El CNI pone la lupa en Facebook, Twitter e Instagram y advierte de sus peligros

- El organismo publica un decálogo de recomendaciones para protegerse de ciberataques y otras amenazas.
- Twitter se contagia de Facebook y paga en Bolsa su reducción de usuarios

7 agosto, 2018 - 13:44

EN: CNI REDES SOCIALES FACEBOOK TWITTER INSTAGRAM

J.G.O.

El usuario es el 'talón de Aquiles' de la seguridad en redes sociales. Bajo esta advertencia, **el Centro Nacional de Inteligencia (CNI)** ha divulgado un informe en el que **explica los principales riesgos** a los que nos exponemos al compartir información en plataformas como Facebook, Twitter o Instagram **y qué medidas debemos tomar** para protegernos.

En el documento se asegura que hasta **un 13% de quienes poseen perfiles** en redes sociales han sido **víctimas de robos de identidad**, y que un 69% de adultos y un 88% de adolescentes se exponen a alguna forma de acoso o crueldad en ellas. Y se subraya que la génesis de estos problemas no está en la tecnología, sino en las personas.

"Aunque el *software* y los dispositivos *hardware* puedan dotarse de las últimas medidas de ciberseguridad, al final -que

Atención a los datos bancarios

El organismo recuerda que cuando un contenido entra en Internet, es muy complicado "hacer que desaparezca de este ecosistema". Y como ejemplo del peligro que esto entraña, señala que **el 81% de los bebés tiene presencia en la web** a través de fotos, vídeos e información compartida por sus padres, con la particularidad de que esos datos, a diferencia del entorno analógico, quedarán archivados en el ciberespacio "probablemente para siempre".

Por este motivo, el CNI aconseja que **nos abstengamos de transmitir números de cuentas bancarias o tarjetas de crédito**, ya que aunque redes sociales como Facebook, Twitter o plataformas como WhatsApp tengan sus conexiones cifradas, una vez que el mensaje circula por la red **deja de estar bajo control**.

Precauciones en el perfil personal

El CCN realiza una serie de recomendaciones sencillas para prevenir que nuestra huella digital pueda ser utilizada por personas o grupos con intenciones maliciosas. Entre ellas está el **evitar que el nombre de usuario en las redes** sociales **coincida con la dirección de correo electrónico** habitual.

Y es que, aunque sea común que una persona intente mantener el mismo nombre en varias redes sociales como un rasgo identificativo en el ciberespacio, hacerlo igual que el del *e-mail* **facilita a los cibercriminales** obtener nuestra dirección y **realizar prácticas de *phishing*** (obtener datos personales y financieros sin consentimiento) **o robo de identidad** en la web.

La buena práctica más evidente, para evitar que los criminales puedan valerse de los datos de las redes para cometer, en este caso, crímenes en el mundo físico como robos de viviendas o vehículos, es **no consignar direcciones postales específicas ni compartir la localización** en nuestro perfil.

Resistir en vacaciones

En este mismo sentido, el organismo adscrito al CNI nos advierte que al **compartir fotos o vídeos que muestren que nos encontramos lejos de casa**, especialmente en vacaciones, podemos **facilitar eventuales robos**. Al igual que construir un perfil que enseñe un determinado 'nivel de vida', puede aumentar el riesgo de sufrir secuestros con el fin de obtener un rescate.

Por último, el informe nos aconseja "hacer lo que casi nadie hace": **leer las condiciones de prestación de servicios de la red social** correspondiente, ya que en ellas se establece no solo la manera en que estas plataformas comparten la información que aportamos voluntariamente, sino también **otros datos del usuario que recogen automáticamente** y utilizan sin que, a menudo, seamos conscientes de ello.