IDENTIDAD DIGITAL

¿Qué es la identidad digital?

TU IDENTIDAD DIGITAL DEPENDE DE TI.

DECÁLOGO DE SEGURIDAD EN REDES SOCIALES

Decálogo de seguridad en Redes Sociales

1. Un sitio permanente encabezado por fotografías, datos personales e información sobre estudios, profesión, gustos, intereses, amigos y familia proporciona mucha más información de la persona que su DNI o Pasaporte. Además, quedaría a la vista de todo el mundo. Es clave, prestar atención a cómo uno define su perfil en redes sociales, ya que será la carta de presentación de su identidad en el ciberespacio.
2. Reflexionar sobre los contenidos que se comparten en redes sociales. Cada vez más personas y empresas observan y analizan las redes sociales para adoptar un juicio sobre otras personas. Si se quiere un juicio justo, se han de controlar los propios contenidos.
3. No compartir contenidos sensibles sobre la vida personal o la de otros en redes sociales: documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, etc. Cuanto más contenidos de este tipo se compartan, más probabilidades hay de ser víctima de un robo de identidad, de ciberacoso u otra conducta ilícita que utilice esa propia información para perjudicar al usuario.
4. En el ciberespacio aplica el principio de "prevención ante lo desconocido". No hacer clic en contenidos sobre los que no se tenga claro su origen o propósito y aumentar la cautela ante mensajes de identidades desconocidas. En definitiva, huir de la tentación de todo aquello que cuanto más desconocido, más atractivo parece.
5. Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.
6. Controlar la geolocalización de perfiles y contenidos en redes sociales. Desactivar la geolocalización por defecto en el menú de configuración de los perfiles y hacer un uso inteligente de la misma, pensando en cada caso si interesa que los demás tengan un mapa de tu vida o de parte de ella.
7. Comprobar la configuración de privacidad tanto en el perfil como en los contenidos que se comparten. Tomar conciencia de que el ciberespacio está lleno de ojos digitales y que se debe mostrar únicamente lo que se está seguro que cualquiera puede ver. Ante la duda, mantener la información privada para amigos y contactos.
8. No difundir información privada sobre otras personas sin su consentimiento y no etiquetar por su nombre a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso para hacerlo.
9. Cuidar y proteger las relaciones en el ciberespacio. Mantener en privado la lista de contactos y analizar en detenimiento las solicitudes de amistad de desconocidos.
10. Adoptar la consciencia de que la primera línea de defensa para la protección en el ciberespacio es uno mismo. De esta manera, la ayuda que instituciones y organizaciones de ciberseguridad presten será mucho más eficiente y uno mismo será de ayuda inapreciable para mantener unas redes sociales seguras.

CCN-CERT BP/08: Buenas Prácticas en Redes Sociales 61

TU DECIDES EN INTERNET