکون، سونی و کانن در حال کار بر روی تعبیه یک امضای دیجیتال در دوربین‌های خود هستند که به عنوان اثباتی بر اصل بودن و یکپارچگی تصاویر عمل خواهد کرد.

امضاهای دیجیتال حاوی اطلاعاتی مانند تاریخ، زمان، مکان و عکاس تصویر است و در برابر دستکاری مقاوم خواهد بود. این فناوری به عکاسان و سایر متخصصانی که نیاز دارند از اعتبار کار خود اطمینان حاصل کنند، کمک می‌کند. نیکون این ویژگی را در دوربین‌های بدون آینه خود ارائه می‌کند، در حالی که سونی و کانن نیز آن را در دوربین‌های تک‌لنزی بازتابی (SLR) بدون آینه حرفه‌ای خود به کار



## مراقب حساب کاربری تان باشید!

این روزها بیشتر مواظب حساب‌های ایمیل و اکانت‌های خود در شبکه‌های اجتماعی باشید. هکرها از ضعف در نحوه مدیریت کوکی‌ها توسط گوگل سوء استفاده می‌کنند؛ یعنی بخش‌هایی از داده‌هایی که وبسایت‌ها در مرورگر شما ذخیره می‌کنند. کوکی‌ها دلیلی است که مرورگر وب شما می‌تواند رمزهای عبور شما و کارهایی که در وبسایت‌ها انجام می‌دهید، به خاطر بسپارد.

با این حال، این کوکی‌ها همچنین می‌تواند توسط عوامل تهدید برای انتشار بدافزار مورد سوء استفاده قرار بگیرد. بدافزار یک فایل یا کد مخرب است که می‌تواند تلفن هوشمند، کامپیوتر دسکتاپ یا لپ‌تاپ شما را آلوده کند.

این نرم افزار به نوبه خود می‌تواند به هکرها امکان دسترسی به اطلاعات شخصی و جزئیات بانکی شما را بدهد. در حالی که گوگل کروم امکان ذخیره کوکی‌ها توسط شرکت‌های ثالث را فراهم می‌کند، راه برای هکرها باز می‌شود.

کارشناسان گفتند، حتی اگر رمز عبور خود را تغییر دهید، بدافزارها همچنان می‌تواند در دسرساز باشد. کارشناسان 9to5Google توضیح دادند: «خطرات چنین سوءاستفاده‌ای قابل توجه است زیرا این کوکی‌ها رمز عبور و احراز هویت دو مرحله‌ای را که معمولاً برای ایمن کردن حساب‌های گوگل استفاده می‌شود، دور می‌زند.»

این بدان معناست که هکرها حتی اگر کاربر واقعی رمز عبور خود را بازنشانی کند یا از سیستم خارج شود، باز هم می‌توانند به حساب‌ها وارد شوند.

### چگونه ایمن بمانیم

برای شروع، مهم است که همیشه دستگاه خود را با جدیدترین نرم افزار به‌روز نگه دارید. کوکی‌ها و حافظه پنهان مرورگر خود را پاک کنید تا کوکی‌های بالقوه مخربی که ممکن است در کمین دستگاه شما باشد، حذف شود.

شما هرگز نباید چیزی را از پنجره‌های پاپ‌آپ عجیب و غریب یا وب سایت‌هایی با ظاهر مشکوک دانلود کنید.

همچنین مهم است که یک آنتی‌ویروس و ضدبدافزار روی دستگاه خود نصب کنید تا بتواند هرگونه مشکلی را اسکن کند.

فعال کردن احراز هویت دو مرحله‌ای همچنین با نیاز به کد دوم برای حساب‌ها، یک لایه امنیتی به حساب کاربری شما اضافه می‌کند.

خواهند برد. سه غول دوربین‌سازی جهان بر روی یک استاندارد جهانی برای ایجاد یک امضای دیجیتال به توافق رسیده‌اند. امضایی که آنها را با ابزار مبتنی بر ویبی به نام وریفای (Verify) سازگار می‌کند. این ابزار که توسط گروهی از سازمانهای خبری جهانی، شرکت‌های فناوری و سازندگان دوربین‌ها راه‌اندازی شده است، به هر کسی اجازه می‌دهد تا اعتبار یک تصویر را به صورت رایگان بررسی کند. اگر تصویر دارای امضای دیجیتال باشد، وریفای اطلاعات مربوطه را نمایش می‌دهد. اگر هوش مصنوعی تصویری را ایجاد یا تغییر دهد، وریفای آن را به عنوان «بدون اعتبار» علامت‌گذاری می‌کند.

نیاز به چنین فناوری مشهود است زیرا که جعل‌های عمیق تصاویر افراد مهمی همچون دونالد ترامپ، رئیس جمهور سابق آمریکا و فومیو کیشیدا، نخست‌وزیر ژاپن، در سال میلادی ۲۰۲۳ در فضای مجازی منتشر شد و سؤالاتی را در مورد قابل اعتماد بودن محتوای آنلاین ایجاد کرد. علاوه بر این، محققان دانشگاه