EL VALOR DE INTERNET

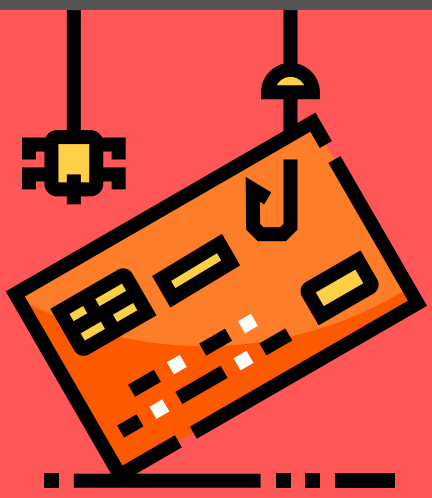
PHISING

Aragonesa de Servicios Telemáticos

#SOMOSAST
#ELVALORDEINTERNET
#PROTEGETE

17/05

ES UNA TÉCNICA UTILIZADA POR CIBERDELINCUENTES PARA OBTENER INFORMACIÓN PERSONAL DE LOS USUARIOS.

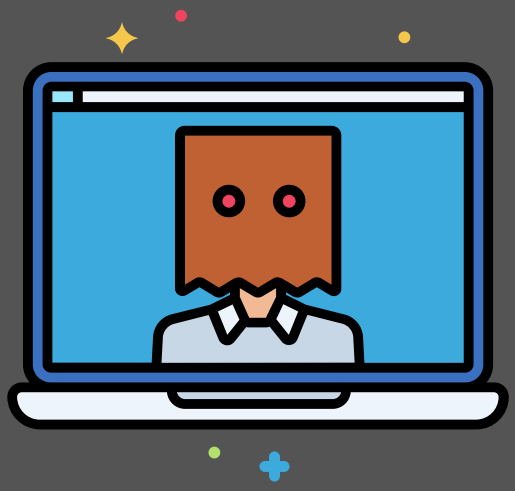


El mecanismo es el envío de mensajes aparentemente verídicos **suplantando** a una entidad para conseguir información de acceso de los usuarios y así poder acceder al resto de sus datos.

El mensaje puede llegar a través del correo electrónico, o de redes sociales, aplicaciones de mensajería instantánea o SMS.

#SOMOSAST
#ELVALORDEINTERNET
#PROTEGETE

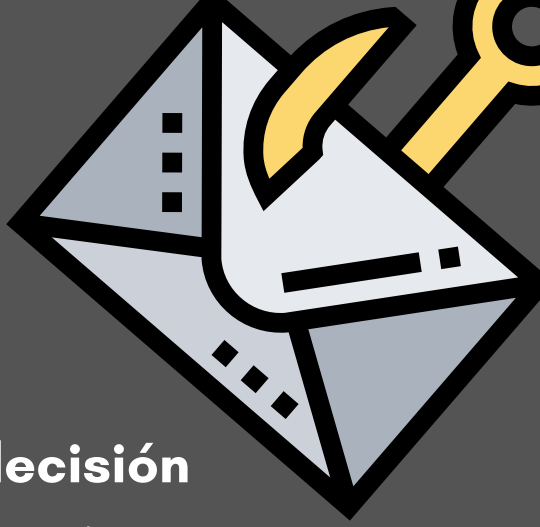
¿QUÉ TIPO DE ENTIDADES SON SUPLANTADAS?



- Organismos de la administración
- Bancos y compañías de crédito
- Servicios técnicos profesionales
- Empresas de servicios (mensajería, comercio,..)
- Instituciones sanitarias

¿QUÉ TEMÁTICAS UTILIZAN?

