

Implicancias del spam



r e d c i e n t í f i c a p e r u a n a

Jack Daniel Cáceres Meza

jcaceres@rcp.net.pe



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



INTRODUCCIÓN

Orígenes de la palabra

- En 1937 aparece una carne en lata originalmente llamada Hormel's Spiced Ham
- Comicidad a costa de la palabra, repetida y sin sentido



INTRODUCCIÓN

- Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico
- Otras tecnologías de internet que han sido objeto de spam incluyen grupos de noticias usenet, motores de búsqueda (spamdexing, para crear la ilusión de popularidad en ciertas páginas Web), wikis y blogs (blog falso)
- El spam también puede tener como objetivo los juegos en línea, teléfonos móviles a través de mensajes de texto (spam sms), los sistemas de mensajería instantánea (spim) y ahora la telefonía IP (spit)

<http://es.wikipedia.org/wiki/Spam>



INTRODUCCIÓN

Un mensaje electrónico es “spam” si:

- La identidad personal del destinatario y el contexto son irrelevantes por que el mensaje es aplicable por igual a muchos otros destinatarios; y
- El destinatario no ha dado permiso de forma demostrable, deliberada, explícita y sin revocatoria para que se le envíe -el mensaje; y
- La transmisión y recepción del mensaje aparenta para el destinatario que provee un beneficio desproporcionado para el remitente.

MAPS website <http://www.mail-abuse.com/>



INTRODUCCIÓN

- El spam por medio del fax (spam-fax), es otra de las categorías de esta técnica de 'marketing directo', y consiste en enviar faxes masivos y no solicitados a través de sistemas electrónicos automatizados hacia miles de personas o empresas cuya información ha sido cargada en bases de datos segmentadas según diferentes variables

<http://es.wikipedia.org/wiki/Spam>



- Introducción
- **Apreciaciones**
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



APRECIACIONES

“El spam, correo basura, correo no solicitado o no autorizado, o como quiera llamársele, constituye, hoy en día, una de las prácticas comerciales más rechazadas por la ciudadanía y la sociedad en general, basta mencionar los elevados costos que se generan para el que recibe el correo -tiempo en eliminar los correos, espacio en servidor, etc.- los que constituyen una verdadera externalidad negativa, para entender este rechazo.”

Alberto Cerda Silva. Coordinador Académico. Centro de Estudios en Derecho Informático de la Universidad de Chile. Julio de 2004

**Productividad del usuario
... o pérdida de productividad**



APRECIACIONES

“Cuando hablamos de Spam nos referimos a correos electrónicos de carácter comercial no solicitados. Se considera que los correos tienen la calidad de no solicitados “si no existe relación previa entre las partes y el receptor no ha consentido explícitamente en recibir la comunicación. El problema principal con el Spam recae en el volumen de los mensajes de correo y no en su contenido”. Así, la recepción de correos no deseados de forma masiva y permanente, afectaría diversos derechos constitucionalmente previstos como por ejemplo, el derecho a la intimidad y a la tranquilidad individual.”

Gustavo Rodriguez Garcia (Pontificia Universidad Católica del Perú), Alfa-Redi: Revista de Derecho Informático, Edición 092 – Marzo 2006

Marco legal
¿quién realmente envía?



APRECIACIONES

“El correo basura es el azote del correo electrónico y los grupos de noticias en la Internet. Puede interferir seriamente con la operación de servicios públicos, por no mencionar el efecto que puede tener en los sistemas de correo electrónico de cualquier individuo... Los spammers están, de forma efectiva, sustrayendo recursos de los usuarios y proveedores de servicio sin compensación y sin autorización.”

Vint Cerf, Senior Vice President, MCI

Servicios – Distribución
¿quién paga por la tecnología?

