



فیرنامه فاوای نفت



تاریخ انتشار: ۹۶/۰۲/۰۶ شماره نسخه: ۲۸۴

فاوای نفت، مجموعه‌ای از خدمات و محصولات دیجیتال برای صنعت نفت است.



دستیابی به صنعت نفتی مبتنی بر اندیشه و خرد با محوریت فاوا
ارتقای دانش با محوریت سرمایه فکری به منظور افزایش کارایی و اثربخشی
ایجاد بسترهای مناسب و مطلوب فاوا جهت دستیابی به صنعت نفت پیشرفته
ارتقاء کارایی و اثربخشی ارکان مدیریتی و اجرایی از طریق فاوا در صنعت نفت
برنامه‌ریزی و هوشمندسازی فرایندهای کسب و کار الکترونیک صنعت نفت
استقرار فراگیر و یکپارچه کاربردها و خدمات فاوا در صنعت نفت



در این شماره می‌خوانید:

- ← فیبر نوری خانگی
- ← اوراکل
- ← سرعت اینترنت
- ← هک مودم
- ← سایت های HTTP

چگونه درخواست فیبر نوری بدهیم؟



درخواست فیبر نوری و تبدیل سیم مسی به فیبر برای مشترکان رایگان است و با ارائه سرویس فیبر، آنها می‌توانند از هر یک از بسته‌های موجود در پورتال مخابرات در بخش تانومای اینترنت استفاده کنند. مشترکان مخابرات ایران می‌توانند به پورتال این شرکت مراجعه کرده، شماره تلفن منزل یا محل کار خود را وارد کنند و اعلام این‌که امکانات فیبر نوری برای آنها وجود دارد یا خیر را بگیرند. در صورتی که منطقه آنها تحت پوشش باشد، ثبت نام انجام و مراحل تبدیل به فیبر نوری طی می‌شود و در غیر این صورت می‌توانند برای این سرویس به صورت رایگان درخواست دهند. تانوما (تار نوری مخابرات ایران) به معنی «فیبر نوری تا ساختمان/خانه» است.

این سرویس به تکنولوژی جدیدی اطلاق می‌شود که به جای استفاده از کابل مسی از فیبر نوری برای انتقال اطلاعات تا ساختمان و یا محل مشتری بهره می‌برد و می‌توان سرویس‌های گوناگونی از جمله تلفن، اینترنت، سرویس‌های چندرسانه‌ای و دیگر سرویس‌های بر بستر دیتا را با سرعت و کیفیتی بسیار بالاتر از کابل مسی در اختیار مشترکان قرار داد. درخواست فیبر نوری و تبدیل سیم مسی به فیبر برای مشترکان رایگان است و با ارائه سرویس فیبر، آنها می‌توانند از هر یک از بسته‌های موجود در پورتال مخابرات در بخش تانومای اینترنت استفاده کنند.

مشترکان ADSL اگر محدوده‌شان تحت پوشش باشد، می‌توانند فیبر را جایگزین کنند. بنابراین مشتریانی که در حال حاضر روی ADSL هستند می‌توانند شماره تلفن خود را در پورتال وارد کنند و به آنها نشان داده می‌شود که تحت پوشش هستند یا خیر. در صورتی که کاربر تحت پوشش باشد، فرآیند راه‌اندازی فیبر ۴۸ ساعت طول می‌کشد. در غیر این صورت می‌توانند تقاضا دهند که کابل مسی برای آنها تبدیل به فیبر شود. اگر کاربر با مراجعه به پورتال مشاهده کنند که منطقه آنها تحت پوشش فیبر نوری قرار ندارد، می‌توانند در پورتال به صورت رایگان درخواست دهند و یا به مخابرات منطقه مراجعه کنند تا در نوبت قرار بگیرند. طبق اظهارات مدیرهای مخابراتی، طراحی فیبر بر اساس نیاز کاربران خواهد بود و با جمع‌آوری دیتابیس، همه می‌توانند در اولویت توسعه می‌باشد.

همچنین درخواست تبدیل کابل مسی به فیبر نوری برای کاربران هزینه نخواهد داشت، تنها زمان انعقاد قرارداد بر اساس طرح‌هایی که ارائه شده، هزینه می‌پردازند. بسته‌های اینترنتی متعددی در پورتال مخابرات موجود است و کاربران می‌توانند هر کدام از این بسته‌ها را خریداری کنند.



