- Nunca respondas a solicitudes de información personal a través de correo electrónico. Si tienes alguna duda, ponte en contacto con la empresa que supuestamente te ha enviado el mensaje.
- Pon mucha atención en el URL del sitio Web que estas visitando. Los sitios Web maliciosos pueden parecer idénticos a los sitios legítimos, pero el URL puede tener variaciones o un nombre de dominio diferente.
- Asegúrate que el sitio Web utiliza cifrado.
- Instala y actualiza tu software antivirus, firewalls personales y filtros de correo electrónico.
- Instala en tu sistema operativo todas las actualizaciones de seguridad que se publican periódicamente.
- Instala una barra antiphishing en tu navegador Web (conocidas también como scam blocker). Estas herramientas están disponibles para los principales navegadores de Internet como Mozilla Firefox e Internet Explorer.

¿Qué barras antiphishing existen?

Para ayudar a protegerse contra ataques de Phishing Scam, varios proveedores han desarrollado barras que te pueden ayudar a identificar sitios Web maliciosos que usurpen la identidad de alguna organización que tenga presencia en Internet.

A continuación se listan los principales proveedores de barras antiphishing:

Netcraft
http://toolbar.netcraft.com/
Filtro de Suplantación de Identidad (Phishing) en Microsoft Internet Explorer
http://support.microsoft.com/kb/930168/es
Cloudmark Anti-Fraud Toolbar
http://www.cloudmarkdesktop.com/
Filtro de Phishing en Firefox
http://www.mozilla.com/en-US/firefox/phishing-protectionom/