

CIBERSEGURIDAD

El CNI nos pide que usemos un poco la cabeza cuando entremos en las redes sociales

El Centro Criptológico Nacional (CCN-CERT), en su Informe de Buenas Prácticas en Redes Sociales, defiende que un uso inteligente de las redes sociales no difiere del uso responsable que cualquier persona adoptaría en el espacio físico.



Imagen: GERALTJ PIXABAY

MADRID, 07/08/2018 11:32

EUROPA PRESS

El 42% de la población mundial, 3.196 millones de personas, utiliza las redes sociales, donde **los usuarios se enfrentan a riesgos como la ingeniería social, la suplantación de identidad o la publicidad dañina o engañosa**, como recoge la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT), en su [Informe de Buenas Prácticas en Redes Sociales](#).

El CCN-CERT, adscrito al Centro Nacional de Inteligencia (CNI), defiende que un uso inteligente de las redes sociales no difiere del uso responsable que cualquier persona adoptaría en el espacio físico.

Por un lado, explica que los usuarios bienintencionados acceden a las redes sociales para mantenerse en contacto con sus familiares y amigos o para ver contenido de su interés. Sin embargo, **en ellas también hay usuarios malintencionados, que emplean las redes sociales como puerta de entrada para realizar ciberataques** y comprometer la seguridad de los demás.

La ingeniería social, el robo o la suplantación de identidad, el ciberacoso, el daño a la reputación, la publicidad dirigida son algunos de los riesgos a los que se enfrentan los usuarios de redes sociales. Además, la información que se comparte puede dar lugar a amenazas en el mundo real, como robos o acoso.

En este sentido, el informe alerta a los usuarios de que la cantidad de detalles personales disponibles en el ciberespacio incrementa el riesgo de que sean utilizados maliciosamente, y ofrece **una serie de consejos** para hacer un uso seguro y responsable de estas herramientas de comunicación.

Ojo a lo que se comparte

Desde CCN-CERT explican que el perfil de usuario, un "sitio permanente encabezado por fotografías, datos personales e información sobre estudios, profesión, gustos, intereses, amigos y familia", **aporta "mucho más información de la persona que su DNI o pasaporte"**.

Los perfiles suelen estar a la vista de todo el mundo, por lo que es "clave" revisar la información que se comparte en ellos, ya que serán "la carta de presentación" de la identidad del usuario en Internet.

Además de la información que se comparte en el perfil, **el usuario debe "reflexionar" sobre los contenidos que publica en las redes sociales**. Estos contenidos están a la vista de otras personas, que los ven y los analizan y emiten juicios. "Si se quiere un juicio justo, se han de controlar los propios contenidos", recomiendan desde CCN-CERT.

Las redes aportan "mucho más información de la persona que su DNI"

Hay una serie de contenidos sensibles que no se deben compartir, como documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos. Estos contenidos, propios o

sobre otras personas, aumentan las probabilidades de que alguien sea víctima de robo de identidad, de ciberacoso u otra conducta ilícita que utilice esa propia información para perjudicar al usuario.

Tampoco se puede difundir información privada sobre otras personas sin consentimiento, ni etiquetar con su nombre a aquellas personas que no tienen perfil en la red social sin su permiso.

Extremar las precauciones

Desde CCN-CERT señalan que **"en el ciberespacio aplica el principio de prevención ante lo desconocido"**. Esto se traduce en no hacer clic en contenidos sobre los que no se tenga claro su origen y aumentar la cautela ante mensajes de identidades desconocidas.

Una contraseña robusta ayudará a proteger la cuenta de usuario, una protección que se incrementará si se emplea un sistema de dos factores de autenticación, siempre que este método sea viable.

Las redes sociales disponen de un menú de configuración de privacidad que conviene revisar, tanto para el perfil como para el contenido que se comparte. Internet está lleno de "ojos digitales", como apuntan desde CCN-CERT, por lo que **hay que compartir sólo aquello de lo que se está seguro que se quiere mostrar a los demás**.

Por lo mismo, también se recomienda desactivar la geolocalización desde el menú de configuración, puesto que puede ofrecer "un mapa" de la vida del usuario o de parte de ella que lo puede poner en riesgo.

Actuar igual que en el mundo físico

El CCN-CERT, como ha indicado, defiende un uso inteligente de las redes sociales, que entiende como actuar en Internet de la misma manera en que se haría en el mundo físico. Esto significa, por ejemplo, que hay que cuidar y proteger las relaciones en el ciberespacio y **no aceptar sin más todas las solicitudes de amistad de desconocidos**.

Se trata de ser conscientes de que la primera línea de defensa para la protección en el ciberespacio es uno mismo. De esta forma, la ayuda que puedan prestar las instituciones y organizaciones de ciberseguridad será mucho más eficiente.