Publicado en Valencia el 06/11/2024

S2 Grupo alerta sobre el riesgo de fake news y estafas ante la situación de DANA en Valencia

La empresa valenciana de ciberseguridad y ciberinteligencia S2 Grupo ha emitido un comunicado a la ciudadanía para evitar caer en la desinformación y las estafas que proliferan tras el paso de la DANA por Valencia. En momentos de crisis, como el actual, la difusión de noticias falsas puede aumentar el caos y exponer a los usuarios a ciberataques, especialmente en contextos de solidaridad y donaciones, advierten

"Todo lo que difundimos genera un impacto y muchas veces no es precisamente positivo. Por eso, es esencial que nos cercioremos de la veracidad de lo compartido", afirma Eva López Granero, responsable de comunicación en ciberseguridad para sociedad y pymes de S2 Grupo.

En su comunicado, S2 Grupo destaca que es fundamental recurrir a fuentes oficiales de información, como las webs de los ayuntamientos de las zonas afectadas, la Agencia Estatal de Meteorología (AEMET), el 112 o la Policía Nacional, para asegurarse de que las noticias sean confiables y evitar contribuir a la cadena de desinformación que, en momentos de emergencia, suele extenderse rápidamente por WhatsApp y redes sociales.

La compañía también insiste en la importancia de que los ciudadanos verifiquen la autenticidad de los mensajes que reciben, ya sea comprobando lo que dicen las cuentas oficiales o realizando búsquedas adicionales. "Si algo no nos cuadra, si vemos algo raro en la imagen, antes de compartirlo de forma automática es importante que tomemos responsabilidad y hagamos una búsqueda correcta para comprobar que la información es veraz", añadió López Granero, quien recomendó herramientas de verificación como Maldita, EFE Verifica o Newtral, además de la búsqueda inversa de imágenes en Google.

Aumento de los ciberataques

Además de la desinformación, S2 Grupo ha advertido sobre el posible aumento de ciberataques de ingeniería social, como el phishing, que aprovechan el contexto de incertidumbre. "Es probable que nos encontremos emails pidiendo ayuda o donaciones que no hayan sido creados con fines legítimos", señala López Granero. En situaciones de emergencia, los ciberdelincuentes suelen intensificar su actividad, enviando correos electrónicos y mensajes que simulan peticiones de ayuda o donaciones para aprovecharse de la buena voluntad de las personas.

Para protegerse de estos fraudes, S2 Grupo recomienda prestar atención a detalles como el dominio del remitente del correo electrónico, ya que los organismos oficiales no utilizan cuentas genéricas de proveedores como Gmail, sino que emplean dominios específicos que deben revisarse con atención. "Estar atentos a este detalle puede ser clave", subraya López Granero.

Asimismo, antes de hacer clic en enlaces o descargar archivos adjuntos, es importante revisar que el contenido y el formato del mensaje coincidan con la identidad corporativa de la entidad que

aparentemente lo envía, y que no presenten errores ortográficos u otras señales de alerta. También se sugiere verificar los perfiles oficiales en redes sociales o la página web de la organización para confirmar la legitimidad de las solicitudes de donación, ya que "si es una donación legítima, estará comunicado en todas sus plataformas", concluyó la responsable de comunicación.

Datos de contacto:
Luis Núñez
S2 Grupo
667574131

Nota de prensa publicada en: Valencia

Categorías: Valencia Ciberseguridad Solidaridad y cooperación Servicios Técnicos Otros Servicios