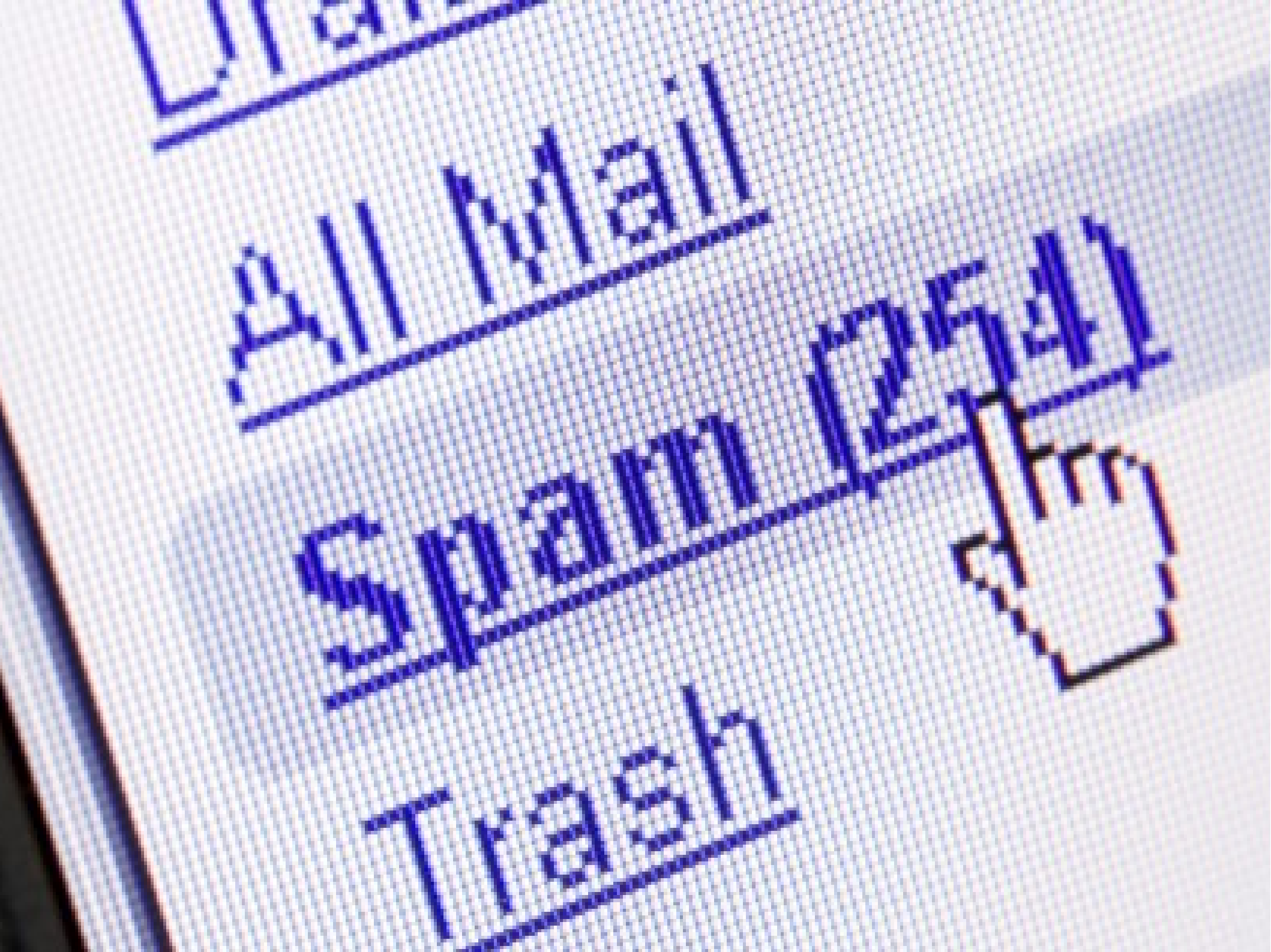

تحلیل اسپم ها و چگونه با اسپم ها مبارزه کنیم

محمد رضا کمالی فرد

ایمیل چیست

- ایمیل یک راه هست برای انتقال نامه های دیجیتال رو شبکه
- نسخه های اولیه ایمیل که ارائه شد نیاز داشتن که هم زمان فرستنده و گیرنده آنلاین باشن تا ایمیل فرستاده بشه درست مثل IM
- بعد تر مدل Store and forward اومد که در اون ایمیل ها به سرور ها مقصد فرستاده میشدن و اونجا آرشیو می شدن.
- ایمیل از وب قدیمی تره و قبل تر از اون بوده حتی اوایل توسعه وب از e-mail delivery برای گرفتن صفحات استفاده می شد.
- ایمیل ها از نظر محتوا دو دسته اند یا متن ساده اند یا HTML ایمیل هستند.
- فرستادن ایمیل شبیه سازی شده از فرستادن نامه های معمولی هست وقتی دکمه ارسال رو بزنین کامپیوتر شما با mail host تماس می گیره و با پروتکل SMTP ایمیل رو می فرسته اون میل ایجنت ایمیل رو با SMTP به mail host مقصد می فرسته و در نهایت به mail delivery agent تحویل داده میشه
- ایمیل از بخش های Header و Body و Attachment تشکیل شده بخش هدر نگه داره اطلاعات گیرنده و فرستنده و اطلاعات مسیریابی هست Body هم متن نامه ارسالی هست.

اسپم چیست

- به هر ارتباط ناخواسته ای اسپم می گن
- ایمیل اسپم ها یا هرزنامه ایمیل هایی هستن که به صورت ناخواسته برای افراد فرستاده میشن.
- اسپم ها بیشتر برای اهداف تبلیغاتی فرستاده میشن اما اهدافی مثل بدست آوردن اطلاعات شخصی شما و فروش اونها به شرکت ها از اهداف دیگر اونهاست.
- تجارت اطلاعات هویتی و رفتار انسان ها بسیار سود آور هست.
- ۹۴ درصد تبلیغات دیجیتال از طریق اسپم هاست.
- بیشتر افراد که سن کمی دارن یا مسن هستند نمی دونن اصلا اسپم چی هست

اسپم چه ضرر هایی دارد

- بیشتر ایمیل های ناخواسته خطری ندارند و آسیبی جدی ای وارد نمی کنن اما اسپم ها خیلی زود مثل قارچ رشد می کنن و زیاد می شن انقدر اینباکس شما رو شلوغ می کنن که اعصابتون کاملا خورد میشه یا مثلا نوع خطرناکترشون می تونه با ترفند های مهندسی اجتماعی و کسب اعتماد شما اطلاعاتی در مورد هویت یا کارت اعتباری تون درخواست کنه و در خوشبینانه ترین حالت اطلاعات هویت شما رو به بقیه اسپمر ها بفروشه یا دست به دزدی از کارت اعتباریتون بزنه.
