دوشنبه 16 فروردین 1400 - 07:26

چگونه از رد پای دیجیتالی خود محافظت کنیم؟

از آنجا که اینترنت تقریبا همه جنبه های زندگی ما را دربرگرفته است، اجتناب از این که نوعی حضور آنلاین داشته باشیم، دشوار است.

از آنجا که اینترنت تقریبا همه جنبه های زندگی ما را دربرگرفته است، اجتناب از این که نوعی حضور آنلاین داشته باشیم، دشوار است.

به گزارش ایسنا، ردی پای دیجیتالی، به آثار به جا مانده از فعالیتهای آنلاین شما اطلاق می شود؛ مثل وقتی که به طبیعت گردی می روید و آثار حضور شما مانند چوبهای سوخته، باقی مانده های غذا و مسیری که هنگام پیاده روی در جنگل ایجاد کرده اید، دیده می شود. در قضیه رد پای دیجیتالی، آثاری که از خود بر جای می گذارید، دیتا هستند. این رد پای دیجیتالی بر حسب فعالیتی که داشته اند در دو شاخه فعال و غیرفعال قرار می گیرد. پایگاه خبری بیزنس اینسایدر در گزارشی به بررسی این موضوع پرداخته است.

انواع مختلف رد پای دیجیتالی

یک رد پای دیجیتالی فعال، با آگاهی و هدفمندی ایجاد شده و دیتایی است که خودتان با آگاهی در اینترنت از خود بر جای می گذارید. برخی از مثالهای متداول دیتای هدفمند عبارتند از:

ایمیلها و پیامهای متنی
فرمهای آنلاینی که تنظیم و ارسال می کنید
دیدگاههایی که پای یک مقاله یا ویدیو می گذارید
پستهای وبلاگ و وب سایتهای شخصی
پستهای رسانه اجتماعی، آپدیتهای وضعیت، عکسها و ویدیوها

باید به خاطر داشته باشید که اگرچه این اطلاعات را آگاهانه ایجاد کرده اند اما ممکن است نخواهید به مدت طولانی نگه دارید یا آن را در دسترس افراد دیگری برای استفاده به شیوه هایی که مورد قبول شما نیست، قرار دهید.

رد پای دیجیتالی غیرفعال شما با اطلاعات ناخواسته ای ایجاد شده که بدون نیت و آگاهی و بی آنکه انتخابی داشته باشید، از خود بر جای گذاشته اند. این اطلاعات ناخواسته می توانند مواردی باشند نظیر:

کوکیها و اطلاعات ردگیری که توسط فعالیت وبگردی شما ایجاد شده است
موقعیت مکانی شما که در هنگام استفاده از نقشه ها و سایر اپلیکیشنهای مکان یاب ایجاد شده اند
آدرس آی پی، آدرس ایمیل و سایر اطلاعات شخصی که می توانند به فعالیتهای آنلاین شما مرتبط باشند

ریسک برجای گذاشتن رد پای دیجیتالی

رد پای دیجیتالی شما می تواند اطلاعات زیادی از شما به دیگران ارائه کند. در برخی از موارد استفاده مشروع از اطلاعات شما وجود دارد مانند صاحبان وب سایت و تبلیغات کنندگان که اطلاعات مربوط به عادتهای آنلاین و علاقمندیهای خریدتان را جمع می کنند تا بهتر قادر به پاسخگویی به نیازهای شما باشند. اما رد پای دیجیتالی شما می تواند توسط هکرها، خلافکاران، کلاهبرداران و سایر عوامل خرابکار مورد استفاده قرار گیرد. قابل توجه ترین ریسک مربوط به این دسته عبارتند از:

دزد هویت: شاید بزرگترین ریسکی که افراد در فضای آنلاین با آن مواجه هستند، به سرقت رفتن هویتشان است که در صورت بر جای ماندن اطلاعات حساس و شخصی کافی در محیط آنلاین، می تواند اتفاق بیافتد.