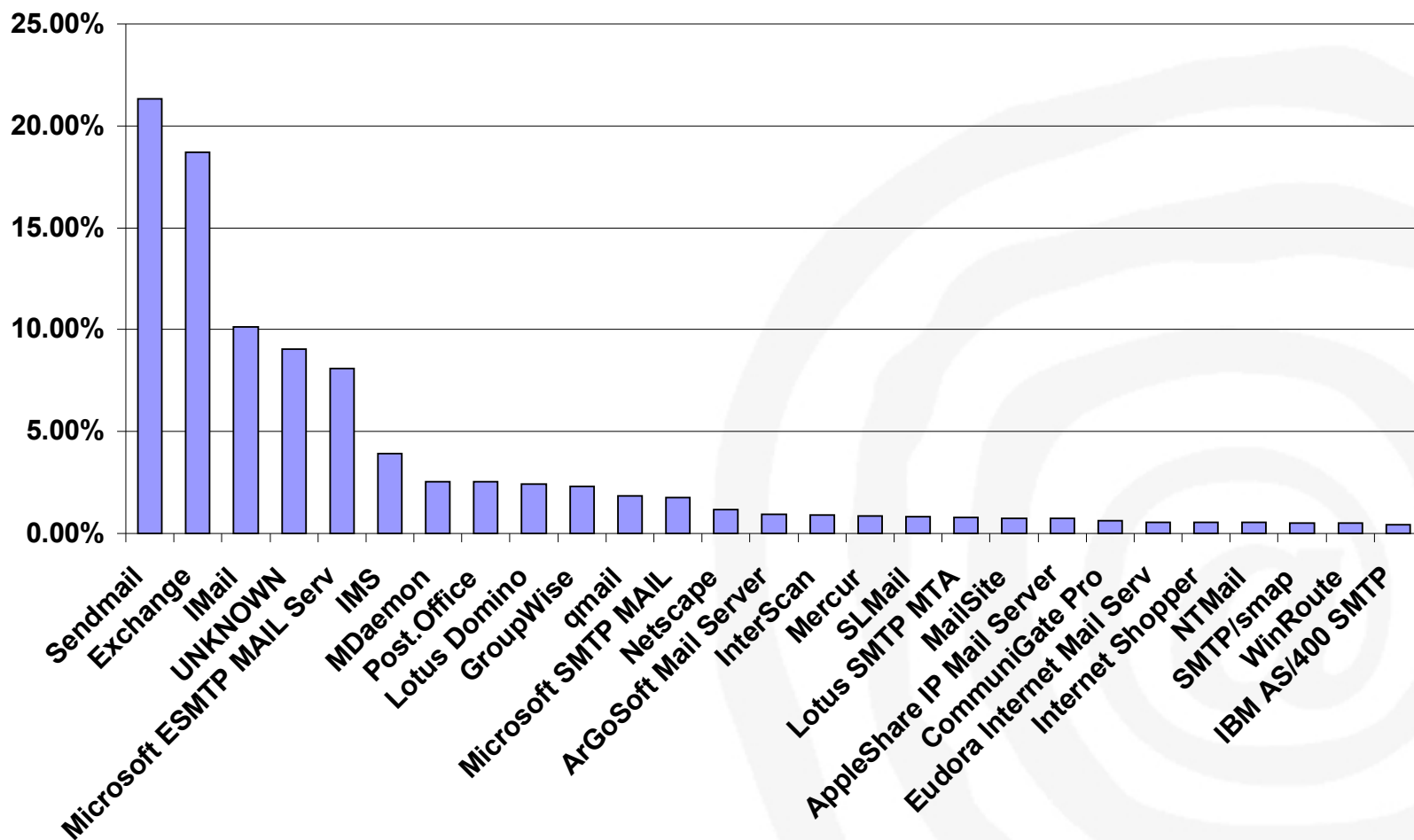


- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



ESTADÍSTICAS DEL PROBLEMA

Distribución de servidores por MTA

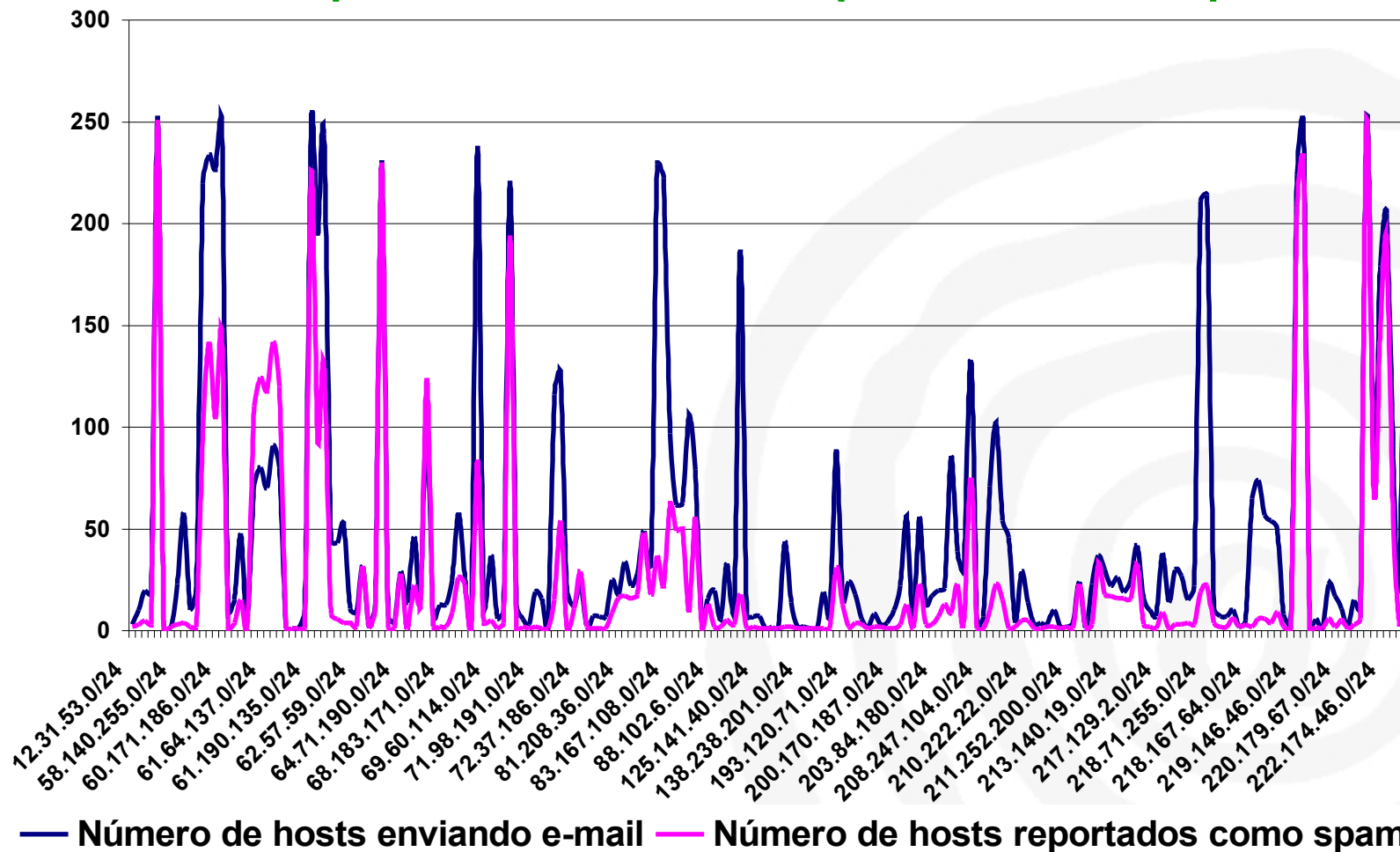


Open Relay Database: ORDB.org



ESTADÍSTICAS DEL PROBLEMA

Hosts que envían Vs. Hosts reportados como spam

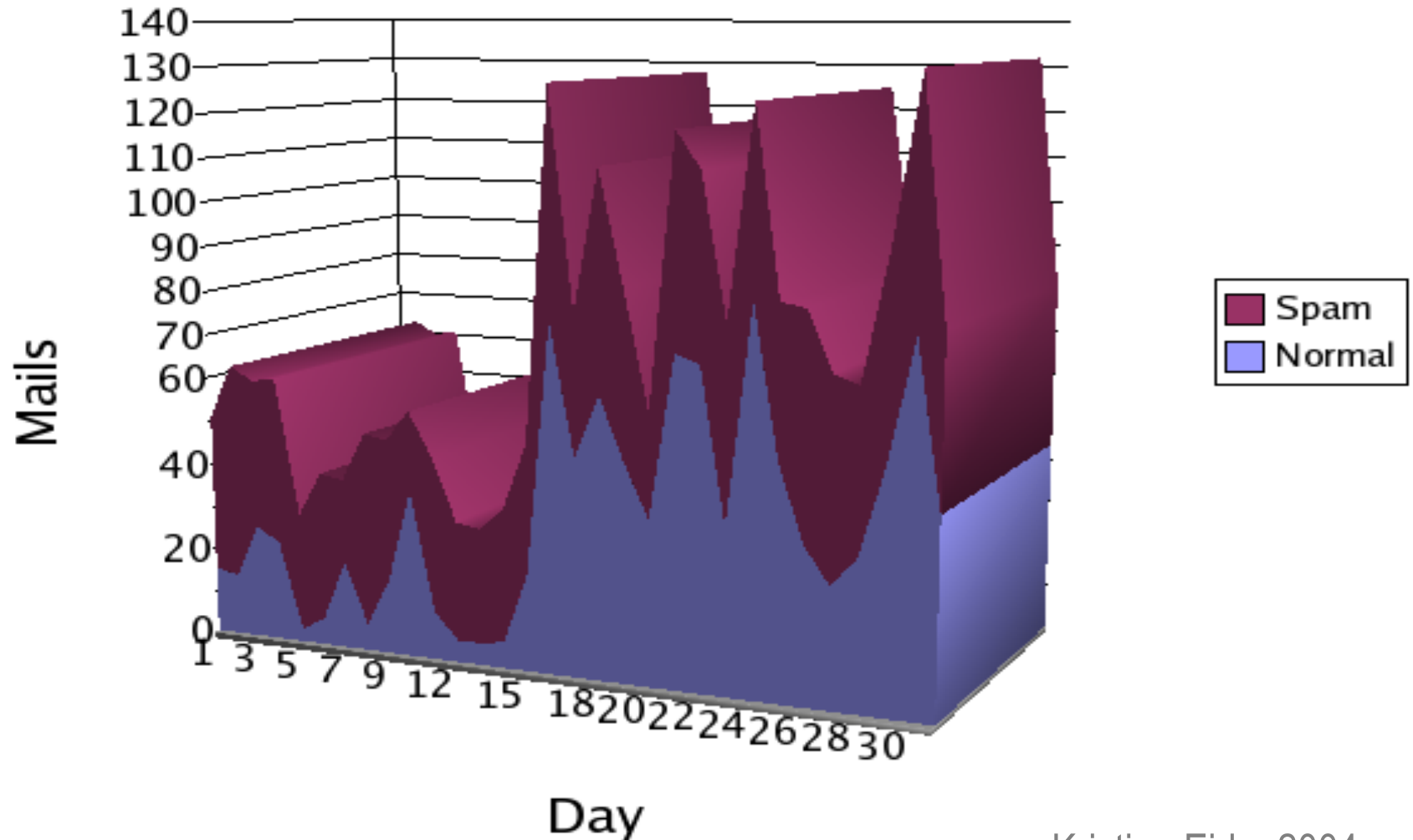


IronPort Systems, owner of SpamCop, Copyright (C) 1998-2006



ESTADÍSTICAS DEL PROBLEMA

E-Mail enviado Vs. E-Mail reportado como spam



Kristian Eide, 2004



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano: **Ley N° 28493**
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



MARCO LEGAL PERUANO

- **ART. 5°.-** Correo electrónico comercial no solicitado. Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:
 - a) La palabra "publicidad", en el campo del "asunto" (o subject) del mensaje.
 - b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
 - c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.



MARCO LEGAL PERUANO

- **ART. 8°.-** Derecho a compensación pecuniaria. El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente ley, con un máximo de dos (2) Unidades Impositivas Tributarias.

