Los 7 "pecados" digitales de la Navidad

La empresa de ciberseguridad S2 Grupo ha advertido de que con la llegada de las Navidades, es fundamental incrementar las precauciones con el uso de la tecnología para evitar caer en las redes de los ciberdelincuentes que aprovechan el aumento de la interacción digital a través de felicitaciones, compras, etc., para actuar con fines delictivos

Por medio de un comunicado, el equipo de expertos de S2 Grupo ha destacado que durante las fiestas de Navidad pueden señalarse, principalmente, "7 pecados digitales".

El primero es no tener actualizado el antivirus. "Son muy frecuentes los envíos de felicitaciones divertidas en las que puede aparecer nuestra cara en un duendecillo, por ejemplo", apuntan desde S2 Grupo. Sin embargo, muchas veces, éstas llevan enlaces, en los que al clicar, se puede descargar malware directamente.

El segundo son los hoax o bulos. Se trata de noticias falsas para generar desinformación. Ejemplo de ello son "aquellos mensajes que advierten que si no lo reenvías la aplicación que utilizas puede pasar a ser de pago", informa la compañía.

El tercero es regalar un móvil usado sin hacerle un borrado seguro de los datos. Uno de los regalos más comunes en Navidad es un smartphone. Esto hace que el móvil antiguo se regale o venda de segunda mano. En ese caso, "es fundamental el realizar un borrado seguro de la información porque si no, el nuevo usuario podría tener acceso a fotografías y otros datos personales".

En cuarto lugar, está el "pecado" de no restringir los SMS Premium. En estas fechas, hay muchos programas de televisión en los que se insta a votar para participar en concursos enviando un SMS. Al hacerlo, se puede caer en la trampa de inscribirse a servicios de mensajes Premium que tienen elevados costes y de los que el usuario puede no ser consciente. Para evitarlo, la recomendación de S2 Grupo es restringir este tipo de servicios con la operadora de telefonía.

El quinto pecado digital que se señalan los expertos en ciberseguridad es utilizar pendrives sin cifrado, porque en caso de pérdida cualquiera podría acceder a la información que contengan.

En sexto lugar, está no tener instalado un software de localización para el Smartphone. Esto es importante para poder localizarlo si extravía o es robado.

En último lugar, S2 Grupo enfatiza que es clave no caer en la trampa de los descuentos excesivos. "Ésta es otra vía por la que podemos acabar siendo víctimas de la ciberdelincuencia. En estas fechas, especialmente, tenemos que comprar en páginas de confianza y evitar caer en la tentación del ciberchollo", apostilla el comunicado de S2 Grupo.

Datos de contacto:

Luis Núñez

667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional](#) [Sociedad](#) [Entretenimiento](#) [E-Commerce](#) [Ciberseguridad](#) [Ocio para niños](#)

NotasdePrensa

<https://www.notasdeprensa.es>