Medidas para combatir o SPAM

O correo electrónico non desexado (SPAM)

O envío de correos non desexados, ou SPAM, é unha das formas máis habituais e molestas de abuso de servicio de correo electrónico. Os correos de publicidade non desexada saturan os servidores de correo e as contas dos usuarios/as, ocasionando unha seria degradación do servizo prestado. Segundo algunhas estatísticas, máis da metade do correo electrónico que circula por internet é spam.

Por outra banda é cada vez máis frecuente que parte de este correo non desexado consista en intentos de fraude (phishing), para obter os datos da conta do usuario para empregala en posteriores envíos de SPAM, ou para obter outro tipo de información (persoal, datos bancarios, etc.).

Como reducir o SPAM recibido na súa conta de correo

Medidas para evitar o SPAM

As persoas dedicadas a este tipo de abusos (spammers) dedícanse a buscar enderezos en páxinas web, grupos de discusión, correos encadeados, etc... O seu obxectivo é enviar o maior número de mensaxes, esperando que alguén se interese. Hai varios frontes para combater o spam, pero o máis efectivo é sen dúbida a prevención ou evitación.

Isto implica que **ten que tentar evitar que os spammers capturen o seu enderezo de correo**. Para iso a solución non pasa por instalar ningún programa concreto, senón que o camiño que debe seguir é cumprir unhas poucas regras básicas imprescindibles. A continuación detállanse as máis importantes:

1. **Ocultar o seu enderezo de correo en páxinas web**

   Un dos métodos máis empregados polos spammers son programas que percorren internet na busca de direccións de correo dentro das páxinas web. Evite na medida do posible que o seu enderezo de correo apareza en moitas páxinas web. Nunca engada o seu enderezo nunha web en modo texto nin cun enlace "mailto". Ten que evitar engadila no formato habitual. No seu lugar pode publicala empregando algunha das seguintes ideas:

   - Empregando unha imaxe.
     Pode xerar automáticamente unha imaxe co seu enderezo de email premendo aquí
   - Póndoa en forma descriptiva. Por exemplo, unha forma moi común de amosar o enderezo webmaster@uvigo.es sería ***webmast er arroba uvigo dot es.***
   - Un terceiro método algo máis complexo podería ser construir o enderezo de correo concatenando caracteres en formato decimal ou hexadecimal, en especial a arroba.
     Pode xerar unha representación deste tipo do seu enderezo premendo aquí

   En xeral trátase de de amosar o enderezo de correo nun xeito entendible polos humanos e que non sexa entendible ou fácilmente adiviñable por un programa informático. A mesma norma débese estender a foros, chats, grupos de noticias etc. Poden ver varios exemplos de cómo **NON** publicar as direccións de correo nas súas páxinas web premendo aquí.
2. **Nunca responda a mensaxes de correo basura nin prema nos seus enlaces**

   Non responda a ningunha mensaxe lixo nin abra as páxinas nas que o invitan a obter máis información ou a borralo da lista. Con ísto o único que consegue é confirmarlles a existencia do seu enderezo e enviaranlle moitas máis mensaxes. En xeral é desaconsellable responder a mensaxes non solicitadas que resulten sospeitosas, en especial se son de descoñecidos.
3. **Non facilite o enderezo da uvigo a páxinas de pouca confianza ou alleas á Universidade.**

É aconsellable ter unha segunda conta de correo gratuíta do tipo yahoo, hotmail etc. para facilitala en sitios web que non sexan da Universidade ou dun organismo de confianza. Deste xeito o seu enderezo de correo só vai ser coñecido polas súas amizades e contactos profesionais. É aconsellable ler a política de privacidade da empresa antes de facilitarlle os datos, xa que poden ter contempladas cesions de datos a terceiros.

4. **Non participar na difusión de mensaxes encadeadas**

   Debe ignorar o contido de mensaxes nas que se apela á súa caridade, o avisan de peligrosos virus e lle indican que os reenvíe a outras persóas con urxencia. Tampouco debe reenviar mensaxes graciosas ou enxeñosas que lle envíen os seus coñecidos. Todos estes tipos de mensaxes sérvenlle aos spammers para recopilar milleiros de enderezos de correo que se van engadindo á mensaxe a medida que ésta se difunde.

