

### Antecedentes

La Internet y la información a la que conecta es un recurso del que muchos dependen hoy en día. Datos que en el pasado demoraban varios días en ser localizados en una biblioteca de investigación, ahora se pueden obtener instantáneamente, usando su computador personal o incluso un aparato móvil portátil. Las personas pueden publicar para una audiencia a nivel mundial, combinar contenido existente previamente para generar nuevas creaciones o actuar como tutores, compartiendo con sus amistades el mejor material de última hora que aparece en la Internet. Sin embargo, debido a que casi todos quienes poseen un computador o un aparato inalámbrico pueden conectarse a la Internet, algunas personas malintencionadas han encontrado formas de usarla para causar daño. Numerosas agencias del gobierno de Estados Unidos, incluyendo la FCC y organizaciones sin fines de lucro, se han unido en un esfuerzo por proveer a los consumidores con información útil, fácil de comprender, relativa a la seguridad en Internet, la que puede encontrar en [www.alertaenlinea.gov/default.aspx](http://www.alertaenlinea.gov/default.aspx). Esta hoja informativa resume parte de esa valiosa información.

### El correo indeseado (y sus peligros)

El correo electrónico no deseado es como el correo no deseado que recibe en su casa, es inconveniente y hace perder tiempo. El correo electrónico no deseado puede pasar de ser molesto a malicioso, si los mensajes o lo que adjuntan se apoderan de su información personal ("spyware" en inglés) o actúan causando problemas en su computador personal o en su aparato inalámbrico, implantándoles virus o "gusanos." Algunos programas computacionales pueden integrar su computador a una red para distribuir correo no deseado, convirtiéndolo en un "zombie" que pasa a formar parte de una "botnet" o red robot. Formas en que usted puede reducir el correo electrónico indeseado:

- Busque un proveedor de correo electrónico que posea una alta capacidad para filtrar mensajes indeseados. Usted no necesita usar el correo electrónico de su Proveedor de Servicio de Internet (ISP, por sus siglas en inglés), puede elegir un servicio de correo electrónico independiente. Una forma en que los servicios de correo electrónico compiten es ofreciendo mejores servicios de filtrado de mensajes. Hable con su proveedor, si usted piensa que se puede mejorar el filtro.

### El correo indeseado (y sus peligros) (Cont.)

- Algunos filtros de correo indeseado poseen niveles que pueden alterarse para otorgar más protección. Revise su filtro para asegurarse de que está en el nivel que usted desea. Si tiene dudas sobre cómo cambiar niveles de filtro, contacte a su proveedor de correo electrónico.
- Identifique el correo indeseado con el botón para "spam." Muchos servicios de correo electrónico le permiten seleccionar el correo indeseado y luego presionar el botón de "spam" para identificarlo como correo indeseado. Use ese botón si lo tiene, porque le informa a su proveedor de Internet que correos electrónicos usted no desea recibir.
- Los niveles de filtro para mensajes también le permiten evitar la exhibición automática de logos o imágenes cuando abre un mensaje electrónico. Las imágenes pueden contener programas nocivos o espías e informar a los generadores de correos no deseados que sus mensajes fueron abiertos y que han sido enviados a una dirección electrónica válida.

(Sigue)



## El correo indeseado (y sus peligros) (Cont.)

- Programe su correo electrónico de tal manera que no acepte automáticamente lo que ingresa ni baje automáticamente documentos adjuntos.
- Trate de limitar el envío o exhibición de su dirección de correo electrónico a personas o grupos que usted conoce. Revise la política de privacidad de un sitio o directorio electrónico, antes de enviar su dirección electrónica y si puede, elija la opción "opt out" cuando le pidan autorización para compartir su dirección de correo electrónico con terceros.
- Proteja las direcciones electrónicas de sus amigos, poniéndolas en la línea "bcc" cuando envíe mensajes electrónicos a un grupo de personas que no se conocen entre sí.
- Considere el uso de dos direcciones de correo electrónico, una para mensajes personales y otra para su correspondencia con compañías o grupos con los que se comunica regularmente.
- Nunca responda a un correo electrónico indeseado.