- روزانه بیش از ۲۰۰ میلیارد ایمیل اسپم ارسال میشه بخش امنیتی مایکروسافت اعلام کرده که بیش از ۹۷ درصد ایمیل ها که روزانه ارسال میشن ناخواسته هستن.
- ایمیل های اسپم تاثیر منفی زیادی روی بهره وری افراد و سیستم ها اداری می ذارن و هر سال ملیون ها دلار به صنایع ضرر می زنن.
- بیشتر ایمیل های اسپم به وسیله شبکه های بات نت و از کامپیوتر کاربران عادی ارسال میشه .بیشترشون ویندوزی هستن :دی اما خوب بات نت لینوکسی هم داریم :(

مقابله با اسپم ها

شناخت روش های اسپمر ها

- اسپمر ها باید آدرس شما رو پیدا کنند و طوری به شما ایمیل بفرستند که ایمیل داخل پوشه اسپم نره. اگه این اتفاق بیفته یه اسپم موفق انجام شده.
- اسپمر ها از موتور های جستجو خاص و اسکریپت ها برای پیدا کردن آدرس های ایمیل در آدرس های مختلف وب استفاده می کنند.
- اونا از برنامه های خاصی هم استفاده می کنن که اسم آدها رو جستجو می کنه و با روش هایی از این اسامی ایمیل های تصادفی می سازه.
- اسپمر ها از گروه های ایمیلی هم برای پیدا کردن آدرس افراد استفاده می کنند.
- اسپمر ها ایمیل های مشاغل و افراد خاص رو از سایت ها و شرکت های مختلف می خرند.معمولا سایت های خرید و فروشگاه های اینترنتی از این دست هستند.

اسپمر هاچطور ناشناس می مونند

- روش معمول برای اسپم کردن این هست که این افراد معمولا یه SMTP سرور را می اندازن.
- بعد برای این که ناشناس بمونن در حقیقت از پراکسی ها استفاده می کنن یا از کامپیوتر های قربانی های بات نت برای مخفی موندن آدرس اصلی شون استفاده می کنن.
- با دست بردن در هدر ایمیل برای افراد مختلف آدرس های مختلفی به عنوان فرستنده در نظر می گیرن و با عوض کردن اطلاعات مسیریابی سیستم کنترل اسپم رو فریب می دهند.
- با نوشتن عنوان های حرفه ای برای ایمیل سیستم های ها کنترل اسپم رو فریب می دهند.
- سعی می کنن به ایمیل سر و شکل حرفه ای بدن تا اعتماد خواننده رو برای خواندن ایمیل جذب کنن حتی از شکل های اچ تی ام ال استفاده می کنن.

