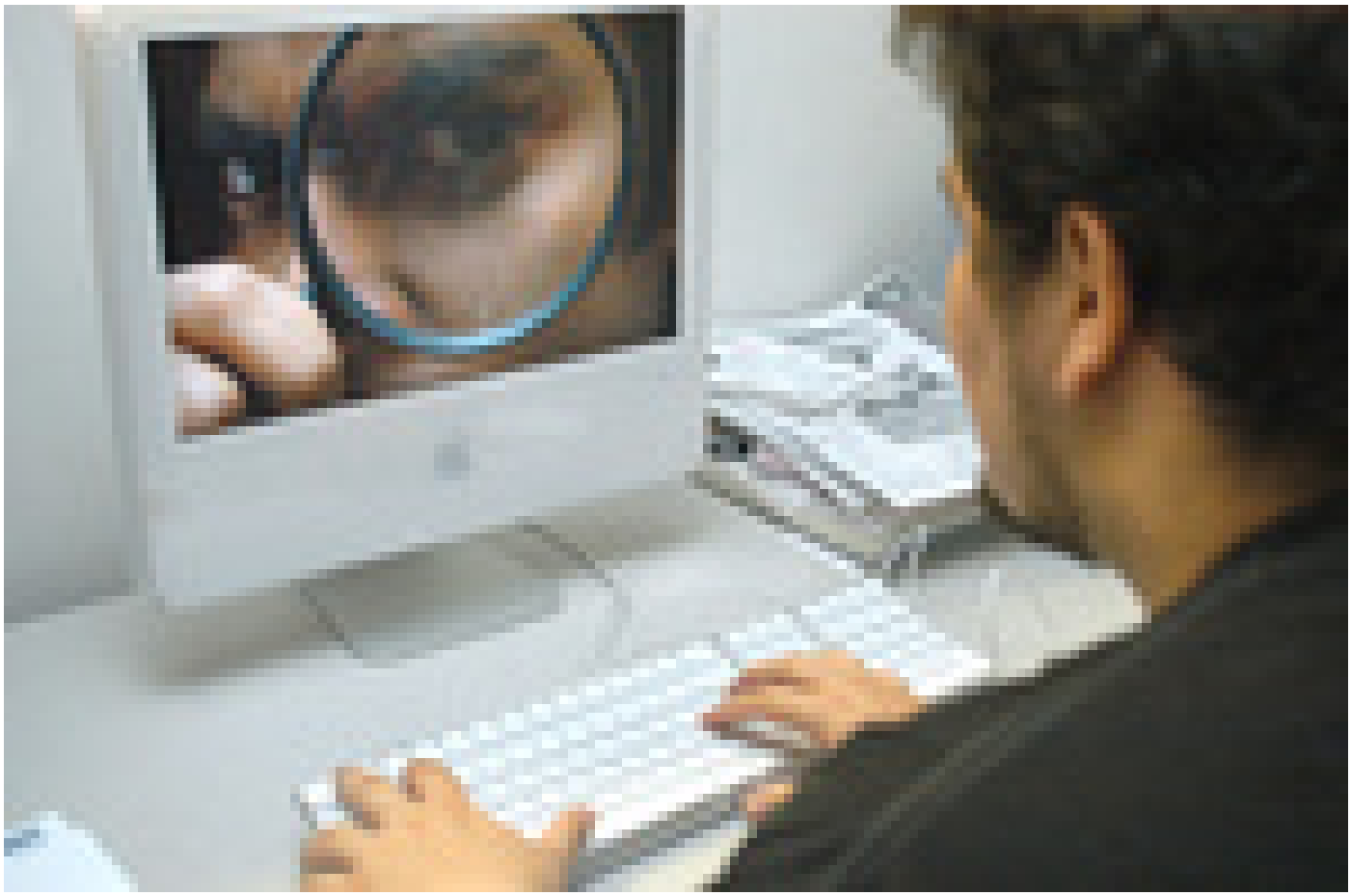
UNIVERSIDAD DE COSTA RICA

La privacidad no está garantizada en internet

24 MAR 2008



La experta en seguridad informática dijo que los usuarios de internet son observados por las empresas proveedoras de servicios gratuitos mientras envían un correo electrónico, durante la navegación web y en la transmisión de datos. (foto: Omar Mena)

Enviar un correo electrónico, conversar por el *chat*, realizar una transacción o introducir información personal en sitios web que así lo requieren no garantiza ninguna seguridad para los usuarios de internet, quienes se ven expuestos a que sus datos sean utilizados por empresas, gobiernos, patronos y por personas particulares con malas intenciones.