El Decreto CAN-SPAM, una ley federal, exige a quienes envían correos electrónicos comerciales dar una dirección electrónica u otro método de respuesta vía Internet, para que el público pueda optar a no recibir nuevos correos electrónicos. Quienes envían los correos deben cumplir con su petición de no recibir nuevos correos, a más tardar en un plazo de diez días y no pueden vender o transferir la dirección de Internet incluida en su solicitud para no recibir correos, a menos que la transferencia tenga por fin permitir a otro emisor de correos dar cumplimiento al Decreto. Averigüe más sobre este Decreto en:

[www.ftc.gov/bcp/edu/microsites/spam/pespanol.htm](http://www.ftc.gov/bcp/edu/microsites/spam/pespanol.htm).

## El correo indeseado (y sus peligros) (Cont.)

Usted puede denunciar el correo no deseado que recibe en su computador ante la Comisión Federal de Comercio (FTC, por sus siglas en inglés) enviando una copia del mensaje a [spam@uce.gov](mailto:spam@uce.gov). El Decreto CAN-SPAM también prohíbe el envío de mensajes comerciales no deseados a aparatos inalámbricos usando una dirección de Internet sin autorización previa. Para más información sobre correo electrónico indeseado en aparatos inalámbricos y cómo presentar quejas ante la FCC sobre el tema, vea la hoja informativa para el consumidor en [www.fcc.gov/cgb/consumerfacts/spanish/canspam.html](http://www.fcc.gov/cgb/consumerfacts/spanish/canspam.html).

Formas en que usted puede restringir los programas espías y nocivos:

- Instalando un programa antivirus y anti espionaje que monitoree los correos y archivos que ingresan a su computador para detectar problemas y mantenerlo actualizado. Estos programas pueden venir ya instalados en su computador o aparato, pueden ser bajados de su ISP o de los sitios en Internet que diseñaron su programa computacional, o adquiridos en tiendas de venta al detalle. Debido a que algunas personas malintencionadas están continuamente creando nuevos virus y programas espías, su programa necesita ser actualizado regularmente. Algunos programas computacionales son actualizados de manera automática.
- Programe su sistema operativo (como Windows o un sistema operativo de computadoras Apple) para que baje e instale automáticamente nuevos dispositivos de seguridad.
- Tenga cuidado cuando abra documentos adjuntos o baje archivos, aunque crea que conoce a quien los envía. El mensaje electrónico de presentación debe mencionar el documento adjunto y describir lo que contiene.

(Sigue)



## El correo indeseado (y sus peligros) (Cont.)

- Baje programas gratuitos, incluyendo juegos y barras, solamente de sitios que conoce y en cuya autenticidad confía.
- Cuando se conecte a la Internet, use un programa de seguridad que bloquee todas las comunicaciones de fuentes no autorizadas.

Señales de que su computador podría estar infectado incluyen la aparición repetida de mensajes indicando un error, los que le restan rapidez; el aumento de avisos que aparecen automáticamente en su pantalla o “pop-ups” o el ingreso a sitios distintos a los que usted intenta visitar. Escanee su computador con regularidad y contacte a su proveedor de programas de seguridad o busque otro tipo de asistencia si encuentra problemas que usted no puede resolver. Usted también puede quejarse de un computador infectado ante la FTC en Internet, <https://www.ftccomplaintassistant.gov> (en inglés), llamando gratuitamente al 1-877-382-4357 (voz) o 1-866-653-4261 (TTY) o escribiendo a:

Federal Trade Commission  
CRC-240  
600 Pennsylvania Ave., NW,  
Washington, DC 20580.

## Estafas

Algunos de los correos electrónicos más peligrosos son los que simulan ser correos electrónicos legítimos, de empresas u organizaciones con las que usted hace negocios, como su banco, compañías de tarjetas de crédito, clubes a los que usted pertenece o incluso una agencia del gobierno. Los correos electrónicos piden que usted ponga al día o confirme su cuenta u otra información personal y proporcionan un enlace a un sitio de Internet que simula ser el sitio en Internet de la “organización” que lo está contactando. En una nueva variación, este tipo de estafas conocidas como “phishing scams” (pronunciado *fishin scams*) en busca de incautos se usa para obtener nombres y claves de ingreso a cuentas de correo electrónico, dando acceso a

## Estafas (Cont.)

los estafadores a toda la información personal contenida en sus propios correos electrónicos y en correos electrónicos que usted recibe de otras personas. Las “phishing scams” también pueden derivar en el robo de identidad. Aquí hay algunas formas de evitar ser víctima de estafadores:

