Phishing: el fraude que intenta robar nuestros datos personales y bancarios

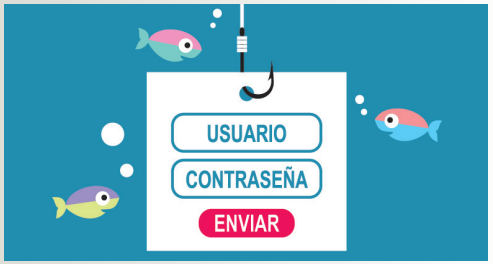
"He recibido un correo electrónico el cual me solicita que actualice los datos personales de mi cuenta corriente haciendo clic en un enlace, pero me extraña que la URL de mi banco no sea la misma de siempre. He llamado al banco y me han dicho que es una estafa conocida como phishing."

Entre los riegos con los que nos podemos encontrar cuando hacemos uso de Internet, está el phishing, una técnica usada por ciberdelincuentes para obtener información personal y bancaria de los usuarios suplantando a una entidad legítima como puede ser un banco, una red social, una entidad pública, etc.

Es importante que conozcas cómo funciona el phishing

*Los ciberdelincuentes que **ponen en circulación el phishing**, utilizan la **ingeniería social** para intentar obtener nuestra información privada. Captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser las legítimas de un determinado servicio o empresa.*

*Cualquier sistema que permita el envío de mensajes puede ser usado como medio para intentar robar nuestra información personal. En algunos casos pueden llegar intentos de robo de nuestra información personal a través de emails, mensajes SMS o MMS (**smishing**), de la misma manera que por cualquier herramienta de mensajería instantánea (WhatsApp, LINE, etc.) o red social.*



Consejos y recomendaciones

Trucos para evitar ser víctima de phishing

- *Sé precavido ante los correos que aparentan ser entidades bancarias o servicios conocidos con mensajes del tipo:*
  - *Problemas de carácter técnico de la entidad.*
  - *Problemas de seguridad en la cuenta del usuario.*
  - *Recomendaciones de seguridad para evitar fraudes.*
  - *Cambios en la política de seguridad de la entidad.*
  - *Promoción de nuevos productos.*
  - *Vales descuento, premios o regalos.*
  - *Inminente cese o desactivación del servicio.*
- *Sospecha si hay errores gramaticales en el texto.*
- *Si recibes comunicaciones anónimas dirigidas a "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta.*
- *Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.*
- *Revisa que el texto del enlace coincide con la dirección a la que apunta.*
- *Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com o @hotmail.com, no es buena señal.*

¿Qué debes hacer si detectas un caso de phishing?

- *No contestes en ningún caso a estos correos. Si tienes dudas pregunta directamente a la empresa o servicio que representa o **ponte en contacto con nosotros** para hacernos llegar tu consulta.*
- *No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto.*
- *Elimínalo y, si lo deseas, alerta a tus contactos sobre este fraude.*

No hagas clic en enlaces que recibas a través de un mensaje para acceder a un sitio web en el que te tienes que identificar o facilitar información personal

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta