Recomendaciones básicas contra el SPAM

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-cv

CSIRT-cv es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, englobado dentro del III Programa de Servicios de Telecomunicaciones Avanzados Corporativos y de Comunicación con los Ciudadanos incluido en el Plan Estratégico Valenciano de Telecomunicaciones Avanzadas (PEVTA) del programa Avantic, como una apuesta de la **Generalitat de la Comunitat Valenciana** por la seguridad en la red.

Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico.

Datos de contacto

CSIRT-cv Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
Generalitat de la Comunitat Valenciana,
C/Cardenal Benlloch, 69 Entlo
46021 Valencia, España

Teléfono: +34-96-398-5300
Telefax: +34-96-196-1781
Email: csirtcv@gva.es
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

CSIRT-cv, dispone de un **catálogo de servicios**[1] donde se recogen las funciones y prestaciones que ofrece a todo su ámbito de actuación, diferenciado por colectivos. Estos recursos son gratuitos y se ampliarán gradualmente. Con ellos, **CSIRT-cv** espera contribuir de manera eficaz al correcto funcionamiento de las administraciones, PYMES y de sus servicios a favor de los ciudadanos.

Se sigue el patrón clásico de los Equipos de Respuesta a Incidentes y unifica los servicios en tres grandes grupos en función del momento y la forma en la que actúa ante un incidente.

CSIRT-cv dentro de su catálogo de servicios ofrece ciertos servicios de valor añadido que aumentan los servicios ya existentes y son independientes de la gestión de incidentes. Con éstos, brinda su experiencia para ayudar a mejorar la seguridad general de la organización identificando riesgos, amenazas y debilidades del sistema. Estos servicios contribuyen indirectamente a reducir la cantidad de incidentes.

Algunos de estos servicios de valor añadido son los servicios de **Formación y Concienciación** y como parte de los mismos **CSIRT-cv** decidió elaborar este documento para aconsejar de manera básica cómo protegernos ante el spam[2].

[1] http://www.csirtcv.gva.es/es/paginas/servicios-csirt-cv.html
[2] http://es.wikipedia.org/wiki/Spam

¿Podemos defendernos frente ataques SPAM?

Se llama spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (en algunos casos de manera masiva) que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

La recepción de SPAM, o correo basura, se ha convertido en uno de los principales problemas de la comunicación por correo electrónico. Estamos tan acostumbrados a recibir diariamente correos publicitarios (no solicitados) con múltiples promesas, que ya no luchamos contra ellos.

¿Realmente podemos protegernos del SPAM?

Hay una serie de **recomendaciones** que, si bien no son la panacea, sí pueden ayudarnos a mitigar el riesgo de sufrir ataques antispam:

· Ser muy **cuidadosos** con las webs a las que facilitamos nuestra dirección de correo. Podemos revisar las políticas de seguridad para comprobar la seguridad del sitio web y garantizar que no se comparta el e-mail.

· No colgar nuestra dirección de correo electrónico en sitios donde pueda ser visible **públicamente**, como foros, blogs o páginas de sociales. Si es imprescindible que el e-mail sea visible en una web determinada, podemos escribirlo de manera que no pueda ser detectado por programitas de reconocimiento automático. Por ejemplo, colocando caracteres entre medias como espacios en blanco. Por ejemplo: “ana @ hotmail.com”.

· Utilizar **diferentes cuentas** de correo electrónico dependiendo de la finalidad. Así, podemos emplear direcciones diferentes para el trabajo, contactar con amigos o participar en foros abiertos en la web. Se recomienda el uso de cuentas genéricas para aquellas operaciones en internet que entrañen mayor riesgo.

· Al reenviar e-mails recibidos a una lista de contactos, debemos los e-mails anteriores para que no sean visibles por futuros receptores y detener su circulación por internet.

· No participar en cadenas de e-mails divertidos, que también pueden considerarse un tipo de SPAM puesto que implican una gran pérdida de tiempo.

· Asegurarse de que nuestro proveedor de Internet cuente con protección contra spam, virus y spyware porque los mensajes de spam suelen están ligados a virus.

· Crear una dirección de correo electrónico única con letras y números. Muchos spammers utilizan aplicaciones para enviar correos electrónicos a distintas combinaciones de nombres a numerosos IPS.

· Activar un filtro de correo electrónico. La mayoría de los clientes de correo electrónico (incluso los correos web) ofrecen posibilidades para filtrar o guardar en una carpeta, cualquier correo que venga de spammers o aquellos que tengan contenido dudoso en la línea de asunto o en el cuerpo del mensaje.

Si a pesar de las recomendaciones anteriores recibimos correo electrónico no deseado debemos seguir las **siguientes indicaciones:**

· No abrir mensajes los mensajes de spam. Con frecuencia los mensajes de spam incluyen software que permite al spammer determinar qué direcciones de correo electrónico han recibido y abierto el mensaje.

· No responder a los correos con direcciones desconocidas o sospechosas. La mejor solución es borrarlos, o dejar que el filtro anti-spam los ponga en cuarentena.

· No abrir ningún adjunto ni acceder a ningún vínculo (incluso en una dirección para
cancelar suscripción) que aparezca en un mensaje de spam. Podría infectar el equipo o el enlace puede ser utilizado por spammers para evaluar direcciones de e-mail válidas para envíos futuros de SPAM.

· No comprar nada que le ofrezcan en un correo sospechoso. Evitaremos sufrir un fraude y de paso, financiar a los spammers.

· No creer todo lo que se lee: Con los correos electrónicos reenviados que alertan de algún peligro o las habituales cadenas, los spammers recopilan cuentas de correo electrónico.

· Observar las direcciones de e-mail de las que reciba spam o el contenido del mensaje para activar filtros que bloqueen correo futuro con las mismas características.

· Si utilizamos una página web como base para los servicios de correo electrónico, informar a su proveedor. Esto ayudará a seleccionar de forma precisa cuáles de los mensajes son spam y tal vez pueda bloquear la dirección de correo spam.

· Quéjarse al ISP del remitente. La mayoría de los ISP tienen normas contra el uso del
sistema para enviar SPAMS a los otros y pueden cerrar la cuenta del spammer.

· Instalar un programa anti-spam, ya que bloquea del 97-99% del correo no deseado.

Así se reducirá en gran medida la cantidad de spam recibido. Una vez somos objeto de ataques spam, la única protección posible pasa por utilizar **aplicaciones antispam** que pueden ayudarnos a evitar las molestias del correo no deseado.

Entre otras posibilidades, los programas antispam: cuentan con filtrado por listas de spammers, verifican de la política del remitente (SPF), identifican URLs spam en el contenido del mensaje, tienen bases de datos heurísticas de contenidos spam y de firmas léxicas, bloquean el spam gráfico y se mantienen actualizados de manera dinámica.

Ejemplos de antispam gratuitos:

- Spamihilator http://www.spamihilator.com/
- Crm114 http://crm114.sourceforge.net/
- Dspam http://dspam.nuclearelephant.com/
- Bogofilter http://bogofilter.sourceforge.net/
- SpamAssassin http://spamassassin.apache.org/