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 ***webmaster 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.

  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.

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

Non me chega un correo adxunto

Debido á proliferación de correos adxuntos cifrados con contrasinal que conteñen virus e de arquivos executables con virus nos últimos meses de 2020 e inicios de 2021 foi necesario, no filtro antispam que emprega a Universidade de Vigo, filtrar estes adxuntos, nestes casos o remitente recibe unha mensaxe cun enlace á política de adxuntos permitidos no filtro antispam: http://www.rediris.es/lavadora/pol/

En xeral é preferible que empreguen, para enviar arquivos deste tipo, servizos específicos para compartir arquivos: DPV ou OneDrive.

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

Non recibo mensaxes con documentos adxuntos

Por motivos de seguridade o filtro antispam elimina algúns tipos de arquivo potencialmente perigosos das mensaxes recibidas

Estes arquivos pódense enviar ou recibir mediante outros mecanismos:

- DPV
- Filesender

Os tipos de arquivo filtrado son:

- Arquivos Visual Basic (executable/vba)
- Imaxes ISO (application/x-iso9660-image)
- Executables Windows (application/x-ms-dos-executable)
- Comprimidos Windows Media (image/x-wmz)

E extensións de moitos arquivos executables de uso común (pódense enviar comprimidos ou dende as ferramentas DPV ou Filesender:

.ade , *.adp ,.apk, **.appx, *.appxbundle , *.bat, *.cab, *.chm, *.cmd, *.com, *.com1, *.cpl, *.dll, *.dmg,**.exe, **.hta, *.inf, *.ins,**.iso, **.isp,**.jar , **.java,**.js,**.jse,**.lib, **.lnk, *.mde, *.msc, *.msi ,**.msix, **.msixbundle, *.msp, *.mst, *.nsh, *.ocx, *.pif, *.ps1, *.reg, *.scr, *.sct, *.sh, *.shb, *.sys, *.themepack,**.thmx, **.vb ,**.vbe,**.vbs ,**.vxd , **.wmz, *.ws,**.wsc,**.wsf,**.wsh, *.xpi

Os correos que envío son marcados como SPAM

Pode haber moitas razóns para que o filtro antispam detecte os seus correos como SPAM, entre elas

1. **Enviar correos dende servizos externos á UVIGO** (proveedores de recursos externos, Gmail, Otlook.com), empregando un remitente nas cabeceras (From:) dos dominios de uvigo (@uvigo.es, @uvigo.gal, ...).
   No apartado anterior recóllese a política de envío SPF da Universidade de Vigo.
2. **Enviar correos con enlaces de seguimento de correo** (mailtracker)
   Algúns servizos externos (mailtrack.io, p.ex.) permiten, engadindo un enlace no pe dos correos, detectar se o correo foi lido polo usuario (se o seu cliente de correo abre automáticamente os enlaces). Este tipo de servizos, a maiores de moi invasivos, envían datos de uso do correo electrónico dun usuario sen consentemento de este a provedores externos, polo que se recomenda encarecidamente non empregalos.
3. **Enviar correos adxuntos executables ou documentos de Word con macros**
   En xeral, se ten que enviar un arquivo executable por algún motivo, é preferible que empregue un servizo de disco compartido (https://dpv.uvigo.es, https://filesender.uvigo.es, OneDrive, ...)
4. **Enviar correos con enlaces a páxinas con incidentes recientes de seguridad**
   É moi habitual que estas páxinas sexan detectadas durante un tempo como posibles atacantes, polo que se a súa páxina web (p.ex. usuario.webs.uvigo.es) tivo un incidente de seguridad reciente, pode ser preciso durante un tempo non incluir o enlace á mesma no pe dos correos. De persistir a situación uns días despois de solventado o incidente poderían poñerse en contacto con nós para que solicitemos a reitrada da web dos listados de sitios perniciosos.

Non recibo correos e teño o correo redirixido a un provedor externo

Esta é unha situación que se da ás veces con usuarios que teñen contas no dominio @uvigo.es (@uvigo.gal), redirixidas a provedores externos (gmail, hotmail, ...).

Non sendo en ningún caso esta unha configuración recomendada, de facer isto é recomendable que opten por descargar estes correos no provedor con IMAP ou POP3, en lugar de reenviar os correos. Casi todos os provedores grandes dan esta opción.