- No proporcione información personal o financiera, nombre de usuario ni clave de ingreso en respuesta a un correo electrónico porque en general, las compañías legítimas no solicitan dicha información de esa manera.
- Si se pregunta si un correo electrónico realmente proviene de una empresa que conoce, contáctese con la firma usando un número telefónico o una dirección de Internet distinta a la que proporciona el correo electrónico y consulte a la empresa si realmente lo envió.
- Use los consejos de resguardo que se enumeran más arriba para evitar los correos electrónicos no deseados y los programas espías o maliciosos.
- Revise las cuentas bancarias y de tarjetas de crédito apenas las reciba, para monitorear si aparecen cobros no autorizados. Use el número o dirección de Internet que aparece en la cuenta para contactarse con la firma que la envió, si ve cobros como los mencionados.
- Reenvíe los correos electrónicos sospechosos de intentar una “phishing scam” a la organización que imitan y a la FTC a: [spam@uce.gov](mailto:spam@uce.gov). Si usted piensa que ha sido víctima de una “phishing scam” o de un intento de estafa de este tipo, infórmelo a la FTC usando la información de contacto proporcionada más arriba. Usted también puede visitar el sitio de la FTC en Internet para Robo de Identidad en

(Sigue)



## Estafas (Cont.)

[www.ftc.gov/bcp/edu/microsites/idtheft/n-espanol/index.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/n-espanol/index.html) para encontrar formas de evitar este problema adicional.

Además de cuidarse de los correos electrónicos intentando hacer “phishing scams”, tenga cuidado con los correos electrónicos que ofrecen ventas o promesas demasiado buenas para ser verdaderas. Antes de comprar o actuar en base a una oferta en Internet, espere a recibir respuesta a todas sus preguntas y lea la “letra chica.” Para obtener más información sobre estafas comunes en Internet, visite [www.ftc.gov/bcp/menus/consumer/tech/scams.shtm](http://www.ftc.gov/bcp/menus/consumer/tech/scams.shtm) (en inglés).

## ¿Tiene hijos?

Todo padre, madre o persona con menores a su cargo sabe que los niños pasan cada vez más tiempo frente al computador y cada vez comienzan desde más pequeños. Con los nuevos teléfonos inteligentes y cada vez más populares, el acceso a Internet es más fácil que nunca. Los niños pueden ser más vulnerables a las estafas y al sofisticado mercadeo en Internet y comparten cada vez más información personal en los sitios de redes sociales. El mejor consejo para los padres y personas a cargo de menores es hablar con los niños sobre la seguridad en Internet y mantenerse al tanto de lo que los niños hacen en la Internet. Para obtener más información sobre la seguridad de los niños en Internet visite [www.alertaenlinea.gov/topics/net-cetera.aspx](http://www.alertaenlinea.gov/topics/net-cetera.aspx).

## Para más información

Para obtener información sobre otros asuntos de telecomunicaciones, visite el sitio en Internet de la Oficina de Asuntos Gubernamentales y del Consumidor de la FCC, [www.fcc.gov/cgb/spanish/](http://www.fcc.gov/cgb/spanish/) o contáctese con el Centro del Consumidor de la FCC, llamando al 1-888-CALL-FCC (1-888-225-5322) de voz o al 1-888-TELL-FCC (1-888-835-5322) TTY; enviando un fax al 1-866-418-0232 o escribiendo a:

Federal Communications Commission  
Consumer & Governmental Affairs Bureau  
Consumer Inquiries and Complaints Division  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554.

*Para obtener ésta u otra publicación para el consumidor en formato accesible (texto electrónico ASCII, Braille, letra grande o audio) escríbanos o llame a la dirección o teléfono indicados abajo o envíe un correo electrónico a [FCC504@fcc.gov](mailto:FCC504@fcc.gov).*

*Para recibir información sobre éste y otros temas de la FCC para el consumidor a través del servicio de suscripción electrónica de la Comisión, visite [www.fcc.gov/cgb/contacts/](http://www.fcc.gov/cgb/contacts/) (en inglés).*

*Este documento tiene como único propósito educar al consumidor y no afectará ningún procedimiento o caso sobre este asunto u otros relacionados.*

*Última revisión: 12 de mayo, 2011*

