

## تعریف وب تاریک

وب تاریک (*dark web*) مجموعه ای پنهان از سایت های اینترنتی است که فقط توسط یک **مرورگر وب** تخصصی قابل دسترسی است. این برای ناشناس و خصوصی نگه داشتن فعالیت های اینترنتی استفاده می شود که می تواند در برنامه های کاربردی قانونی و غیرقانونی مفید باشد. در حالی که برخی از آن برای فرار از سانسور دولتی استفاده می کنند، همچنین وب تاریک به این صورت شناخته شده است که برای فعالیت های بسیار غیرقانونی مورد استفاده قرار می گیرد.

## وب تاریک، وب عمیق و وب سطح

### چیست؟

اینترنت با صدها میلیون ها صفحه وب، پایگاه داده و سرور قابل توجهی است که همگی ۲۴ ساعت در شبانه روز اجرا می شوند. اما به اصطلاح اینترنت “مرئی” (معروف به وب سطح یا وب باز - *visible Internet, aka surface web or open web*)، آن دسته از سایت هایی که می توان با استفاده از موتورهای جستجو مانند گوگل و یاهو پیدا کرد، فقط نوک کوه یخ از دنیای بزرگ اینترنت و فضای مجازی هستند.

## وب سطح یا وب *The surface web or open web*

وب باز یا وب سطح، لایه سطحی “مرئی” است. همچون تصویر بالا، اگر به تجسم کل وب مانند یک کوه یخ ادامه دهیم، وب باز قسمت بالایی و خارج از آب خواهد بود. از نقطه نظر آماری، این مجموعه از وب سایت ها و داده ها کمتر از ۵٪ از کل اینترنت را تشکیل می دهد.

همه وبسایت های عمومی که از طریق مرورگرهای سنتی مانند *Google Chrome*، اینترنت اکسپلورر و فایرفاکس قابل دسترسی هستند، در اینجا قرار دارند. وبسایت ها معمولاً با اپراتورهای رجیستری مانند «*.com*» و «*.org*» برچسب گذاری می شوند و می توانند به راحتی با موتورهای جستجوی محبوب پیدا شوند.

مکان یابی **وب سایت** های سطحی امکان پذیر است زیرا موتورهای جستجو می توانند وب را از طریق پیوندهای قابل مشاهده فهرست کنند (فرآیندی به نام «خزیدن» یا *crawling*)، به دلیل اینکه موتور جستجو مانند یک عنکبوت در وب حرکت می کند



وب عمیق و تاریک چیست؟



## The deep web وب عمیق

وب عمیق در زیر سطح قرار دارد و تقریباً ۹۰٪ از تمام وب سایت ها را تشکیل می دهد. این قسمتی از یک کوه یخ در زیر آب است که بسیار بزرگتر از وب سطح است. در واقع، این وب پنهان به قدری بزرگ است که نمی توان دقیقاً چند صفحه یا وب سایت در هر زمان فعال است. با ادامه قیاس، موتورهای جستجوی بزرگ را می توان مانند قایق های ماهیگیری در نظر گرفت که فقط می توانند وب سایت های نزدیک به سطح را کش (catch) کنند. همه چیز، از مجلات دانشگاهی گرفته تا پایگاه های داده خصوصی و محتوای غیر قانونی بیشتر، دور از دسترس است. این وب عمیق همچنین شامل بخشی است که ما به عنوان وب تاریک می شناسیم. در حالی که بسیاری از رسانه های خبری از «دیپ وب» و «وب تاریک» به جای یکدیگر استفاده می کنند، بسیاری از بخش های عمیق در کل کاملاً قانونی و ایمن هستند.



## وب عمیق

### برخی از بزرگترین بخش های وب عمیق عبارتند از:

اینترنت:  
 • شبکه های داخلی برای شرکت ها، دولت ها و امکانات آموزشی که برای برقراری ارتباط و کنترل جنبه های خصوصی در سازمان هایشان استفاده می شوند.

پایگاه های داده:  
 هم مجموعه فایل های حفاظت شده عمومی و خصوصی که به سایر مناطق وب متصل نیستند و فقط در خود پایگاه داده جستجو می شوند.



پس اگر نمی دانید چگونه به وب عمیق دسترسی پیدا کنید، به احتمال زیاد از قبل هر روز به نوعی از آن استفاده می کنید. اصطلاح "وب عمیق" به تمام صفحات وب اطلاق می شود که توسط موتورهای جستجو قابل شناسایی نیستند. وبسایت های عمیق ممکن است در پشت رمزهای عبور یا سایر دیوارهای امنیتی پنهان شوند، در حالی که دیگران به سادگی به موتورهای جستجو می گویند که آنها را «خزیدن» نکنند. بدون لینک های قابل مشاهده، این صفحات به دلایل مختلف بیشتر پنهان می شوند.