اوراکل در نظر دارد در بازار فضای ابر، با شرکت‌هایی همچون سیلزفورس، مایکروسافت و خدمات وب آمازون به رقابت بپردازد. شرکت اوراکل سرگرم خرید شرکت ورکر (Wercker)، یک شرکت کوچک هلندی است. کار این شرکت، کمک به توسعه‌دهندگان در ایجاد و به‌روزرسانی سریع نرم‌افزارها با استفاده از کانتینرهاست. منظور از «کانتینر»، شکل نوینی از توسعه نرم‌افزاری است که در میان شرکت‌های فناوری، بسیار رواج دارد. گفته می‌شود اوراکل به فضای ابر رو آورده تا در این بازار با شرکت‌هایی همچون سیلزفورس، مایکروسافت و خدمات وب آمازون به رقابت بپردازد.

این خبر که بدون جزئیات مالی منتشر شد، روز دوشنبه هفته گذشته در یک پست وبلاگی توسط میشا هرناندز فان لوفن (بنیانگذار و مدیرعامل ورکر) افشا شد. هرناندز این گونه می‌نویسد: «یک ابر پیشتان، نیازمند ابزارهای مناسب و افزودن مدیریت چرخه عمر کانتینر از سوی ورکر به ابر اوراکل، می‌تواند برای ایجاد، راه‌اندازی و مقیاس‌پذیر کردن برنامه‌ها، تجربه خوبی را برای گروه‌های مهندسی این شرکت به ارمغان بیاورد.»

ورکر و رقبایی همچون **CircleCI** و **CloudBees** وعده می‌دهند که توسعه‌دهندگان، امکان ترکیب و یکپارچگی سریع ویژگی‌های جدید در نرم‌افزارهایشان را داشته باشند. گفتنی است امروزه هر شرکتی از بانک‌ها گرفته تا خرده‌فروشان می‌دانند که برای به‌روزرسانی برنامه‌هایی که هم مشتریان و هم کارمندان همواره با آنها سر و کار دارند، به این ویژگی احتیاج دارند.

یکی از مزایای استفاده از کانتینرها این است که برنامه‌های حاصل از آنها را می‌توان یا در ابر طرف واسط (همچون **AWS**) یا در مراکز داده درونی خود شرکت اجرا کرد. از نگاهی دیگر، منظور از این تصاحب، جذب توسعه‌دهندگان نرم‌افزاری است که بخش مهمی از موفقیت هر ابر را تشکیل می‌دهند. شرکت ورکر که در سال ۲۰۱۲ در آمستردام تأسیس شد، توانسته است تاکنون ۷ میلیون و ۵۰۰ هزار دلار سرمایه جذب کند.



ایلان ماسک» شرکت جدیدی با نام **Neuralink** تاسیس کرده است که در آن می کوشد دستگاه‌های الکترونیکی را با مغز انسان سازگار کند. همزمان با پیشرفت فناوری‌های مختلف، به نظر می‌رسد نبرد برای تسخیر مغز کاربران آغاز شده است. به تازگی «ایلان ماسک» مدیرعامل شرکت خودروسازی تسلا اعلام کرده که با سرمایه‌گذاری‌های گسترده روی سیستم‌های رابط هوشمند مغز-رایانه کار می‌کند و طی چهار سال آینده این سیستم به صورت گسترده وارد بازار می‌شود.

به نقل از پی‌سی‌ورلد، «ایلان ماسک» بدین منظور شرکت جدیدی را با نام **Neuralink** تأسیس کرده است و در این مرکز می‌کوشد تا نسل جدید دستگاه‌های الکترونیکی را گسترده‌تر از پیش، با مغز انسان سازگار کند.

گفتنی است این خبر یک روز پس از آن منتشر شد که شرکت فیس‌بوک در کنفرانس سالانه خود توضیح داد با تشکیل گروهی متشکل از ۶۰ کارشناس، در حال ساخت سیستمی است که می‌تواند ذهن کاربران را بخواند. به گفته فیس‌بوک، این امکان فراهم خواهد شد تا در نسل جدید دستگاه‌های الکترونیکی بدون آنکه کاربر مجبور به تایپ کردن باشد، بتواند متن مورد نظر خود را از طریق پست الکترونیکی یا ابزارهای اجتماعی به مخاطبان بفرستد. شایان ذکر است که سیستمی که ماسک توسعه می‌دهد مبتنی بر تراشه‌های هوشمندی است که در بدن انسان قرار می‌گیرند و به تعبیر برخی کارشناسان، این تراشه‌ها مانند ورودی **USB** به مغز انسان متصل می‌شوند و از طریق یک جراحی کوچک امکان اسکن کردن فکر و ذهن را فراهم می‌کنند.

