**چگونگی تشخیص و جلوگیری از اسپم**

**چگونگی تشخیص اسپم**

تشخیص و جلوگیری از اسپم: در هنگام مطالعه این بخش، به آدرس‌های ایمیل واقعی موجود در مثال‌ها توجه زیادی داشته باشید. توجه کنید که همه آن‌ها بسیار طولانی هستند و تا حد زیادی از حروف و اعداد تصادفی تشکیل شده‌اند. این اقدام عمدی از طرف هرزنامه نویس است که به مبهم شدن هویت آن‌ها کمک شایانی می‌کند.

موارد زیر جهت تشخیص رایج‌ترین انواع ایمیل‌های اسپم موجود کمک قابل توجهی خواهد کرد:

* خدمات بهداشتی و درمانی: درمان‌های معجزه آسا، میانبرهای کاهش وزن، مکمل‌های غذایی با رندهای مشکوک، درمان‌های ریزش مو، راه حل‌های ضد پیری، داروهای جایگزین و بسیار از موارد دیگر اغلب توسط اسپمرها ارسال می‌شوند. اکثریت این محصولات چیزی بیش از وعده‌های پوچ نیستند.
* محتوای دوستیابی و بزرگسالان: این دسته همچنین زمینه‌های زیادی را شامل می‌شود، از خدمات دوستیابی آنلاین و آژانس‌های همسریابی گرفته تا وب سایت‌های بزرگسالان و افزایش عملکرد روابط جنسی.
* رایانه، اینترنت و فناوری: هرزنامه نگاران سعی می کنند از تعداد افرادی که متخصص کامپیوتر نیستند استفاده کنند. اجازه ندهید آن‌ها شما را با پیشنهادات نرم افزاری یا سخت افزاری، خدمات اینترنت یا تلفن همراه یا تبلیغات الکترونیکی عمومی فریب دهند.
* ثبت نام در سرویس: این موارد شامل اسپمر می‌شود که شما را متقاعد می‌کند تا در یک سرویس طولانی مدت ثبت نام کنید. برنامه‌های آموزشی و انواع بیمه‌ها موارد انتخابی آن‌ها هستند. توجه داشته باشید که چگونه از ایمیل به عنوان یک ابزار [مهندسی اجتماعی](https://softyab.com/%d8%aa%d8%b9%d8%b1%db%8c%d9%81-%d9%85%d9%87%d9%86%d8%af%d8%b3%db%8c-%d8%a7%d8%ac%d8%aa%d9%85%d8%a7%d8%b9%db%8c-%d8%a7%d8%b2-%d8%b2%d8%a8%d8%a7%d9%86-g-data/) استفاده می‌شود تا خواننده را در تصمیم گیری سریع سوق دهد.

نمونه‌ای از ایمیل‌های اسپم که طرح بیمه درمانی را تبلیغ می‌کند که به نظر می‌رسد این ایمیل هرزنامه توسط یک آژانس بیمه درمانی ارسال شده است.

* خدمات مالی و جوایز: سافت یاب به شما توصیه می‌کند از ایمیل‌هایی با پیشنهادات وسوسه انگیز مانند وام‌های کم بهره، کمک بدهی یا جوایز نقدی کامل، کاهش مشکلات پولی خرید نکنید!

قابل ذکر است، این مثال‌ها همه زوایای احتمالی را که هرزنامه نویس ممکن است به کار بگیرد نشان نمی‌دهد و فقط چند مورد از آن‌ها ذکر شده است.

[اسپم چیست؟](https://softyab.com/4557-2/)

**چگونه از اسپم جلوگیری کنیم**

جلوگیری از اسپم : هرزنامه‌ها نباید بخشی از زندگی دیجیتالی روزانه شما باشند. با چند نکته و ترفند ساده می‌توانید یاد بگیرید که چگونه ایمیل‌های اسپم را متوقف کنید و همچنین میزان ارسال هرزنامه‌هایی را که برای شما ارسال می‌شود کاهش دهید. در عین حال، نحوه مسدود کردن ایمیل‌های اسپم با جلوگیری از ظاهر شدن آن‌ها در صندوق ورودی شما را یاد خواهید گرفت.

