

digitando personalmente la dirección IP. No copie y pegue el link del mensaje.

- No envíe su información por e-mail. Este no es un método seguro para transmisión de información personal. Si requiere enviar sus datos por Internet, verifique que el sitio contenga indicadores acerca de su seguridad, como un candado en la ventana del navegador o la sigla "https" al inicio de la dirección. La "s" indica que se trata de un sitio seguro. Desafortunadamente, ningún icono es garantía de seguridad total, algunos estafadores han falsificado íconos de seguridad.
- Use un antivirus actualizado. Algunos mensajes de *phishing* contienen programas espías (spyware) que detectan sus actividades en la red o bien pueden contener virus que destruyan su información. En caso de poseer banda ancha, un cortafuegos (firewall) es esencial. Ayuda a mantenerse invisible en Internet y bloquea los intentos de acceso no autorizados desde el

exterior. Finalmente, mantenga actualizado su sistema operativo, instalando los parches gratuitos que se pueden bajar de los sitios corporativos.

- Siempre sea cauto al momento de abrir o descargar cualquier archivo adjunto de correos electrónicos que reciba, sin importar la fuente que se lo envió.

Lo mencionado anteriormente puede parecer cercano a la paranoia, pero estas medidas no tienen otra finalidad que dar algo de tranquilidad mientras se aprovecha todo lo bueno que ofrece Internet en sus muchas aplicaciones, sin correr el riesgo de caer en manos inescrupulosas que sacan partido de las deficiencias del sistema para su propio beneficio.

Fuentes:

Comisión Federal de Comercio para el Consumidor, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

Enciclopedia en Internet "Webopedia", <http://www.webopedia.com/TERM/p/phishing.html>

* * *