این فناوری که قرار است در مرحله نخست برای بیماران مورد استفاده قرار گیرد، به افراد معلول و ناتوان امکان می‌دهد تا بتوانند بدون هیچ مشکلی، از طریق دستگاه‌های الکترونیکی با دنیای پیرامون ارتباط داشته باشند. ماسک همچنین بر این مسئله تأکید کرده است که توسعه هوش مصنوعی و به کارگیری گسترده‌تر آن باعث نمی‌شود تا حریم شخصی افراد به خطر بیفتد و خواندن فکر مردم به معنی ورود به حریم شخصی آنها نیست.



با اتصال منازل به شبکه فیبر نوری، سرعت دسترسی به ۱۰۰ مگابایت خواهد رسید. معاون وزیر ارتباطات با اشاره به افتتاح فاز نخست شبکه دسترسی فیبر نوری در منازل گفت: با اجرای این پروژه سرعت ۵۰ تا ۱۰۰ مگابیت در ثانیه برای کاربران پیش‌بینی شده است.

برات قنبری امروز در مراسم بهره برداری از فاز نخست شبکه دسترسی فیبر نوری در منازل (تانوما) که صبح امروز با حضور معاون اول رئیس جمهور گفت: این پروژه تمامی نیازهای کاربران را در کمترین زمان و بهترین کیفیت فراهم می‌کند. رئیس هیئت مدیره شرکت مخابرات ایران ادامه داد: پروژه اتصال منازل به شبکه فیبر نوری مصوب ستاد فرماندهی اقتصاد مقاومتی در جهت تکمیل فاز سوم شبکه ملی اطلاعات است و پیش‌بینی می‌کنیم سرعت دسترسی به شبکه را از ۵۰ تا ۱۰۰ مگابیت بر ثانیه برای کاربران فراهم کند. وی ایجاد ظرفیت برای یک میلیون مشترک در هر شهر را از جمله ویژگی‌های فاز نخست این پروژه عنوان کرد و افزود: در این زمینه ۱۲۰۰ میلیارد تومان سرمایه گذاری شده و دو هزار کیلومتر فیبر نوری جدید در کشور نصب شده است. به گفته معاون وزیر ارتباطات شرکت مخابرات موفق به ایجاد بیش از ۱۰۰ هزار فرصت شغلی پایدار در این زمینه شده است.

وی با بیان اینکه ۵۰ درصد از سرمایه گذار ۲۵ هزار میلیارد تومانی صورت گرفته در حوزه فناوری اطلاعات و ارتباطات توسط مخابرات انجام شده است، گفت: طبق اهداف برنامه ششم توسعه برای ارتقا جایگاه کشور در منطقه باید جایگاه ایران ۳۰۰ درصد افزایش یابد. در این زمینه تغییر نگاه، اصلاح ساختار و اتخاذ رویکردهای جدید در توسعه بخش فناوری اطلاعات و ارتباطات در دستور کار قرار گرفته است.

در این مراسم شبکه فیبر نوری منازل به صورت نمادین و با سرعت ۸۸۴ مگابیت بر ثانیه در حضور معاون اول رئیس جمهور، وزیر ارتباطات، استاندار تهران و نمایندگان مجلس تست و راه اندازی شد.



مشکل دورزدن احراز هویت اس.ان.ام.پی می‌تواند برای دسترسی به صدها هزار مودم کابلی در سراسر دنیا مورد استفاده قرار گیرد و کاربران مختلف با سطوح امنیتی مختلف را تحت تأثیر خود قرار دهد. صدها هزار دستگاه دروازه اینترنت در سراسر دنیا و در درجه اول، مودم‌های کابلی خانگی، به خاطر ضعف جدی در پیاده‌سازی پروتکل مدیریت آسان شبکه، نسبت به هک شدن آسیب‌پذیر هستند.

SNMP یا همان پروتکل مدیریت آسان شبکه، برای تعیین هویت، نظارت و تنظیم از راه دور دستگاه شبکه خودکار مورد استفاده قرار می‌گیرد. بسیاری از این دستگاه‌ها مانند سرورها، چاپگرها، هاب‌های شبکه، سوئیچ‌ها و روترها به صورت پیش‌فرض پشتیبانی می‌شود. به نقل از پی.سی.ورلد، از یکویل فرناندز و برتین برویس که دو پژوهشگر مستقل هستند، اخیراً راهی برای دورزدن احراز هویت **SNMP** در ۷۸ مدل از مودم‌های کابلی پیدا کرده‌اند.

ارائه دهندگان خدمات اینترنتی (**ISP**) این مودم‌ها از کشورهای مختلفی بودند. اسکن‌های اینترنتی آنها نشان داد که صدها هزار دستگاه وجود دارد که می‌توان تنظیمات آنها را به خاطر ضعف **SNMP** تغییر داد. از سوی دیگر، نسخه‌های ۱ و ۲ پروتکل **SNMP**، دارای سیستم احراز هویت قوی نیستند. مدل دسترسی آنها به پیکربندی یک دستگاه از طریق رمز عبور، رشته‌های اجتماع نامیده می‌شود.

