

08/02/2010

[www.enisa.europa.eu](http://www.enisa.europa.eu)

## 17 reglas de oro para combatir los riesgos y navegar con seguridad en las redes sociales móviles

En breve estará en Internet: Las 17 reglas de oro para combatir los riesgos en línea y para una navegación más segura en las redes sociales móviles

La agencia europea de 'ciberseguridad', ENISA (European Network and Information Security Agency) presenta hoy un [nuevo informe](#) sobre el acceso a las redes sociales a través de teléfonos móviles. El informe señala los riesgos y amenazas del uso de las redes sociales a través de los dispositivos móviles (por ejemplo: usurpación de identidad, fuga de datos corporativos y riesgos de daños en la imagen). Además, en el informe se ofrecen 17 reglas de oro para combatir estas amenazas.

Las redes sociales online (SNSs por sus siglas en inglés) han vivido una tendencia de crecimiento extraordinario 211 millones de usuarios (de 283 millones) en Europa utilizan los SNS, sobre todo, Facebook en 11 de los 17 países estudiados. Los SNS y otras herramientas digitales son la nueva manera de comunicarse con los contactos laborales y personales. Por consiguiente, las formas de conocer gente, compartir opiniones, aportar información e ideas están cambiando. Con el aumento de la popularidad de las SNS, la demanda de un acceso al instante y continuo a través del teléfono móvil ha aumentado, por ejemplo, las redes sociales móviles (MSN). Más de 65 millones de usuarios acceden a la red social Facebook mediante su dispositivo móvil. Los usuarios de MSN son un 50% más activos que los usuarios que no utilizan móviles, y se estima que en Europa serán unos 134 millones para el año 2012.

Muchos usuarios de MSN utilizan también su teléfono como un dispositivo de respaldo para correos electrónicos empresariales, datos personales, contactos, imágenes y códigos de acceso. Como consecuencia, perder un móvil puede suponer un grave daño, por ejemplo, cuando se utilizan para entrar de manera ilegítima al MSN. Muchos teléfonos móviles vienen con funciones preempaquetadas y aplicaciones de MSN integradas (servicios listos y preparados).

Varios casos de Italia, Francia, España, Grecia y el Reino Unido son testigo de que muchos usuarios de los SNS y MSN no son conscientes de los riesgos y peligros que afectan a la privacidad, y las amenazas relacionadas con el uso inadecuado de la información que se expone en una SNS y la adecuada protección de la privacidad en línea.

08/02/2010

[www.enisa.europa.eu](http://www.enisa.europa.eu)

En este informe se identifican riesgos y amenazas de MSN. [El informe](#) de la ENISA ofrece una descripción general de la situación y subraya que los usuarios de MSN en particular, deben de ser más conscientes de cómo utilizar de una manera más segura MSN en un teléfono móvil para evitar consecuencias inesperadas y dañinas. Los riesgos incluyen: usurpación de identidad, daños graves a la reputación personal o empresarial o fuga de datos. Dos casos de estudio de interés:

- **Perfil falso en Facebook.** Un profesor de la Universidad de Turín descubrió que alguien había creado un perfil haciéndose pasar por él en Facebook con características ofensivas que afectaban a su reputación.

- **Fuga de datos/reputación corporativa.** Tras un incidente ocurrido en 2008, la aerolínea Virgin Atlantic despidió a 13 miembros de su personal que habían escrito comentarios en Facebook en los que, por ejemplo, criticaban la limpieza de la flota de la compañía y los pasajeros. Igualmente, el personal de facturación de British Airlines de Gatwick escribió mensajes en Facebook diciendo que los viajeros 'olían mal' y las operaciones en Heathrow eran caóticas.

El documento ofrece también una perspectiva completa sobre el mundo de los SNS bajo el punto de vista de la directriz europea de la protección de datos (Dir. 95/46/EC). El director ejecutivo de la ENISA Udo Helmbrecht comenta: "Este informe ofrece consejos prácticos a los usuarios sobre cómo estar en línea de manera más segura, en cualquier lugar y momento, y al mismo tiempo pueda disfrutar de las redes sociales móviles".

En el documento se incluyen 17 'reglas de oro' prácticas. Algunas de ellas son:

- Recuerde desconectarse de la red social una vez ha finalizado la navegación.
- No permita que la red social recuerde su contraseña (esta función se llama 'Autocompletar').
- No mezcle los contactos empresariales con sus amistades.
- Informe inmediatamente de la pérdida de un teléfono robado o perdido que contenga contactos, imágenes o datos personales en su memoria.
- Configure correctamente el nivel de seguridad del perfil.

Para ver todas las recomendaciones, puede descargarse el informe entero. (<http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens>).

08/02/2010

[www.enisa.europa.eu](http://www.enisa.europa.eu)

Para concertar entrevistas: Ulf Bergstrom, portavoz, ENISA, [press@enisa.europa.eu](mailto:press@enisa.europa.eu), Móvil:  
+30-6948-460143, o Isabella Santa, Senior Expert Awareness Raising. ENISA,  
[awareness@enisa.europa.eu](mailto:awareness@enisa.europa.eu)