El correo electrónico corporativo

Todos/as los/as trabajadores/as que realizan un tratamiento de datos están obligados a adoptar medidas técnicas y organizativas que garanticen la protección de datos personales. El conocimiento de los siguientes aspectos sobre el **correo electrónico corporativo** está al alcance de todos/as y contribuye a reducir los riesgos inherentes de su uso para los derechos y libertades de los/as interesados/as.

El correo electrónico corporativo hace referencia a aquellas cuentas de correo electrónico que se encuentran bajo un dominio de propia creación y no están asociadas a dominios como Hotmail o Gmail.

A continuación, se exponen algunas recomendaciones para hacer un buen uso del mismo, y así prevenir cualquier ciberataque a través de técnicas de ingeniería social:

- **Remitente seguro:** en primer lugar, hemos de fijarnos en el nombre, es decir, si es remitente conocido/a. Por otra parte, hemos de verificar si el correo es el que normalmente utiliza o si es el correo esperado. Finalmente, hay que comprobar que el nombre (antes del @) y el dominio (después del @) se encuentran bien escritos, ya que con frecuencia se utilizan dominios o nombres parecidos para engañarnos.
- **Asunto pendiente**: El asunto suele ser el primer gancho o reclamo, junto con el remitente, para engañarnos. Si han podido espiar con antelación nuestro correo, con quién nos escribimos, qué tipo de mensajes recibimos, etc., sabrán qué asunto poner e incluso cuándo esperamos recibir ese tipo de mensajes; por ello es importante tener claro qué correos tenemos pendientes a corto plazo.
- **Cuerpo del mensaje lógico:** hemos de comprobar que el cuerpo del mensaje sea coherente con todo lo anterior. Los/as ciberdelincuentes pueden emular logotipos o pies de firma, incluso el aspecto que tendría el mensaje que se quiere suplantar (por ejemplo, utilizando el mismo saludo o despedida). El mínimo

cambio ha de hacernos sospechar. Si el mensaje no se encuentra bien escrito (utiliza modismos, vocabulario poco frecuente, faltas de ortografía), o se encuentra en otro idioma; también puede considerarse como un indicio del que sospechar.

- **Archivos o ficheros adjuntos reconocibles:** verificar el nombre del fichero o archivo adjunto puede indicarnos si estamos ante mensaje malicioso, y por ello es importante comprobar el icono del archivo y la extensión del mismo (por ejemplo, en lugar de **.pdf** incluir la extensión **.exe**); o insertando un código que invierta el orden de los caracteres del documento adjunto.
- **Enlaces:** antes de hacer clic en ningún enlace lo revisaremos, es decir, comprobaremos que el enlace está relacionado con el contenido del mensaje (previa verificación de todo lo anterior). Para identificar enlaces sospechosos nos fijaremos en que pueden tener letras o caracteres de más o de menos (y pasarnos desapercibidas o podrían estar utilizando caracteres que se parecen en determinadas tipografías (1 y l, O y 0). Los enlaces aparentemente legítimos podrían ser enlaces que nos llevan a sitios web modificados para infectarnos o robarnos datos.

Ante cualquier duda, contacte con el Responsable informatica@huesca.es o el Delegado de Protección de Datos Personales dpdhuesca@unive.es