



مدیریت کردن دیجیتال فوت پرنٹ (Digital Footprint) خود

دیجیتال فوت پرنٹ شامل تمامی آنده از اطلاعاتی است که به دلیل فعالیت آنلاین شما در اینترنت وجود دارد. این اطلاعات شامل پست های شبکه های اجتماعی، گفتگوها، پیامها، تاریخچه مرور، ایمیلها، خریدهای آنلاین و اطلاعات موقعیت مکانی شما است، اما محدود به آن نیست. دیجیتال فوت پرنٹ شما می تواند:

- **تأثیر منفی بر کیز مهاجرت شما.** اکنون باید حساب های شبکه های اجتماعی، یوزرنیم/هیندل ها و سایر اطلاعات دیجیتال در ارتباط با بسیاری از درخواست های مهاجرت عمومی افشا شوند. همچنین، ممکن است دستگاه های الکترونیکی هنگام ورود به ایالات متحده یا در زمان توقیف توسط اداره امنیت داخلی (Department of Homeland Security) بررسی شوند. فعالیت آنلاین افراد می تواند در تصمیم گیری های مربوط به توقیف، اخراج، تنظیم وضعیت، کسب تابعیت، پناهندگی یا سایر اشکال کمک های مهاجرتی تأثیر گذار باشد.

- **خطر گرفتار شدن تان در کلاهبرداری را افزایش می دهد.** کلاهبرداران و افراد متقلب می توانند از دیجیتال فوت پرنٹ شما استفاده کنند تا شما را هدف قرار دهند، هویت شما را جعل کنند یا اطلاعات شما را سرقت کنند.
- **شما را در معرض نظارت قرار می دهد، از جمله توسط نهادهای دولتی و افراد سوء استفاده گر یا کنترل کننده.** این شامل دانستن موقعیت مکانی شما می شود، اگر موقعیت شما فعال باشد یا اگر در شبکه های اجتماعی "checking in" انجام دهید.
- **احتمال قربانی شدن را افزایش می دهد.** جنایتکاران از دیجیتال فوت پرنٹ افراد برای هدف قرار دادن و جذب آنها به شرایط کاری اجباری یا تحت فشار استفاده می کنند. بنیادگرایان و دیگر عاملان خطرناک نیز می توانند

مدیریت دیجیتال فوت پرنٹ شما برای مصوونیت، امنیت و شهرت شما بسیار مهم است!

12 نکته برای مدیریت دیجیتال فوت پرنٹ شما

- 1. از دستگاه ها و حساب های خود محافظت کنید.**
مطمئن شوید که تمامی دستگاه های شما دارای پسورد قوی هستند و ترجیحاً احراز هویت دو مرحله فعال باشد. احراز هویت دو مرحله زمانی است که دو روش تأیید وجود داشته باشد، مانند یک پسورد به همراه وارد کردن کدی که در تلفون موبایل خود دریافت می کنید.
- 2. اطلاعات خصوصی خود را به اشتراک نگذارید.**
نام کامل، آدرس، شماره تلفون یا سایر اطلاعات خصوصی خود را در انترنت، از جمله در شبکه های اجتماعی، منتشر نکنید.
- 3. اکاونت های خود را خصوصی کنید.** اگر اکاونت های شبکه های اجتماعی دارید، مطمئن شوید که آنها خصوصی هستند. معمولاً می توانید این کار را با رفتن به اکاونت خود، ورود به تنظیمات (Settings) یا بخش حریم خصوصی (Privacy) و انتخاب گزینه "خصوصی" (private) انجام دهید.
- 4. اکاونت های قدیمی را حذف کنید.** اگر دیگر از یک اکاونت استفاده نمی کنید، آن را حذف کنید. به همین ترتیب، ذخیره سازی کلاود یا اکاونت های موجود در دستگاه های قدیمی که هنوز دارید اما به ندرت از آنها استفاده می کنید را غیرفعال کنید.
- 5. تکرر یا ردیاب موقعیت مکانی خود را خاموش کنید.** برای غیرفعال کردن ردیابی موقعیت مکانی در یک دستگاه، به تنظیمات دستگاه بروید، که معمولاً در بخش "حریم خصوصی" (Privacy)، "امنیت" (Security) یا "موقعیت مکانی" (Location) قرار دارد. سپس، خدمات موقعیت مکانی را خاموش کنید تا اپلیکیشن ها و سرویس ها نتوانند مکان شما را شناسایی کنند.
- 6. میزان انتشار اطلاعات خود را محدود کنید.** حداقل مقدار اطلاعات را به صورت آنلاین منتشر کنید. مراقب باشید که چه چیزی را نشر می کنید، زیرا ممکن است برداشت اشتباه شود یا شما را در معرض خطر بالاتری قرار دهد. برای مثال، انتشار تصویری که نشان دهنده نوشیدن الکل یا در دست داشتن سلاح باشد و غیره.
- 7. درخواست های دوستی از افراد ناشناس را قبول نکنید.** مطمئن شوید که فقط درخواست های دوستی از افرادی را می قبول می کنید که واقعاً آنها را می شناسید. هر کسی می تواند پشت یک پروفایل مخفی شود، از جمله کلاهبرداران، قاچاقچیان و افرادی که قصد نظارت بر شما را دارند.

