

Los 5 peores errores que puedes cometer en Facebook

Las [redes sociales](#) son una forma genial de comunicarnos y estar en **contacto con amigos**, familiares y seres queridos que por cualquier razón no vemos tan a menudo como nos gustaría en directo; **pero son también uno de los mejores vehículos para ponernos en peligro frente a delincuentes, que encuentran en ellas una excelente fuente de información** que pueden utilizar para suplantar tu identidad, para atacar tus ordenadores o incluso para entrar a robar en tu domicilio. Por ello, **el desarrollador de [aplicaciones de seguridad](#) Kaspersky Lab ha publicado en su blog los 5 peores errores que puedes en Facebook.**

1.- Publicar tu biografía completa

Para el desarrollador, publicar tu biografía completa, aunque te dará un montón de felicitaciones cuando sea tu cumpleaños o cuando seas padre, **puede servir a ciber-delincuentes para recabar datos sobre ti o entrar en tus cuentas de banco.** Del mismo modo, no publiques los nombres de familiares, mascotas y [otros](#) datos similares que pueden servir para ataques de ingeniería social.

2.- Publicar tus posts de manera pública

Revisa bien tu cuenta de Facebook para que tus actualizaciones de estado sean vistas sólo por tus amigos o si acaso por los amigos de tus amigos. Ten en cuenta que, por ejemplo, redes como Facebook se están empleando para examinar los perfiles de candidatos a un trabajo; de manera que quizá lo que a ti te parece que es algo que publicas en una red privada o para tus amigos puede hacer que no te contraten, o incluso que te despidan.

3.- Usar contraseñas que no son seguras

Seguramente tienes mucha información privada en Facebook y si quieres que siga siendo así, **debes usar una contraseña segura en esta red ([consulta nuestros consejos para ello](#))**, activar la doble verificación y **no usar tu contraseña de Facebook con ningún otro servicio.**

4.- Compartir tu ubicación

Aunque te parezca divertido compartir tu ubicación a menudo para contar que estás en sitios geniales, **al hacerlo ayudas a los posibles delincuentes a saber donde vives o trabajas**, o cuándo te ausentas de tu domicilio, lo que puede ser especialmente peligroso para niños y jóvenes. **Así, desactiva la localización de las fotos, no uses la función lugares** o crea una lista reducida y controlada de contactos que pueden ver tu ubicación.

5.- Agregar amigos que no son amigos

Esto puede que te haya pasado: **de repente te pide agregarte como amigo alguien que no conoces en absoluto o que apenas conoces, pero como tienes muchos amigos en común aceptas la solicitud.** Pues no deberías hacerlo porque **al aceptarle puede ver tu información personal** y porque el mismo engaño que ha usado para que le agregues puede extenderlo a tus amigos que confiarán en esa persona.

**ES UNA INFORMACIÓN DEL PUNTO DE INFORMACIÓN
JUVENIL**

P.I.J