Ley N° 28493
Diario Oficial El Peruano el 12 de abril del 2005



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



IMPACTO SOBRE LA PRODUCTIVIDAD

- El spam nuestro de cada día ...
- Pérdida de productividad





IMPACTO SOBRE LA PRODUCTIVIDAD

- Usuario final (el que finalmente paga por el mensaje spam)
 - Tiempo
 - ¿Posible ofensa, posible utilidad?
 - Filtrado (sirve, no sirve)
 - Distracción (... mira qué bonito auto, ¿habrán más? ...)
 - Espacio (¡técnico, más disco!)
 - Costo (¡se me acabó el tiempo en la cabina!)
 - Malestar -> queja -> ira -> aceptación y filtrar
 - Borrar mensajes por error (... lo siento jefe ...)



IMPACTO SOBRE LA PRODUCTIVIDAD

- Administrador de la red (el que finalmente paga por el tráfico spam)
 - Análisis y actualización continuos
 - Identificación de nuevos patrones
 - Listas negras y listas blancas
 - Falsos positivos y falsos negativos
 - Re-dimensionar
 - Capacidad de los servidores
 - Capacidad del ancho de banda de Internet
 - Re-diseñar
 - Distribución y configuración de servicios y servidores
 - Alternativas de solución
 - Alternativas para manejar a los usuarios



IMPACTO SOBRE LA PRODUCTIVIDAD

- Pérdida de ingresos económicos
 - Empresa (la que finalmente paga la cuenta)
 - Provisión de protección
 - Provisión de mayor ancho de banda (¿mayor ancho de banda => mayor ventaja para spammers?)
 - Provisión de recursos internos, políticas y procedimientos
 - Proveedor del servicio de correo o del servicio Internet (ISP)
 - Provisión de protección (al que se responsabiliza de todo)
 - ¿Elección / depuración de clientes?



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



ASPECTOS LEGALES

- ¿Quién envía el mensaje realmente?
 - ¿El usuario o el ISP?
 - Recibo algo falso pero de un remitente verdadero
 - Si fraguaron el mensaje, ¿de quién me quejo?
- ¿Porqué soy sujeto de envío?
 - Recibo algo verdadero de un remitente verdadero pero no autorizado
 - ¿Quién vendió mi cuenta?



ASPECTOS LEGALES

- **Ética** del proveedor del servicio de correo o del servicio Internet (ISP)
 - ¿Es culpable?
 - ¿Porqué no filtra?
 - ¿Porqué acepta spammers como clientes?
- El spam, ¿es legal o ilegal?, ¿ofensivo o comercial?
 - Un mismo mensaje puede ser considerado como spam por un grupo de personas pero, a su vez, ser considerado como válido por otro grupo
 - El único con capacidad para distinguir entre un spam o un mensaje legítimo es el usuario



ASPECTOS LEGALES

- **Daños indirectos** (yo no envié el mensaje, fue algún virus en mi computadora)
- El bloqueo por parte del proveedor (ISP), ¿implica una violación de la privacidad del usuario del servicio?
- El bloqueo / revisión por parte del proveedor (empresa), ¿implica una violación de la privacidad del usuario del servicio?
- Problemas para la empresa que se anuncia mediante este sistema de correos (¿imagen solamente?)



ASPECTOS LEGALES

- Las opciones 'opt-in', ¿son aceptadas legalmente?
- Modificación del marco legal para incluir otros ámbitos de comunicaciones
- ' ... La comunicación debe ser vista como un derecho humano y los derechos de propiedad pueden y deben limitarse dónde, cómo y cuando sea necesario para asegurar esos derechos humanos ... '



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



ALGUNAS TÉCNICAS DE SPAM

- Envío de correo - verificación de la recepción
- Open relay, open proxies
- Troyanos y computadoras zombis
- Suplantación (spoofing), camuflaje (munging)
- Ataques del tipo DDoS (distributed denial-of-service) contra servicios DNSBL y otras fuentes anti-spam
- Emplear configuraciones deficientes de servicios DNS
- Emplear dominios caducados
- NDR falso (notificación de entrega fallida -Non-Delivery Report)
- Mensajes con sólo un archivo con extensión '.jpg' o '.gif'



ALGUNAS TÉCNICAS DE SPAM

- Envío alfabético (mensajes enviados a grupos en orden alfabético)
- Envío horizontal (muchos mensajes enviados a muchos grupos)
- Envío vertical (muchos mensajes enviados a un grupo)
- Crosspost (un mismo mensaje se envía una vez a varios grupos)
- Multi-Post (un mismo mensaje se envía varias veces a varios grupos)
- Hash Buster (contenido válido mezclado con contenido errático)
- Payload (la parte del spam que realmente se difunde)
- Enviar mensajes y cerrar cuentas



