Pasos a seguir ante una sospecha de correo malicioso (phising)

Image

La Subdirección de Tecnologías de la Información y Comunicaciones os informa que, ante la sucesión de ataques de phising contra las administraciones públicas de la Junta de Andalucía y el Servicio Andaluz de Salud que se han venido produciendo en las últimas semanas, os detallamos una serie de pautas a tener en cuenta para no caer en el objetivo de estos ciberataques.

- **No pulsar nunca** en los **enlaces** de estos correos maliciosos o no deseados
- **No abrir ni descargar** los archivos adjuntos de estos mensajes
- **No responder** a estos correos electrónicos **ni reenviarlos** salvo para informar sobre ellos
- **No proporcionar** jamás **nombres de usuario, contraseñas y otros datos personales** en las páginas webs a las que nos llevan estos enlaces sospechosos
- Ante la llegada de un correo sospechoso de *phishing*, **informar** a través de los canales de comunicación de ayudaDIGITAL

Os recordamos también que, bajo ningún concepto, está permitida la instalación de software sin licencia en los puestos de usuario. Esta acción también puede comprometer la seguridad de nuestros sistemas.

Rogamos tengáis en cuenta todos estos consejos para no caer en situaciones que ponen en riesgo tanto la prestación de la asistencia sanitaria como la privacidad de profesionales y pacientes.