**تعریف فیشینگ و اسپم**

**تفاوت بین فیشینگ و اسپم**

فیشینگ رایج ترین شکل حمله سایبری است که در آن قربانیان از طریق ایمیل، پیام‌های متنی که به نظر می‌رسد از طرف منبع یا سازمان موجهی برای افشای اطلاعات شخصی، مانند شماره‌های تأمین اجتماعی، حسابهای بانکی، شماره کارتهای اعتباری، گذرواژه‌های حساب و موارد دیگر هستند، مردم را فریب می‌دهند.

اسپم یک معادل الکترونیکی از ایمیل‌های ناخواسته است که به طور معمول برای ارسال بدافزارها، انجام حمله فیشینگ یا تبلیغات برای افراد زیادی ارسال می‌شود. هرزنامه عموماً ارسالهای گروه خبری ناخواسته است که تبلیغات ایمیل را برای نوعی محصول یا خدمات نشان می‌دهد.

در حالی که مردم اغلب ایمیل‌های اسپم را غیراخلاقی می‌دانند، اما بسیاری از مشاغل هنوز از ایمیل‌های اسپم برای اهداف تجاری استفاده می‌کنند، زیرا هزینه هر ایمیل فوق العاده پایین است و مشاغل می‌توانند مقادیر زیادی را به طور مداوم ارسال کنند. هرزنامه‌ها را می توان به صورت گسترده توسط بات نت‌ها، که شبکه‌های رایانه‌های آلوده هستند، ارسال کرد.

فیشینگ با یک ایمیل متقلبانه یا سایر ارتباطات که برای جلب قربانی طراحی شده است شروع می‌شود. این پیام طوری ساخته شده است که انگار از طرف یک فرستنده معتمد است. اگر قربانی را گول بزند، او را مجبور به ارائه اطلاعات محرمانه می‌کند. گاهی اوقات بدافزار روی رایانه قربانی بارگیری می‌شود.

شباهت و تفاوت اسپم و فیشینگ

هر دو اسپم و فیشینگ به مهندسی اجتماعی مربوط می‌شوند، یک اصطلاح کلی برای هرگونه فعالیتی که در آن مهاجم سعی می‌کند اطلاعات شخصی شما فاش شود. گذرواژه‌ها، اطلاعات حساب، شماره‌های امنیت اجتماعی قبل از ارائه این اطلاعات باید دوبار فکر کنید. همیشه تأیید بگیرید که واقعاً در آن طرف خط کیست.

هرزنامه‌ها معمولاً بی ضرر هستند در حالی که، فیشینگ قصد تخریب دارد. ایمیل‌ها یا تماس‌های اسپم معمولاً سعی می محصول یا خدماتی را به شما بفروشند، اما کلاهبرداری‌های فیشینگ تلاش می‌کنند اطلاعات شخصی شما را برای انجام کلاهبرداری یا حملات سایبری به دست آورند. بنابراین، به عبارتی، فیشینگ نوعی هرزنامه است، هرچند نوعی با قصد مخرب.

**هدف از فیشینگ در مقابل اسپم**

اسپم نوعی تبلیغات تجاری در قالب ایمیل است زیرا ایمیل هنوز هم یکی از مقرون به صرفه ترین وسیله تبلیغات است. هدف از ارسال اسپم ارسال ایمیل های تجاری با محتوای تجاری به صورت عمده به صورت عمده به منظور کسب درآمد از گیرنده‌هایی است که در واقع به ایمیل‌ها پاسخ می‌دهند.

فیشینگ برخلاف هرزنامه، فقط به ایمیل محدود نمی شود. فیشینگ در بین مجرمان سایبری کاملاً مشهور است و به دنبال بدست آوردن اطلاعات حساس یا کنترل سیستم آنها، افراد را قادر می سازد با کلیک بر روی لینک های مخرب، اطلاعات مورد نیازشان را در اختیارشان قرار دهند.

**تکنیک های اسپم و فیشینگ**

حملات فیشینگ بصورت پیچیده‌ و سازمان یافته برنامه ریزی و اجرا می‌شوند. آن‌ها با دقت طراحی شده‌اند تا قربانیان را در به اشتراک گذاشتن یا آشکار کردن اطلاعات شخصی خود مانند ورود و رمز ورود، فریب دهند تا مهاجم بتواند کنترل جهان آنلاین قربانی مانند سایت‌های شبکه‌های اجتماعی‌، حساب‌های بانکی، ایمیل و موارد دیگر را به دست آورد.

هرزنامه‌ها محتوای واقعی ایمیل‌ها را پنهان می‌کنند تا قربانیان پول خود را برای کالاهایی که در حقیقت کالاهای جعلی یا تقلبی نیستند و بیشتر تبلیغاتی مانند مواد دارویی یا گاهی نرم افزار امنیتی هستند، خرج کنند.

**تفاوت بین ایمیل‌های اسپم و فیشینگ**

برای اینکه بتوانید تفاوت بین اسپم و فیشینگ را بهتر درک کنید، مشاهده آنها در کنار هم در جدول ذیل مفید خواهد بود.

|  |  |  |
| --- | --- | --- |
|  | فیشینگ | اسپم |
| هدف | برای کلاهبرداری از کاربران | برای تبلیغ و بازاریابی محصولات و خدمات |
| ماهیت | پیام‌های گمراه کننده‌ای که به نظر می‌رسد از نهادهای قانونی آمده اما ماهیتی مخرب دارند. | ایمیل‌های تجاری ناخواسته که معمولاً ماهیتی خوش خیم دارند اما گاهی اوقات می‌توانند مخرب باشند |
| محتوی | پیوست‌های بارگذاری شده از بدافزار، لینک‌های آلوده، لینک‌هایی که به وب سایت‌های ناخواسته هدایت می‌شوند، پیام‌های فریبندهای که گیرندگان را وادار می‌کند تا اطلاعات مالی PII خود را به اشتراک بگذارند. | تبلیغات محصولات/خدمات، کدهای کوپن، معاملات، تخفیف‌ها، فرمهای پرس و جو یانظرسنجی |
| قانون گذاری | قوانین مختلف ایالتی، قوانین جزایی فدرال ایالات متحده | قانون بازاریابی و پورنوگرافی بدون درخواست ایالات متحده در سال 2003 برای سایر کشورها: قوانین ضد هرزنامه |

منبع: [sectigostore](https://sectigostore.com/blog/spam-vs-phishing/)

مقاله فوق را به رایگان دانلود کنید

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.**