روش های شناسایی اسپمر ها

- معمولا به دو روش هست روش های در سطح مدیران شبکه و روش های درسطح کاربران که به دو نوع دستی و خودکار تقسیم میشه.

روش های سطح مدیران شبکه

- لیست های DNSBLکه در اون آدرس آی پی های فرستندگان اسپم نگهداری میشه.
- استفاده از آدرس های دروغین که در اینترنت به صورت کلی انتشار داده میشود تا بعد از استفاده اسپمر ها از این آدرس ها بتونن اونها رو شناسایی کنند (spamtrap)
- کنترل کردن رعایت استاندارد های کامل SMTP که در استاندارد های RFC اومده. با توجه به این که کامپیوتر های درون یه بات نت از برنامه های ساده و بسیار کوچیک برای کنترل ارسال ایمیل استفاده می کنن احتمالا تمام استاندارد ها در اونها رعایت نمیشه.
- میل سرور ها برای کنترل برنامه فرستنده ایمیل یک تاخیر عمدی در فرستادن SMTP greeting banner ایجاد می کنن. طبق استاندارد فرستنده ایمیل باید تا دریافت این بنر صبر کند و بعد ایمیل را ارسال کند.اما اسپمر ها معمولا به خاطر نیاز به سرعت بالا در ارسال بلافاصله بعد از برقرای ارتباط با سرور مقصد اطلاعات رو متنقل می کنند.همچنین باید ارتباط از طریق دستور Quit پایان یابد ولی اسپمر ها معمولا این کار را نمی کنند
- چک کردنMXرکورد های هدر یک ایمیل در هر مرحله و تایید حقیقی بودن فرستنده ها
- مطابقت دادن متن پیام با الگو های اسپم و گشتن به دنبال کلمات خاص

اسپم فیلتر

- مهمترین نکته در مقابله با اسپم شدن استفاده از یه سرویس ایمیل هست که فیلترهای خوبی برای شناسایی و جدا کردن ایمیل های اسپم از دیگر ایمیل ها داشته باشه.
- اگر از میل سرور شخصی برای ارسال ایمیل استفاده می کنید هم برنامه های رایگان و غیر رایگان برای کنترل اسپم ها وجود دارند که باید از آنها استفاده کنید.
- برنامه اپن سورس spamassassin یکی از بهترین هاست
- جیمیل سرویس ایمیل گوگل دارای فیلتر قوی است که با روش های گوناگون و خاص ایمیل های اسپم رو مشخص می کند.

آدرس اصلی ایمیل تان را منتشر نکنید

- آدرس ایمیل اصلی تون رو به صورت متن ساده و به شکل عمومی در اینترنت منتشر نکنید تا موتور های جستجوی اسپمر ها نتونن ایمیلتون رو پیدا کنند. ایمیلتون رو در وب سایت ها چت روم ها و لیست های پستی به صورت متنی وارد نکنید تا نرم افزار های جستجو اون ها رو پیدا کنند.
- برای ثبت نام در هر فرمی در اینترنت از ایمیل واقعی خودتون استفاده نکنید خیلی از این فرم ها توسط اسپمر ها طراحی شدن و شما بعد از ثبت نام ایمیل خودتون رو در اختیار این افراد قرار می دین خیلی از این فرم ها در حقیقت نرم افزار ها خودکاری هستند که ایمیل شما را در دسته مربوطه قرار می دن و بلافاصله شروع به ارسال اسپم می کنند یا اینکه آدرس ایمیل شما را به دیگر اسپمر ها می فروشن.
-

چند آدرس ایمیل بسازید

- می تونین تعداد زیادی ایمیل های عمومی بسازین و اونها رو به یک ایمیل فوروارد کنید بهترین راه استفاده از جمیل هست که ضمن رایگان بودن امنیت بالایی رو هم داره و همیشه از پروتکل های امن برای انتقال تمامی اطلاعات شما استفاده می کنه.البته این امکان برای اکثر برنامه های مدیریت ایمیل وجود داره.
- از آدرس هایی برای ایمیل خودتون استفاده کنین که امکان تصادفی ایجاد کردن اونها نباشه مثلا نرم افزارهایی که برای اسپمر ها آدرس می سازند با ترکیب اسمتون سعی می کنن یه آدرس صحیح از شما ایجاد کنند.
- ایمیل هایی که می دونین ناخواسته رو باز نکنید هیچ موسسه ای خبر برنده شما در قرعه کشی یا مسابقه ای بزرگ رو در حالی که حتی درش شرکت نکردین برای شما ایمیل نمی کنه مواظب باشید تا در دام افراد باهوش نیفتید.