رمز عبور این دستگاه‌ها به صورت پیش‌فرض، در حالت عمومی برای صرفاً «خواندن» و در حالت خصوصی در حالت «نوشتن» قرار دارد، اما سازندگان این دستگاه‌ها می‌توانند این حالت‌ها را تغییر دهند. متخصصین می‌گویند انتشار اطلاعات حساس پیکربندی از طریق رشته اجتماع **SNMP** عمومی، مشکلی است که در طی چند سال اخیر روی بسیاری از دستگاه‌ها اثر گذاشته و آسیب‌های فراوانی در پی داشته است. در سال ۲۰۱۴، پژوهشگران دریافتند که تقریباً نیم میلیون دستگاه متصل به اینترنت که توسط شرکت‌های بروکید، آمبیت و نتوپیا تولید شده است، در **SNMP** مشکل دارند. البته واقعیتی که فرناندز و برویس کشف کردند، در حقیقت بسیار خطرناک‌تر بود و نشان می‌داد که مشکلات موجود در این دستگاه‌ها خیلی بیشتر از عدد اولیه نیم میلیون است. پژوهشگران بر این باورند که مشکلات اساسی در پیاده‌سازی پروتکل مورد بحث در مودم‌ها وجود دارد که باید فکری اساسی برای رفع این مشکل بشود.



کروم از اکتبر ۲۰۱۷ تمام سایت های HTTP را نا امن می داند کروم قصد دارد که از اکتبر ۲۰۱۷، روی سایت های اچ.تی.تی.پی. برچسب ناشناس بزند و آن ها را در زمره سایت های نا امن قرار دهد. به تازگی گوگل اعلام کرده که گام دوم برای امنیت وب سایت ها را خواهد برداشت. بدین منظور سایت های HTTP را در زمره سایت های نا امن قرار می دهد و این کار را از اکتبر ۲۰۱۷ و با مشخص کردن این سایت ها با حالت ناشناس شروع خواهد کرد.

اطلاعاتی که در صفحات وب رد و بدل می شوند، در بستر پروتکل HTTP انتقال می یابند، از آنجا که در انتقال داده ها با این پروتکل، داده ها رمزنگاری نمی شوند، افراد سوم شخص می توانند همواره به داده ها دسترسی داشته باشند. به همین دلیل است که HTTP از لحاظ امنیتی برای کارهایی که به اطلاعات حساس از جمله حساب های بانکی و رمزهای مشتریان مربوط می شود مناسب به شمار نمی روند. به همین جهت است که عموماً در وب سایت هایی که امنیت کاربران اهمیت زیادی دارد، از پروتکلی دیگر به نام HTTPS استفاده می نمایند. برای اتصال کاربران به اینترنت و وب سایت ها، مدل امن تری از HTTP وجود دارد که به آن HTTPS گفته می شود. یکی از اقدامات لازم و ضروری برای کاهش ریسک آسیب پذیری کاربران به اینترنت، همین مسئله HTTPS است. گفتنی است که با استفاده از این نسخه تبادل اطلاعات، داده ها و اطلاعات از دسترسی اشخاص دیگر مصون می ماند و کاربران می توانند با خیالی آسوده با وب سایت های مناسب و مدنظر خود ارتباط برقرار نمایند.

با انتشار کروم ۵۶ در ژانویه ۲۰۱۷، این مرورگر گوگل صفحات HTTP که خدمات مربوط به کارت های بانکی را انجام می دادند و از رمز عبور استفاده می کردند را در زمره سایت های نا امن قرار داد و از همان زمان، شاهد کاهش ۲۳ درصدی در ورود کاربران به سایت های HTTP از طریق کروم بوده ایم؛ البته لازم به ذکر است که کروم ۶۲ حتماً این روند را در سطوح بالاتر ادامه خواهد داد. طبیعتاً رمزهای عبور و کارت های بانکی، مهم ترین اطلاعاتی هستند که باید حالت خصوصی آنها حفظ شود و مسلماً نباید در دسترس هیچ شخص دیگری قرار بگیرد. گوگل از برخی از روش ها برای تشویق وب سایت ها استفاده کرده است. از نوامبر ۲۰۱۶، بیش از نیمی از صفحات کروم، به صورت HTTPS درآمده است و با ادامه این روند، تمامی سایت ها تحت پوشش این سرویس امنیتی قرار خواهد گرفت.