فیشینگ و کلاهبرداریهای دیگر: خلافکاران گاهی اطلاعات کافی درباره شخصی به دست می آورند تا بتوانند وی را طعمه کلاهبرداری قرار دهند. در حمله فیشینگ، خلافکار اینترنتی با قربانی خود تماس گرفته و وانمود می کند یکی از افراد آشنای وی است تا از وی پول یا اطلاعات ارزشمند درخواست کند.

تبلیغات: تبلیغات معمولا از رد پای دیجیتالی شما استفاده مشروع می کند اما بسیاری از افراد برای اهداف تبلیغاتی ردیابی می شوند.

تحقیقات کارفرما: کارفرمایان فعلی یا احتمالی می توانند برای پی بردن به زندگی شخصی شما، به بررسی پستهای شبکه اجتماعی و سایر فعالیتهای آنلاین شما بپردازند. با توجه به این که تا چه حد در اینترنت فعال هستید، زندگی شخصی شما می تواند در معرض دید عموم قرار گیرد و برخی رفتارها یا عقاید مذهبی و سیاسی شما ممکن است مورد پسند کارفرمایان قرار نگیرد.

چگونه رد پای دیجیتالی خود را مدیریت کرده و به حداقل برسانیم؟

این که هیچ رد پای دیجیتالی از خود در محیط آنلاین بر جای نگذارید، غیرممکن است اما اقداماتی برای به حداقل رساندن آنها می توانید انجام دهید. این اقدامات عبارتند از:

اجتناب از استفاده از آدرس ایمیل اصلی خود در زمان ایجاد اکانتها در وب سایتها و پلتفرمهای کامنت گذاری: آدرسهای ایمیل موقتی بسازید تا مانع از آن شوید کسی بتواند تصویری از سایتها و سرویسهایی که از آنها استفاده می کنید ایجاد کند.

تنظیم دقیق گزینه های حریم خصوصی در حسابهای رسانه اجتماعی: شاید لزومی نداشته باشد زندگی شخصی شما در معرض دید همه قرار گیرد بنابراین هر محتوایی را به اشتراک نگذارید. پستهای توییتر، فیس بوک و اینستاگرام را به دوستان یا تماسهای نزدیکتان محدود کنید و استفاده از پلتفرمهای رسانه اجتماعی که چنین اجازه ای را به شما نمی دهند را متوقف کنید.

جدا کردن شخصیهای شخصی و حرفه ای خودتان: این ایده خوبی است که آدرسهای ایمیل متفاوتی برای فعالیتهای شخصی و برای کاریابی و امور دیگر استفاده کنید. این امر تحقیقات کارفرمایان درباره حضور آنلاین شما را دشوارتر می کند.

مراقبت از شهرت و اعتبارتان: درباره پستها، اظهارنظرها و پیامهای آنلاینی که ارسال می کنید، دقت کنید زیرا نمایانگر شخصیت شما هستند. از عبارت و دستور زبان صحیح استفاده کرده و از بی ادبی و توهین اجتناب کنید. همچنین بیش از حد از خودتان اطلاعات ندهید. تصور کنید کارفرمای احتمالی تان اگر اطلاعاتی که پست کرده اید را مشاهده کند، درباره شما چه فکری خواهد کرد.

مخالفت با فروش اطلاعات از سوی وب سایتها: وب سایتها ابزارهایی را اضافه می کنند که به شما اجازه می دهند با فروش اطلاعات شخصی خود یا با اشتراک گذاری آنها با شرکایشان مخالفت کنید. اگر چنین کنترلهایی وجود دارند، دنبالشان بگردید و فعالشان کنید. به عنوان مثال می توانید در صفحه حریم خصوصی گوگل، توقف شخصی سازی تبلیغات بر اساس سلایق و نیازهایتان در سرویسهای گوگل را غیرفعال کنید.

عدم اتکا به حالت پرایوت یا محرمانه در وب سایتها: گزینه پرایوت مرورگرتان ممکن است برای به حداقل رساندن اطلاعاتی که در رایانه شخصی شما ذخیره می شود، مفید باشند اما برای رد پای دیجیتالی خود بیش از آن به این گزینه متکی نشوید زیرا تاثیری در اطلاعاتی که درباره شما در اینترنت ذخیره می شود، ندارد.