• Alertas (pago de una tasa, devolución de un pago, ingreso pendiente,...)
• Problemas con cuentas bancarias (bloqueo, problemas de seguridad, problemas con el saldo, necesidad de confirmación de PIN de tarjeta,...)
• Problemas con cuentas de usuarios (bloqueo, necesidad de confirmación de contraseña, caducidad, borrado, problemas de seguridad, ...)
• Ofertas y promociones (vales de descuento, productos gratis, ...)
• Ofertas de empleo



Los mensajes suelen contener **faltas de ortografía** y errores gramaticales.
Intentan engañar y forzar a tomar una **decisión rápidamente** para evitar unas consecuencias negativas para el usuario.
Normalmente llevan **archivos adjuntos infectados**, links a páginas web dañinas, o a páginas web que simulan ser la página oficial de un organismo o institución

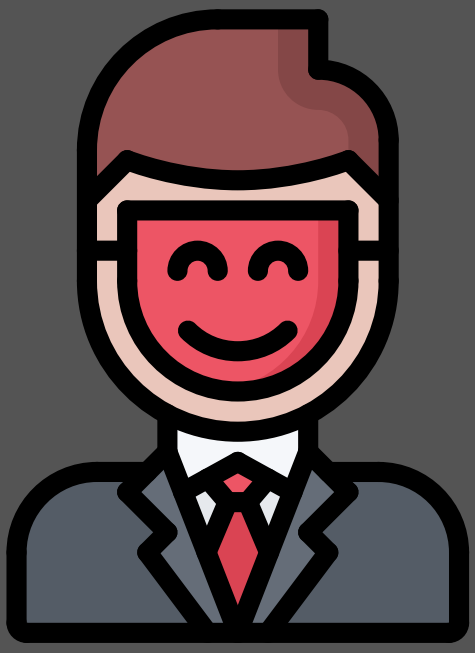
SI DETECTAS UN PHISHING

• **No facilites la información que te solicitan.**

• Si tienes dudas **consulta** directamente con la empresa o servicio que supuestamente te envía el mensaje.
• No accedas a los **enlaces incluidos** en el mensaje.
• **No descargues** ningún documento adjunto.
• Si es un mail, no contestes al correo.
• **Elimina el mensaje**, no lo reenvíes y **valora alertar** a tus contactos.

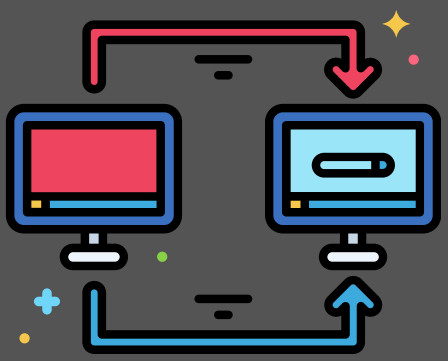
#SOMOSAST
#PROTEGETE
#ELVALORDEINTERNET

#NOPIQUES



No abras mensajes de usuarios desconocidos o sobre información que no hayas solicitado.
(Si te mandan una factura de un servicio que no has contratado, sospecha).

Ten precaución al seguir enlaces y descargar ficheros adjuntos de correos, aunque sean de contactos conocidos. (Si recibes un mensaje extraño de tu banco con un enlace para actualizar tus datos, sospecha).



No des información personal (nombre de usuario, contraseña, datos bancarios, etcétera).
(Si te obligan a enviar un dato con urgencia porque si no vas a perder tu cuenta de correo, o se te va a bloquear la cuenta bancaria, sospecha)

#ELVALORDEINTERNET
#PROTEGETE
#SOMOSAST

#SOMOSASTUR

#ELVALORDEINTERNET

#PROTEGETE

Ten precaución al seguir enlaces y descargar ficheros adjuntos de correos, aunque sean de contactos conocidos.

Si recibes un mensaje extraño de tu banco con un enlace para actualizar tus datos, sospecha).

Sospecha de las gangas y ofertas. (Si te comunican que acabas de recibir una herencia millonaria, sospecha).

QUE ALGO ESTE ESCRITO NO SIGNIFICA QUE SEA VERDADERO.

Si te piden dinero, cambio de cuentas de ingreso o similar **¡desconfía!.**
Usa algún medio alternativo para verificarlo.

Si sospechas de una petición que venga de un superior o de un proveedor o contacto habitual, llama a teléfonos que conozcas de antemano para confirmarlo.

La confianza en la autoridad y en la cercanía son herramientas que utilizan los ciberdelincuentes.

Y No, la AEAT no te va a enviar un correo para devolverte más dinero...

#SOMOSAST

#PROTEGETE

#ELVALORDEINTERNET