5. **Non deixar visibles as direccións de correo en mensaxes dirixidas a moitos destinatarios.**

   Enviar unha mensaxe que vai dirixida a moitas persoas, (milleiros se engadimos aos destinatarios a algunha listas como comunidade), ten un risco potencial de que poida ser coñecido o noso enderezo. Por exemplo, varias desas persoas poden ter infectado o ordenador con calquera verme que envíe spam ou facilite enderezos de correo a spammers.

   O problema principal ocorre cando alguén manda unha mensaxe dirixida a unha lista grande de direccións de varios dos seus contactos ao mesmo tempo. Está expondo publicamente os enderezos desas persóas sen o seu consentimento e pódelles causar un prexuízo. Por iso, é comunmente considerado como medida de cortesía engadir as listas de enderezos no campo "**CCO**" (copia oculta) e non no campo "**Para**". Deste xeito evítase que os destinatarios podan verse entre eles.

6. **Elixir unha dirección de correo que non sexa fácilmente adiviñable**

   Os spammers utilizan programas para descubrir enderezos de correo que van probando distintos enderezos de correo inventados. Se o seu enderezo é moi curto ou moi común ou intuíble é moi probable que o adiviñen sen necesidade da súa intervención. Por exemplo, enderezos como pepe, gonzalo, monica ou nominas van existir en calquera empresa, e van ser descubertas moi cedo e por moitos spammers. En xeral débese evitar por enderezos que **só consten dun nome propio, un apelido, alcumes, diminutivos, nomes de departamentos**, etc. Outra medida necesaria é **evitar nomes de usuario de menos de cinco letras**. Teñen algoritmos que van probando todas as combinacións de letras, polo que contas cun nome demasiado curto non son aconsellables.

7. **Empregar un lector de correo que non descarge automáticamente as imaxes**

   En ocasións, a visualización dunha imaxe é un medio que confirma que se leu a mensaxe. É moi aconsellable que o lector de correo non amose automáticamente estas imaxes. As últimas versións dos lectores de correo máis populares xa o fan de forma predefinida.

Medidas para combater o SPAM

Mover as mensaxes marcadas como SPAM a un cartafol separado

Cando xa está recibindo mensaxes de spam na súa conta de correo, as medidas que debe tomar pasan por aplicar algún filtro que sexa capaz de detectar cales das mensaxes recibidas son spam para sometelas a algún tratamento especial que evite a molestia que causan. Nos nosos servidores principais de correo dispomos dun filtro antispam capaz de detectar unha alta porcentaxe dos correos lixo.

O principal perigo de empregar filtros é a posibilidade de que existan falsos positivos. É dicir, pode resultar que se detecte como spam algún correo lexítimo. Aínda que isto sexa pouco probable, supón un problema moi importante, en especial se se trata dunha dirección de contacto dun servizo ou departamento.

Os correos detectados como SPAM trátanse de dous xeitos distintos:

- Se a probabilidade de que sexan SPAM é moi alta ou se incumpren reglas básicas (envío dende servidores non autorizados para un dominio) rexéitanse as mensaxes
- O resto das mensaxes que o filtrado do correo considera como SPAM márcanse engadindo, ó principio do título do correo a cadea: "[Posible SPAM]"

As mensaxes marcadas como "[Posible SPAM]" chegarán ó buzón do usuario, o máis práctico é movelas automáticamente a un cartafol separado:

- **Se usa o correoweb da Universidade**:

  Este pode mover automáticamente estas mensaxes ó cartafol "SPAM"

  Compre habilitar esto como se indica *nesta páxina*.

  Compre que revise e baleire periódicamente este cartafol.

