TÉCNICA DEL PHISHING
-¿CÓMO PREVENIRLO?-

POLICÍA NACIONAL

¿EN QUÉ CONSISTE?

→ Es un **envío indiscriminado** de **correos electrónicos** en los que se **suplanta la identidad** de entidades públicas o empresas privadas. También puede darse en distintas **modalidades,** como a través de SMS (**smishing**) o de llamadas telefónicas (**vishing**).

→ Los delincuentes **copian el estilo corporativo** de la organización que suplantan para **engañar a la víctima** y hacerle pensar que se trata de una entidad oficial.

→ A través de esta técnica se obtienen los **datos bancarios o personales de la víctima,** que son utilizados por los delincuentes para consumar delitos como **estafas o suplantación de identidad.**

¿CÓMO DETECTARLO?

→ Se comunica un **problema técnico, un envío pendiente de entrega, la suspensión de un servicio o suministro, un aviso urgente de cualquier tipo,** etc.

→ Se solicita la remisión de **datos personales, bancarios o fotografía de documentos de identidad.**

→ El mensaje puede contener **faltas de ortografía, errores sintácticos, etc.**

→ Remitente **desconocido o dominio mal tecleado** (ej: @policiia.es)

→ Se pide expresamente abrir **un adjunto o se acceda a un enlace.**

¿CÓMO SE PUEDE PREVENIR?

→ **No descargues** ningún tipo de archivo.

→ **No accedas** a ningún enlace.

→ **No facilites** nunca **datos personales ni bancarios.**

→ **No respondas** al correo si sospechas de que se trata de un phishing.

→ Mantén una **correcta configuración y actualización** de los equipos informáticos y del **antivirus.**

→ En caso de duda, **contacta** con la empresa o entidad de la que supuestamente se trate y **confirma** que efectivamente te han enviado dicho correo.

PARTICIPACIÓN CIUDADANA
POLICIA NACIONAL

participa@policia.es

SI ERES VÍCTIMA, ACUDE A UNA COMISARÍA DE POLICÍA NACIONAL PARA PRESENTAR DENUNCIA O PONLO EN CONOCIMIENTO DE LAS UNIDADES ESPECIALIZADAS A TRAVÉS DEL APARTADO "CONTACTA" DE WWW.POLICIA.ES