

RECUERDA: KIT DE CONCIENCIACIÓN PHISHING

- Ante la más mínima duda, no facilites información **confidencial**.
- Infórmate periódicamente** sobre las últimas noticias de seguridad, para mantenerte informado.
- Es importante utilizar antivirus para evitar la instalación de códigos maliciosos en tu equipo. **Analiza tu ordenador** ante cualquier sospecha.
- Verifica la información.** Si tienes duda de su procedencia, ponte en contacto por otra vía para verificarla.
- Presta atención a **la redacción, y sospecha si** existen expresiones sin sentido y errores ortográficos o gramaticales.
- Recuerda que este tipo de estafa no solo se centra en la banca online. **Mantente alerta.**
- Utiliza el **sentido común** cuando vayas a hacer alguna transacción por internet, "si es demasiado bueno para ser cierto, es que no es cierto".
- No proporciones tu cuenta bancaria** o número de tarjeta de crédito, DNI, número de teléfono móvil, a menos que estés realmente pagando por algún bien o servicio.
- Si has sido víctima de un intento de phishing **informa** a la empresa suplantada y a las autoridades competentes.



CONTÁCTANOS

-  info@incibe.es
-  Twitter
[@incibe](https://twitter.com/incibe)
[@certs_i](https://twitter.com/certs_i)
[@osiseguridad](https://twitter.com/osiseguridad)
-  YouTube
Intecocert
OSIseguridad
-  Facebook
Osiseguridad
-  LinkedIn
Incibe-sa
-  Google+
Oficina de Seguridad del Internauta
-  Tuenti
Oficina de Seguridad del Internauta



Kit de Concienciación Phishing

INSTITUTO NACIONAL DE
CIBERSEGURIDAD

www.incibe.es



Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016

INSTITUTO NACIONAL DE
CIBERSEGURIDAD

SPANISH NATIONAL
CYBERSECURITY INSTITUTE



EL PHISHING es una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un “tercero de confianza”. Este tipo de ataques se han convertido en una de las amenazas externas que más acechan a las empresas.



LOS RIESGOS derivados de estas técnicas son el robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas. Los métodos utilizados para la realización del **PHISHING** no se limitan exclusivamente al correo electrónico, sino que también utilizan SMS (**SMISHING**), telefonía IP (**VISHING**), **REDES SOCIALES, MENSAJERÍA INSTANTÁNEA A TRAVÉS DEL MÓVIL, ETC.**



Para evitar estos riesgos es recomendable adoptar unas buenas prácticas principalmente en **EL USO DEL CORREO ELECTRÓNICO CORPORATIVO.**



APRENDE a identificar correctamente los correos electrónicos sospechosos de ser phishing, en general mensajes que solicitan información confidencial (contraseñas, datos bancarios, número de teléfono móvil,...).



VERIFICA la fuente de información de tus **CORREOS ENTRANTES.** Tu banco no te va a solicitar tus datos o claves bancarias a través del correo electrónico.



EN LUGAR DE UTILIZAR LOS ENLACES incluidos en los correos electrónicos, escribe la dirección directamente en el navegador.



Mantén **ACTUALIZADO TU EQUIPO** y todas las aplicaciones, sobre todo el antivirus y anti-spam. Aplica los parches de seguridad facilitados por los fabricantes.



Antes de introducir información confidencial en una página web, **ASEGÚRATE QUE ES SEGURA.** Han de empezar con <<https://>> y tener un candado cerrado en el navegador.



El **SMISHING** se realiza a través un mensaje de texto intentando convencerte de que visites un enlace fraudulento.



El **VISHING** se realiza a través de una llamada telefónica que simula proceder de una entidad bancaria solicitándote verificar una serie de datos.