ALGUNAS TÉCNICAS DE SPAM

- División de la línea de Asunto del mensaje mediante falsos saltos de línea

```
Subject: =?utf-8?q?Drogas Idénti –cas con p?=  
=?utf-8?q?equeño valor monetar?=  
=?utf-8?q?io!?=
```

- Uso de caracteres nulos (codificación de tipo Quoted-Printable)

```
<=00H=00T=00M=00L=00>=00<=00H=00E=00A=00D=00>=00=  
0D=00=0A=00<=00M=00E=00=
```



ALGUNAS TÉCNICAS DE SPAM

- Permutar letras en las palabras usadas. El mensaje sigue siendo legible para el receptor, pero los filtros no reconocen las palabras usadas

Fnilament lorgé predre peso y me aelgro basatnte

- Invertir el texto, utilizando la anulación derecha-a-izquierda (*right-to-left override*) de Unicode, expresada como entidades HTML (‮ y ‬)

Your B‮na‬k C‮dra‬
Link‮ni‬g



ALGUNAS TÉCNICAS DE SPAM

- Encapsular una etiqueta <map> con una de tipo HREF, de tal forma que en lugar de una URL maliciosa aparezca otra legítima:

```
<A HREF="<URL_LEGÍTIMA>">
```

- Uso de caracteres ASCII para “dibujar” el contenido del mensaje

```
U   U SSSS
U   U S
U   U SSSS
U   U   S
UUUU SSSS
```

- Uso de etiquetas HTML incorrectas
- Codificación de URLs
- Empleo de entidades HTML para ocultar determinadas letras



ALGUNAS TÉCNICAS DE SPAM

- Uso de tinta invisibles
- Incluir el mensaje de spam como archivo adjunto en otro mensaje válido
- Uso de CSS (Cascading Style Sheets) en los mensajes de spam para ocultar determinadas palabras o partes del mensaje
- Otros



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



ALGUNAS FORMAS DE OBTENER DIRECCIONES DE CORREO

- Empleo de robots
- Trampa de spam (opción preseleccionada por defecto en un formulario online)
- Sitios web que solicitan información para brindar un determinado servicio
- Hacer clic en 'Aceptar' sin leer la letra pequeña y sin desmarcar lo no deseado
- Servicios gratuitos de descarga (warez)
- Suscripciones por Internet (opt-in)
- Grupos de noticias, foros de discusión, listas de correo



ALGUNAS FORMAS DE OBTENER DIRECCIONES DE CORREO

- Encuestadoras (de opinión)
- Chat, juegos en línea
- Cadenas y difusión de cadenas
- Bases de datos
- Entrada ilegal en servidores
- Por ensayo y error, ataque por diccionario
- Virus, spyware, cookies, phishing
- Otros



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



ALGUNAS RECOMENDACIONES

Para los usuarios

- Emplear firewall y mantener actualizados el anti-virus y el anti-spyware
- No emplear la cuenta de correo del trabajo en el Web-eo
- No difundir o publicar nuestra cuenta de correo -indiscriminadamente
- Eliminar los mensajes de remitentes desconocidos sin leer -abrir
- No responder a un mensaje spam
- No desuscribirse -a menos que intente una acción legal posterior
- No enviar mensajes a varios destinatarios con CC -emplear CCO
- Emplear filtros en los clientes de correo y mantenerlos actualizados



ALGUNAS RECOMENDACIONES

Para los usuarios

- Evitar el proceso innecesario de los mensajes (plug-in, html, fondos, colores, otros)
- Configurar el cliente de correo para enviar y recibir sólo texto
- Emplear redirecciones o cuentas de correo temporales
- No utilizar 'Vista Previa' en el cliente de correo
- Verificar que nuestra cuenta de correo no esté visible en Internet
- Emplear clientes de correo que incorporen soluciones anti-spam o que al menos permitan configurar filtros
- No abrir documentos adjuntos con extensión desconocida
- No hacer clic en las direcciones adjuntas



