Campaña correo fraudulento (phishing) en nombre de CrowdStrike

Image

Os informamos que se ha detectado una **campaña de correo malicioso**, tipo phishing, que pretende suplantar a la empresa de ciberseguridad CrowdStrike, aprovechando el incidente del pasado viernes que ha causado una interrupción a nivel global en multitud de sistemas Windows.

Los ciberdelincuentes están enviando correos electrónicos fraudulentos, **haciéndose pasar por CrowdStrike** en los que se pide al destinatario que se descargue un “parche de seguridad urgente” que arreglará el problema con su equipo. Los correos electrónicos pueden incluir líneas de asunto como "Acción inmediata requerida: parche de interrupción de CrowdStrike" o "¡Descargar la actualización crítica de recuperación de CrowdStrike!"

Estos mensajes tratan de engañarte para que entres en enlaces a sitios web maliciosos que parecen páginas de soporte reales. También es posible que te pidan descargar un archivo o que ingreses tus credenciales y contraseña.

Si recibes un correo electrónico de este tipo, **no hay que pulsar en ningún enlace**, **ni descargar nada** o meter tus datos en ningún lugar, ya que podrías comprometer tu información y podría dar lugar a que los ciberdelincuentes realizaran ataques contra los sistemas informáticos de la organización, con el enorme riesgo que eso supondría.

En su lugar, reporta siempre estos mensajes, por dos vías complementarias:

- Informando en el área personal de ayudaDIGITAL: https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud/mics/element/r/3850947F36FA01F9A57A001D
- Reenviando el correo sospechoso como archivo adjunto a la dirección: abuse@juntadeandalucia.es

Desde la Subdirección de Tecnologías de la Información y Comunicaciones y la Unidad de Seguridad TIC del SAS estamos llevando a cabo las medidas oportunas para solucionar estas incidencias por lo que **no es necesario que hagas nada** por tu parte, aparte de **reportarnos** cualquier tipo de **incidente** por los medios

habituales.

Extrema la precaución ante posibles correos sospechosos y ayúdanos a difundir este mensaje entre el resto de profesionales para que podamos **mantener la seguridad** y la integridad de nuestra organización.