Os reenvíos de correos poden causar moitos problemas:

- Rexeitamento de correos
  Os remitentes declaran moitas veces políticas (SPF, DMARC), indicando os remitentes autorizados para o correo, que serán polo xeral os servidores de correo ou aplicacións do remitente, en caso de reenviarse os correos estes proveñen da rede da Universidade de Vigo, provocando un rexeitamento da mensaxe.
- Reenvío de SPAM
  O SPAM non descartado reenviarase ó provedor, que detectará un incidente de envío de SPAM dende os servidores da Universidade de Vigo, dando como lugar a
  - Bloqueo dos envíos de correo dende a universidade para todos os usuarios.
  - Retardo dos envíos de correo dende a universidade para todos os usuarios.
  - Rexeitamento de correos reenviados na propia Universidade (dado que para evitar os dous casos anteriores nesta situación endurécense moito as regras de filtrado antispam).

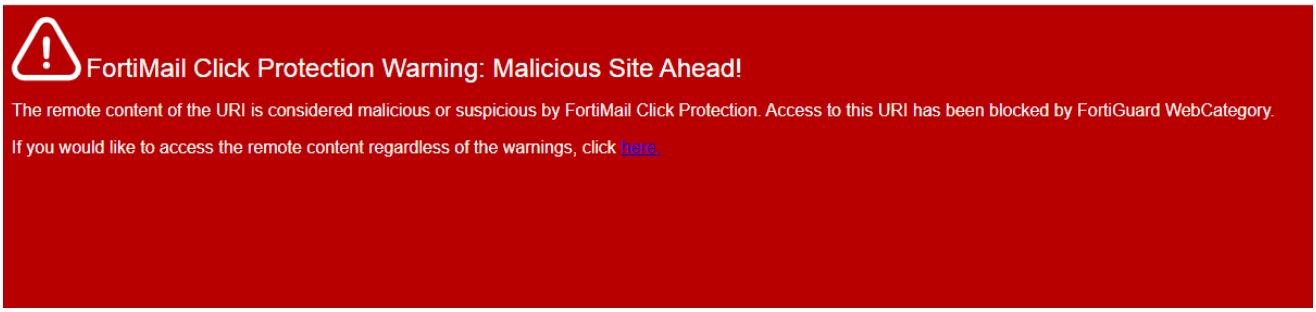
Recibo avisos indicando "Sender Rate Exceeded"

No correo de usuarios e co único fin de limitar os envíos de SPAM e phishing empregando contas de usuarios usurpadas por remitentes de spam, establécense uns controis de fluxo, limitando o número de destinatarios e correos por hora para cada usuario.

Cando este límite se excede estes correos *retárdanse* , e o remitente recibe estas mensaxes (de postmaster@puc.rediris.es) indicando *Sender Rate Exceeded* como título da mensaxe e indicando no corpo cando se entregarán as mensaxes. As mensaxes non se rexeitan nin descartan, só se retarda á súa entrega, co fin de evitar incidentes e bloqueos por parte dos destinatarios (algo moi común con servizos de provedores como Microsoft).

Recibo correos con enlaces a protection.puc.rediris.es

O filtrado antispam empregado pola Universidade de Vigo (Lavadora de Rediris) substitúe en correos cunha moi alta probabilidade de ser un phishing algúns enlaces a sitios que detecta como atacantes o posibles sitios de phishing e os substitúe por un enlace a protection.puc.rediris.es, nesa páxina poden acceder, se o desexan, o sitio orixinal, aínda que se recomenda encarecidamente que non o fagan, dado que na inmensa maioría dos casos trátase de intentos reais de estafa ou infección dos equipos dos destinatarios das mensaxes.
O sitio ó que se redirixe ó usuario ten un aspecto deste tipo



Recibo correos rexeitados coa mensaxe "550 maximum allowed line length is..."

Isto pode ocurrir, con algúns destinatarios, se o número de direccións de correo ás que se envía unha mensaxe é moi grande, compre, en xeral que non se fagan envíos e reenvíos de mensaxes a moitas direccións simultáneamente. Se precisan facer envíos regulares de avisos a grupos grandes de alumnos as listas de correo (https://listas.uvigo.es) poden ser unha mellor opción.

As mensaxes nestes casos poden vir rexeitadas cun texto do tipo

> The following address(es) have yet to be delivered:
> ....@uvigo.es: SMTP error from remote mail server after end of data: host smtp.uvigo.es [193.146.32.85]: 550 maximum allowed line length is 998 octets, got 1003