Así lo aseguró la Dra. Gabriela Barrantes, profesora de la Escuela de Ciencias de la Computación e Informática de la Universidad de Costa Rica.

Barrantes analizó la privacidad en internet y concluyó que contrariamente a lo que la gente cree, internet no es un medio seguro para la protección de información sensible, ya

que todos los datos que circulan en la red son susceptibles de ser interceptados y utilizados con distintos fines.

La experta en seguridad informática aseguró que no hay estudios que revelen cuál es la situación en Costa Rica; sin embargo, en países como Estados Unidos los grupos defensores de los derechos civiles han sacado este tema a la luz pública y defendido el derecho a la privacidad.

De acuerdo con Barrantes, los usuarios de internet son observados mientras realizan distintas operaciones: cuando envían un correo electrónico, durante la navegación web y la transmisión de datos, por las empresas proveedoras de servicios gratuitos, a través de los datos de manejo público y de métodos exóticos.

El protocolo http, de la navegación web, transmite mucha información acerca de los usuarios que no se puede bloquear. Asimismo, mientras se navega se pueden instalar en el computador personal programas mal intencionados, tales como *web bugs*, *cookies*, virus y *spyware*, que son programas que rastrean información sensible.

Otra práctica a la que están expuestos los usuarios es a la ingeniería social, concepto de la seguridad informática definido como la práctica de obtener información confidencial a través de la manipulación o engaño de usuarios.

Correo, el menos seguro

Para Barrantes, uno de los medios menos seguros en la red es el correo electrónico y por algo es la herramienta favorita para la realización de fraudes.

“El correo electrónico es para mí la fuente de todos los males”, dijo la especialista, quien explicó que los mensajes que se envían por la vía electrónica casi siempre se transmiten en texto claro, salvo en muy pocos casos que circulan cifrados.

Los proveedores de correo gratuito no solamente recolectan en su servidor la correspondencia de sus usuarios, sino que también otros datos acerca de los patrones de comportamiento, preferencias e intereses de estos.

En el 2006, el gobierno de George Bush solicitó a las empresas proveedoras de servicios de internet, entre estas Google, AOL, Yahoo y MSN, información sobre sus usuarios como material de apoyo para una ley sobre pornografía infantil.

Igualmente, en cualquier parte del mundo estas compañías están obligadas a proveer información al Poder Judicial cuando este así lo solicite.

Otra manera de espiar a un usuario es durante la transmisión de datos, lo cual se puede hacer con mucha facilidad a través de una red local.

Barrantes llamó la atención sobre el cuidado que se debe tener cuando se realizan compras por internet, ya que la operación puede ser muy segura pero la debilidad está en el destino.

“Algunos vendedores de artículos por internet creen que la seguridad no es importante y no establecen medidas para la protección de información valiosa que tienen en sus computadoras”, advirtió Barrantes.

Según la especialista, los enlaces inhalámbricos, como Wi-Fi, son otra fuente importante de fuga de datos, lo mismo que los teléfonos celulares.

Métodos exóticos

Entre algunas formas exóticas creadas para el rastreo de información sobresale la reconstrucción de “teclazos” mediante análisis acústico y de la imagen del monitor mediante la radiación emitida por una pantalla.

Los datos públicos, que son aquellos solicitados a sus clientes por las instituciones y empresas, atentan también contra la privacidad y la seguridad de las personas, ya que usualmente están disponibles en la red sin restricciones.

Además, existen empresas virtuales que proporcionan información sobre cualquier persona física o jurídica y ofrecen servicios tales como el monitoreo de propiedades.

La experta de la UCR manifestó que en Costa Rica no existe legislación específica que proteja los datos en internet, aunque mencionó algunos instrumentos jurídicos nacionales e internacionales que establecen el derecho a la privacidad, entre ellos la Constitución Política, la Declaración Universal de los Derechos Humanos y la Convención Americana de los Derechos Humanos.

Insistió en que la recolección de datos sobre las personas debería ser regulada y las entidades públicas y privadas están obligadas a tomar medidas.

Finalmente, Barrantes dijo que los usuarios de internet deben aplicar buenas prácticas en relación con lo que escriben en la red, asegurarse de que las transacciones bancarias estén cifradas así como toda la información sensible, y tener en cuenta que los servicios “gratuitos” no lo son pues siempre tienen un doble propósito.

A los jóvenes les recomendó tener mucho cuidado con la información y fotografías que suben a los *blogs* personales.

Patricia Blanco Picado.
Periodista Oficina de Divulgación e Información
patricia.blancopicado@ucr.ac.cr