CIBERSEGURIDAD

CONSEJOS PARA IDENTIFICAR UN PHISHING

Revisa si el **DOMINIO** es correcto. Por ejemplo, podría poner @osakdetza, en lugar de @osakidetza.

Comprueba pasando el **CURSOR** por encima si el enlace al que te redirecciona es correcto y ten cuidado con los **DOCUMENTO ADJUNTOS** que pueda incluir el email.

Ten cuidado si el mensaje genera sensación de **URGENCIA o MIEDO** e incite a hacer clic de forma apresurada solicitando información confidencial.

COMPRUEBA POR OTRA VÍA, como por ejemplo: web oficial, teléfono de contacto u otros medios si la persona remitente es legítima.

Cuida tus **CREDENCIALES** de **ACCESO A LOS SISTEMAS** corporativos. No las compartas con nadie.

Revisa si la **REDACCIÓN** del mensaje contiene faltas ortográficas o el texto es incoherente, podría ser un indicio de mensaje sospechoso.

COMUNICA AL CAU

cualquier comportamiento sospechoso:

cau24x7@osakidetza.eus

Ext: 806350

¡Contamos contigo como agente de ciberseguridad de Osakidetza!

Osakidetza

EUSKO JAURLARITZA
GOBIERNO VASCO
OSASUN SAILA
DEPARTAMENTO DE SALUD