در عصر ۰ و ۱ خرافاتی نباشید

- یکی از شیک ترین راه هایی که اسپمر ها برای به دست آوردن آدرس ایمیل قربانی ها به کار می گیرن درست کردن ایمیل های زنجیری هست.
- ایمیل هایی که شما رو معمولا به دلیل خرافات تحت تاثیر قرار می دن مثلا ایمیل هایی که می گن اگه این رو به ۱۰۰ نفر بفرستی یه خبر خوب می شنوی شما رو وادار می کنن که این ایمیل رو برای تعداد زیادی از دوستان بفرستید به این صورت هر بار که این ایمیل فرستاده بشه تعداد بیشتری آدرس ایمیل در اختیار اسپمر ها قرار می دین.
- اگر می خواین یه ایمیل به صورت گروهی بفرستین آدرس دوستا تون رو در قسمت BCC قرار بدین تا مخاطب ها به آدرس های دیگر افراد دسترسی نداشته باشه.

رفتار با ایمیل های اسپم

- اگه مطمئن هستین که یه ایمیل اسپم هست هیچقوت اون رو باز نکنید. و از دکمه اسپم استفاده بکنید.
- روی دکمه Unsubscribe کلیک نکنید یا به ایمیل اسپم جواب ندید چون که از این طریق نرم افزار ارسال کننده اسپم متوجه میشه که شما ایمیل ها رو دریافت می کنین و ایمیل های اسپم بیشتری رو براتون می فرسته.
- ایمیل ها رو به صورت متن ساده بخونین و نگذارید که کد های HTML اجرا بشن . (این تنظیم معمول خیلی از سرویس های رایگان ایمیل هست)
- اگر کد ها رو اجرا کنید ممکن هست که روی لینک های دانلود نرم افزار های مخرب کلیک کنید و دچار آسیب بشید.

ایجاد آدرس های چند گانه در جیمیل

- در جیمیل می تونین با داشتن هر آدرس ایمیل از اون تعداد بسیار زیادی آدرس بسازید و اون رو در فرم های مختلف اینترنتی بگذارید.
- مثلا اگه آدرس جیمیل من kamalifard@gmail.com باشه می تونم با گذاشتن " . " در بین حروف آدرس های جدید ایجاد کنم مثل این ها
- Kamalifar.d@gmail.com-Kamali.fard@gmail.com-K.amalifard@gmail.com
- می تونیم با اضافه کردن متنی به آخر آدرس ایمیل با " + " هم آدرس های جدید بسازیم.
- نکته مهم اینجا این هست که می تونیم آدرس هر سایت رو + کنیم تا اگه روزی سایتی ایمیل ما رو در اختیار اسپمر ها قرار داد بفهمیم و همچنین به راحتی با یه فیلتر بتونیم کل ایمیل های ارسالی به اون آدرس رو دور بریزیم.
- kamalifard+tehlug@gmail.com

حالا من می تونم با ایجاد یک فیلتر ایمیل هایی که این سایت می فرسته رو دسته بندی کنم و اگر روزی برای من اسپم فرستاد ایمیل های این آدرس رو دور بریزم.

مراقب حملات فیشینگ باشید

- در حملات فیشینگ افراد سعی می کنند با فرستادن یک ایمیل شما را به صفحه ورود یک سایت معتبر یا صفحه ورود اطلاعات بانکی راهنمایی کرده و با شبیه سازی یک سایت دیگر به جای سایت اصلی اطلاعات شما را بدزدند.
- مراقب باشید هیچوقت مدیران شبکه با فرستادن ایمیل از شما درخواستی در رابطه با رمز عبور قبلی و اطلاعات شخصی نخواهند داشت
- ایمیل هایی که می دونین ناخواسته رو باز نکنید هیچ موسسه ای خبر برنده شما در قرعه کشی یا مسابقه ای بزرگ رو در حالی که حتی درش شرکت نکردین برای شما ایمیل نمی کنه مواظب باشید تا در دام افراد باهوش نیفتید.

منابع

- En.wikipedia.org/wiki/E-mail_spam
- News.bbc.co.uk/2/hi/technology/7988579.stm
- Sophos.com/en-us/press-office/press-releases/2008/07/dirtydozjul08.aspx
- Guardian.co.uk/technology/2011/jan/10/email-spam-record-activity
- Googlesystem.blogspot.com/2007/10/how-gmail-blocks-spam.html
- Gmailblog.blogspot.com/2008/03/2-hidden-ways-to-get-more-from-your.html
- howtospamsomeonesemail.com

Mohammad reza Kamalifard