- **Se usa Outlook ou Mozilla:**

  Ten que definir unha regra que detecte no título da mensaxe que este comenza por "[Posible SPAM]" e que meta esas mensaxes nun cartafol separado.Pode atopar un titorial de cómo facelo no Outlook 2003 *nesta páxina*.

Denunciar o SPAM

O correo recibido como SPAM e non detectado como tal polos filtros antispam poden envialo á dirección: denuncias-spam@uvigo.es

Esta dirección reenvía os correos ó fabricante do filtrado antispam para que o empregue para a aprendizaxe automática dos seus filtros.

En caso de que consideren que pode tratarse dun incidente de seguridade poden denuncialo á dirección abuse@uvigo.es

Os usuarios poden establecer as súas propias regras de filtrado non cliente de correo ou no filtrado antiSPAM empregado pola Universidade de Vigo e, se o consideran conveniente ou teñen dúbidas ó respecto, consultar ou denunciar a recepción de estas mensaxes ó administrador do servizo de correo electrónico: postmaster@uvigo.es

Problemas habituais

Correos en "cuarentena"

En ocasións algúns filtros de emerxencia (para frenar tipos de virus ou correos de phishing non detectados correctamente por outros mecanismos), serán retidos polo filtro antispam, Lavadora de RedIRIS.

Nestes casos o usuario recebirá unha mensaxe indicando esta situación, e poden consultar e desbloquear as mensaxes retidas dende:

https://user.puc.rediris.es/m/webmail/

Este servidor está administrador por Red.es e é totalmente seguro, non supón, neste caso, un problema de seguridade o introducir aquí as súas credenciais (usuario de correo e contrasinal).

Deben ter en conta que os arquivos liberados poden ser potencialmente perigosos ⚠️

Falsos positivos

O sistema de filtrado antispam pode ter ocasionalmente falsos positivos, mensaxes que sen ser SPAM son detectadas como tal polos servidores de correo.

Poden enviar ós falsos positivos á dirección: non-e-spam@uvigo.es (no-es-spam@uvigo.es). Estes correos reenvíanse ó fabricante do filtrado antispam para que o empregue para a aprendizaxe automática dos seus filtros.

Os meus correos son rexeitados: SPF ("not permitted to send mail from uvigo.es")

Un dos mecanismos empregados para limitar o SPAM e o envío de SPAM con remitentes falsificados do dominio @uvigo.es e subdominios e a publicación de rexistros SPF, que indican que equipos poden enviar correo empregando estes remitentes, e que está limitado ós servidores de correo controlados pola Universidade de Vigo.

Se un usuario se atopa no exterior da Universidade de Vigo pode empregar, para enviar o correo:

- O acceso web ó correo
- As configuracións recomendadas en: "Datos de configuración dun cliente de correo"

Se tenta enviar este correo dende outros equipos este pode ser rexeitado, indicando unha mensaxe do tipo de algunha das seguintes(pode variar):

```
host servidor.dominio.es[a.b.c.d] said: 550 [SPF] 1.2.3.4 is not allowed to send mail from uvigo.es. (in
reply to RCPT TO command)
```

```
SPF=FAIL: (envelope from: ...@uvigo.es) indicates that MTA (a.b.c.d) is not permitted to send email for
uvigo.es
```

⚠️ Se empregan aplicacións externas (publicacións electrónicas, aplicacións de terceiros), dende as que precisen enviar correos co seu remitente de correo de @uvigo.es este poder ser rexeitado. Se se quere evitar esto o proveedor ou responsable de esa aplicación pode tomar calquera das seguintes medidas:

- **Empregar como remitente SMTP ("envelope sender") un calquera do seu dominio** (noreply@dominio.com, nobody@dominio.com, aplicacion-xxx@dominio.es, etc.) e indicar a dirección do usuario (usuario@uvigo.es) na cabecera que indica o remitente do correo ("From:") e/ou a dirección a que se ten que respostar ("Return-Path:", "Reply-To:"). Esta é a solución máis sinxela e preferible
- **Reescribir o remitente do correo** empregando un esquema do tipo http://www.openspf.org/SRS