* از عملکرد گزارش هرزنامه سرویس گیرنده ایمیل خود استفاده کنید. اکثر ارائه دهندگان رایانامه رایانه دارای یک دکمه مفید هستند که می‌توانید برای گزارش یک ایمیل به عنوان هرزنامه کلیک کنید. با این کار می‌توانید ایمیل خود را "آموزش دهید" تا در تشخیص هرزنامه‌ها بهتر عمل کند. هرگونه ایمیلی که از این طریق شناسایی شود مستقیماً به پوشه اسپم شما ارسال می‌شود و صندوق ورودی شما را به طور کامل دور می‌زند. اگر سرویس گیرنده ایمیل انتخابی شما به طور خودکار ایمیل‌های‌ هرزنامه و [فیشینگ](https://softyab.com/%d8%a2%d8%b2%d9%85%d9%88%d9%86-%d9%81%db%8c%d8%b4%db%8c%d9%86%da%af-%d8%a8%d8%b1%d8%a7%db%8c-%da%a9%d8%a7%d8%b1%da%a9%d9%86%d8%a7%d9%86-%d8%b3%d8%a7%d8%b2%d9%85%d8%a7%d9%86-%d9%87%d8%a7/) را تشخیص نمی‌دهد، به یکی از آنها بروید.
* برعکس، به مشتری ایمیل خود بگویید که کدام ایمیل‌ها هرزنامه نیستند. هر چند وقت یکبار به پوشه هرزنامه خود سر بزنید و اگر چیزی در آنجا پیدا کردید که متعلق به آن نیست، آن را به صندوق ورودی خود منتقل کنید. این به فیلتر هرزنامه شما کمک می کند تا یاد بگیرد کدام ایمیل‌ها را می‌تواند نادیده بگیرد.
* در بعضی موارد با آدرس‌های ایمیل یکبار مصرف یا جعلی ثبت نام کنید. بسیاری از سیستم عامل‌های تجارت الکترونیک و خدمات اینترنتی برای استفاده به آدرس ایمیل نیاز دارند. اگر کاملاً ضروری نیست، از ایمیل اصلی خود برای ثبت نام‌های دور ریز مانند صفحات فرود eBook یا برنامه‌های بازی استفاده نکنید. شما هرگز نمی دانید چه کسی می خواهد آن را به یک اسپمر بفروشد.
* به هیچ وجه با هرزنامه‌ها درگیر نشوید. این امر نه فقط بر روی ایمیل‌ها بلکه در مورد همه نوع اسپم صدق می‌کند. روی پیوندها کلیک نکنید، پیوست‌ها را بارگیری نکنید و هرگز به هرزنامه‌ها پاسخ ندهید. اگر این کار را بکنید، ممکن است آن‌ها را به این باور برساند که آن‌ها موفق شده‌اند، به این معنی که آن‌ها برای شما هرزنامه بیشتری ارسال می‌کنند.
* اطلاعات تماس خود را منتشر نکنید هرزنامه‌ها می‌توانند مخاطبین را آنلاین پیدا کنند و می‌کنند. تمام تلاش خود را بکنید تا آنجا که ممکن است حضور آنلاین خود را خصوصی نگه دارید. این امر به شماره تلفن و آدرس فیزیکی شما نیز کشیده می‌شود.
* اگر شخصی که می‌شناسید برای شما اسپم ارسال کرده است،، به او اطلاع دهید. اگر پیام ناخواسته ای از مخاطب مورد اعتماد دریافت کرده‌اید، به آنها بگویید که حساب آن‌ها هک شده و برای ارسال هرزنامه استفاده شده است. به این ترتیب، آنها می‌توانند اقدامات اصلاحی را انجام دهند و کنترل را دوباره به دست آورند.
* در صورت مدیریت وب سایت، از نرم افزار و اقدامات امنیتی فعلی استفاده کنید. نرم افزار وب سایت خود را به روز نگه دارید تا از خود در برابر اسپم‌هایی که به دنبال سوء استفاده از آسیب پذیری هستند محافظت کنید. در عین حال، فناوری Captcha را در صفحات ورود، نظرات و سایر مناطق تعاملی پیاده سازی کنید.

**با** [**معتبرترین آنتی ویروس جهان**](https://softyab.com/product-brand/bitdefender/) **در امان باشید**

**تشخیص و جلوگیری از اسپم**

با میلیاردها پیام هرزنامه که هر روز ارسال می‌شود، حتی هوای بسته شده صندوق ورودی نیز دیر یا زود نشت می‌کند. مطمئن شوید که در برابر پیوندهای ناخواسته و پیوست هایی که ممکن است برای دستگاه شما مضر باشند، محافظت می شوید. [Bitdefender](https://softyab.com/product-brand/bitdefender/) بدافزار را با یک دفاع دو طرفه شناسایی و مسدود می‌کند: Web Shield برای تهدیدات مبتنی بر اینترنت و File Shield برای هر چیزی که در حال حاضر در رایانه شما وجود دارد.

شبکه اطلاعات تهدید جهانی مبتنی بر هوش مصنوعی ما را قادر می سازد تا از 400 میلیون نفر در سراسر جهان محافظت کنیم.

منبع: [A](https://www.avast.com/c-spam)vast

لطفا جهت مشاوره در [انتخاب آنتی ویروس مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[اجتماعی](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**