Extorsión, usurpación de identidad y bullying: las principales ciberamenazas para niños y mujeres

Multimedia

El incremento de la ciberviolencia "es uno de los grandes problemas que afectan a los segmentos de población más vulnerables en la actualidad", según ha indicado S2 Grupo. Los principales peligros son la ciberextorsión por sexting, la usurpación de identidad, el ciberbullying, dar de alta a la víctima en webs no deseadas para ridiculizarla, crear falsos perfiles compartiendo información denigrante, la instalación de programas espía sin que la víctima lo sepa para controlarla o el acoso en Internet

La empresa valenciana S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, ha contextualizado en una nota de prensa que ONU Mujeres ha anunciado que una de cada diez mujeres de la Unión Europea ha sufrido ciberacoso desde los 15 años de edad (recibiendo correos electrónicos o mensajes SMS no deseados, sexualmente explícitos u ofensivos, etc.). La compañía también ha citado un estudio de la ONG Bullying Sin Fronteras, dónde se asegura que 7 de cada 10 niños sufren ciberacoso o acoso a diario.

"La situación es realmente dura y puede empeorar en los próximos años. Por eso, es necesario que continuemos trabajando en la concienciación y en el uso seguro de la tecnología y los entornos conectados. Por ejemplo, es esencial que conozcamos tanto los principales peligros que nos podemos encontrar como qué tenemos que hacer en caso de ser víctima de la ciberviolencia, para poder protegernos y fortalecernos en estas situaciones", ha declarado José Rosell, cofundador y CEO de S2 Grupo.

Ante esta situación, el equipo de expertos de S2 Grupo ha elaborado un decálogo con consejos que servirán para proteger a toda la sociedad frente a la violencia digital:

1. Utilizar en las redes un doble factor de autenticación
2. Configurar los perfiles como privados para proteger la información.
3. Limitar quién se puede interactuar en las redes sociales.
4. Seleccionar concienzudamente las personas que se aceptan en las redes sociales.
5. Bloquear y reportar comportamientos que incumplan las normas.
6. No contestar ni interactuar ante provocaciones o comportamientos nocivos en redes.
7. Ser cautos y precavidos con la información que compartimos.
8. Instalar solo aplicaciones oficiales y limitar los permisos que se les conceden desde el móvil.
9. Vigilar a los menores cuando utilizan Internet. Es muy importante educarlos en sus relaciones digitales y acompañarlos para que se realicen desde el

respeto y la seguridad.
10. Buscar apoyo emocional y legal si es necesario.

Junto a esto, desde S2 Grupo se ha resaltado que en caso de ser víctimas de la violencia digital es importante seguir estos pasos:

1. No borrar nada. "Muchas veces, el primer impulso es borrar los comentarios ofensivos para deshacernos de ellos porque nos causan dolor o vergüenza. Pero nuestra recomendación es no borrarlos porque son muy importantes para denunciar los hechos ante las autoridades", ha explicado José Rosell.

2. Pedir ayuda y asesoramiento adecuado a la situación . Algunos organismos con los que se puede contactar y que pueden ser de gran ayuda en este punto son la Delegación del Gobierno de España contra la Violencia de Género, la Asociación ¡Stop! Violencia de Género Digital, el Observatorio de Violencia Digital, el Instituto Nacional de Ciberseguridad o la Agencia Española de Protección de Datos.

3. Denunciar los hechos ante los Cuerpos y Fuerzas de Seguridad del Estado . La Policía Nacional cuenta con una brigada especial dedicada a la investigación y persecución de los ciberdelitos que podrá ayudar. Si para certificar los hechos ocurridos ante la policía se necesitará de un perito informático especializado, la asociación ¡Stop! Violencia de género digital cuenta con un formulario en su web.