در وب عمیق بزرگتر، محتوای "پنهان" آن به طور کلی تمیزتر و ایمن تر است. همه چیز از پست های وبلاگ در بررسی و طراحی مجدد صفحه وب در انتظار، تا صفحاتی که هنگام بانکداری آنلاین به آنها دسترسی پیدا می کنید، بخشی از وب عمیق هستند. علاوه بر این، اینها هیچ تهدیدی برای رایانه یا ایمنی شما در کل ایجاد نمی کنند. بیشتر این صفحات برای محافظت از اطلاعات و حریم خصوصی کاربران از وب باز پنهان می شوند، مانند:

- حساب های مالی مانند بانکداری و بازنشستگی
- حساب های ایمیل و پیام های اجتماع
- پایگاه های اطلاعاتی شرکت های خصوصی
- اطلاعات حساس HIPPA مانند اسناد پزشکی
- پرونده های حقوقی

البته توجه کنید که جسارت و فرو رفتن بیشتر در وب عمیق، کمی خطر بیشتری را هم برای شما به همراه دارد. این دقیقاً مثل دریایی است که سطح بالایی آن (خارج از آب)، کاملاً روشن و شفاف است و همه چیز به راحتی دیده می شود و خطرات نیز بسیار کم است؛ اما در سطح زیرین آب، شفافیت دید کم شده و اگر چه خطر این تاریکی در لایه های اولیه آب چندان زیاد نیست، اما هر چه پایین تر بروید، هم قدرت دید بسیار کمتر می شود و هم فشار آب، احتمال مواجهه با ناشناخته های خطرناک و □ همه و همه بیشتر می شود.

برای برخی از کاربران، بخش هایی از وب عمیق فرصتی را برای دور زدن محدودیت های محلی و دسترسی به محتوای بیشتر، خدمات تلویزیونی یا فیلمی و □ که ممکن است در مناطق محلی آنها در دسترس نباشد، به نفع خود به کار می گیرند. دیگران برای دانلود موسیقی دزدی دریایی یا سرقت فیلم هایی که هنوز در سینماها اکران نشده اند، تا حدودی عمیق تر می شوند.

در انتهای تاریک وب، محتوا و فعالیت خطرناک تری را خواهید یافت. وبسایت های چند لایه ای *Tor* در این انتهای وب عمیق قرار دارند که «وب تاریک» در نظر گرفته می شوند و فقط توسط یک مرورگر ناشناس (*Tor Browser*) قابل دسترسی هستند.

## The dark web وب تاریک

وب تاریک به سایت هایی اطلاق می شود که ایندکس نشده اند و فقط از طریق مرورگرهای وب تخصصی قابل دسترسی هستند. وب تاریک که به طور قابل توجهی کوچکتر از وب سطح کوچک است، خود بخشی از وب عمیق در نظر گرفته می شود. با استفاده از تصویر اقیانوس و کوه یخ (تصویر بالا)، وب تاریک نوک پایینی کوه یخ و کاملاً در عمق پایین آب خواهد بود.

وب تاریک، با این حال، بخش بسیار پنهانی از وب عمیق است که کمتر کسی با آن ارتباط برقرار می کند یا حتی می بیند. به عبارت دیگر، وب عمیق همه چیز زیر سطح را که هنوز با نرم افزار مناسب قابل دسترسی است، از جمله وب تاریک را پوشش می دهد.



شکستن ساختار وب تاریک چند لایه کلیدی را نشان می دهد که آن را به پناهگاهی ناشناس تبدیل می کند: عدم وجود نمایه سازی صفحه وب

هیچ نمایه سازی صفحه وب توسط موتورهای جستجوی وب سطحی وجود ندارد. گوگل و سایر ابزارهای جستجوی محبوب نمی توانند نتایج را برای صفحات درون وب تاریک کشف یا نمایش دهند. تونل های ترافیک مجازی

در این سطح، "تونل های ترافیک مجازی" از طریق یک زیرساخت شبکه تصادفی ایجاد شده اند. غیر قابل دسترسی بودن توسط مرورگرهای سنتی

به دلیل اپراتور رجیستری منحصر به فرد آن، توسط مرورگرهای سنتی غیر قابل دسترسی است. همچنین، با اقدامات امنیتی مختلف شبکه مانند فایروال ها و رمزگذاری بیشتر پنهان می شود.

**شهرت** وب تاریک اغلب به مقاصد مجرمانه یا محتوای غیرقانونی و سایت های «تجارت» که در آن کاربران می توانند کالاها یا خدمات غیرقانونی خریداری کنند، مرتبط است. با این حال، احزاب حقوقی نیز از این چارچوب استفاده کرده اند. وقتی صحبت از امنیت وب تاریک می شود، خطرات وب عمیق با خطرات وب تاریک بسیار متفاوت است. لزوماً نمی توان به راحتی با فعالیت های سایبری غیرقانونی برخورد کرد، اما اگر به دنبال آن باشید، بسیار شدیدتر و تهدیدکننده تر است.