دوستانی را که شخصاً نمی شناسید از اکاونت های خود حذف کنید.

8. مواد حساس و اپلیکیشن ها را از تلفون ها و سایر دستگاه ها حذف کنید. اگر بیرون از کشور سفر می کنید، مأموران وزارت امنیت داخلی (Department of Homeland Security) ممکن است دستگاه های الکترونیکی را در هنگام ورود مجدد به ایالات متحده در نقاط ورود بررسی کنند. تمام پیام ها، عکس ها، اپلیکیشن ها و سایر مطالبی را که ممکن است به اشتباه تعبیر شوند، حذف کنید.

9. با امنیت ارتباط برقرار کنید. از اپلیکیشن های ارتباطی که رمزگذاری سرتاسری ارائه می دهند، مانند WhatsApp، Signal و Telegram، استفاده کنید.

نکته: با وجود امنیت بیشتر، حتی پلتفرم های پیام رسان رمزگذاری شده نیز می توانند از طریق متادیتای ذخیره شده، مانند اینکه با چه کسی و چه زمانی ارتباط برقرار می کنید، و همچنین محتوای به اشتراک گذاشته شده مانند ویدیوها، تصاویر و اطلاعات پروفایل، به دیجیتال فوت پرنس شما کمک کنند. مراقب باشید که چه چیزی را مکاتبه می کنید.

10. هنگام گشت و گذار در وب محتاط باشید. روی لینک های مشکوک از ارسال کنندگانی که نمی شناسید کلیک نکنید و به وب سایت های غیرقابل اعتماد نروید، زیرا این کار ممکن است شما را در معرض ویروس ها و نظارت احتمالی قرار دهد.

تنها اطلاعات ضروری را ارائه دهید و نسبت به وب سایت ها یا اپلیکیشن هایی که درخواست اطلاعات شخصی بیشتر از حد لازم دارند، بسیار محتاط باشید.

به شکل منظم کوکی ها و کش (cookies and caches) براوزر خود را پاک کنید. معمولاً می توانید این کار را با رفتن به تنظیمات براوزر (Browser's Settings)، سپس تنظیمات حریم خصوصی (Privacy Settings) و پیدا کردن گزینه "پاک کردن اطلاعات براوزر" (clear browsing data) یا گزینه مشابه انجام دهید.

11. از یک تلفون موبایل موقتی یا یک بار مصرف استفاده کنید. این تلفون ها معمولاً پیش پرداخت شده و به قرارداد خاصی متصل نیستند، که باعث می شود برای ناشناس ماندن و جلوگیری از ردیابی آسان تر باشند. با این حال، اگر از یک تلفون موقتی استفاده می کنید، حتماً مطمئن شوید که افرادی که نیاز دارند با شما در تماس باشند (مانند کیز اورکر [caseworker]، وکیل و غیره)، شماره روز شده شما را دارند. بعضی اوقات افراد تصمیم می گیرند دو تلفون داشته باشند – یک تلفون موقتی برای فعالیت های آنلاین و یک تلفون دائمی برای ارتباطات مهم و پایدار با افراد کلیدی.

12. از پوشش های کامره استفاده کنید. از پوشش های کامره در تلفون ها و لپ تاپ ها برای مسدود کردن لنز در زمانی که از آن استفاده نمی کنید بهره ببرید. این کار می تواند از تجاوز به حریم خصوصی جلوگیری کند.