ALGUNAS RECOMENDACIONES

Para los administradores de la red

- Mantener actualizados el firewall, sistema operativo, anti-virus y anti-spyware de computadoras y servidores y el servicio de correo
- Proteger las direcciones de correo en páginas Web
- Emplear DNS-based Blackhole List (DNSBL), o Real-time Blackhole List (RBL)
- Emplear herramientas que cuenten con mecanismos basados en el análisis del contenido de los mensajes, como análisis sintáctico, cálculo de probabilidades, filtros bayesianos o heurístico, otros
- Emplear herramientas que permitan la modificación manual de listas blancas, negras y grises (para autenticación de remitentes)
- Automatizar la actualización de las herramientas empleadas
- Actualización continua de las herramientas empleadas



ALGUNAS RECOMENDACIONES

Para los administradores de la red

- Investigar casos en Mail Abuse Prevention System (MAPS) y otros RBL, DNSReport
- Emplear firmas digitales
- Emplear registros SPF (Sender Policy Framework) en los servicios DNS para evitar Sender Address Forgery

```
example.net.   TXT    "v=spf1   mx   a:pluto.example.net  
              include:gmail.com -all"
```

- Bloquear por 'character-set', por ejemplo:
'euc-kr' , 'ks_c_5601' , 'GB2312'
- IETF RFC 2505: Anti-Spam Recommendations for SMTP MTAs
- IETF RFC 2821: Simple Mail Transfer Protocol
- IETF RFC 4408: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail



ALGUNAS RECOMENDACIONES

Para todos

- Cuantificar apropiadamente el impacto de los mensajes considerados como spam
- Particularizar cada caso evitando las generalidades
- Ajustar tiempos de ocurrencia y evitar el siempre (falla) o el nunca (funciona)
- Existen diferentes formas de bloquear un spam y esas diferentes formas se aplican en situaciones particulares las cuales pueden llevar a confusión, o falsas expectativas
- En ningún caso una solución anti-spam resolverá al 100% el problema
 - **El único con capacidad para distinguir entre un spam o un mensaje legítimo es el usuario**



- Introducción
- Apreciaciones
- Estadísticas del problema
- Marco legal peruano
- Impacto sobre la productividad
- Aspectos legales
- Algunas técnicas de spam
- Algunas formas de obtener direcciones de correo
- Algunas recomendaciones
- Bibliografía



BIBLIOGRAFÍA

- Regula el uso del spam (Diario Oficial El Peruano el 12 de abril del 2005)

www.congreso.gob.pe/ntley/Imagenes/Leyes/28493.pdf

- Regulan las centrales privadas de información de riesgos y de protección al titular de la información

www.congreso.gob.pe/ntley/Imagenes/Leyes/27489.pdf

www.congreso.gob.pe/ntley/Imagenes/Leyes/27863.pdf
(modificatoria)



BIBLIOGRAFÍA

- <http://www.antispam.org.pe/>
- <http://www.alfa-redi.org/rdi-articulo.shtml?x=5500>
- <http://www.cpsr-peru.org/bdatos/decisiones/europa/directiva>
- <http://www.ironport.com/company/>
- http://www.mail-abuse.com/an_listmgntgdlines.html
- <http://www.spamcop.net/>
- <http://www.ordb.org/>
- <http://www.spamhaus.org/>
- <http://www.robtex.com/rbls.html>
- <http://www.rahul.net/falk/glossary.html#spam>
- <http://www.ietf.org/rfc/rfc2505.txt>
- <http://esp.sophos.com/security/spam-glossary.html>
- http://www.pandasoftware.es/virus_info/spam/
- <http://www.openspf.org/>

- Crear una cultura de uso adecuado de los medios electrónicos y ciberseguridad, para todos
- Paciencia para los que reciben
- Cuidado –y misericordia- para los que envían
- Actualización y previsión constante
- ‘ ... La comunicación debe ser vista como un derecho humano y los derechos de propiedad pueden y deben limitarse dónde, cómo y cuando sea necesario para asegurar esos derechos humanos ... ’



PREGUNTAS

¿ ... ?