

AVISO DE SEGURIDAD SOBRE POSIBLES ATAQUES DE “PHISHING”.

Hacienda Foral de Navarra comunica a la ciudadanía la posible existencia de correos electrónicos que intentan suplantar la identidad (*phishing*) de Administraciones Públicas, y más en concreto, de Administraciones Tributarias.

Si bien hasta ahora no consta ningún ataque directo a este Organismo, es necesario advertir de su existencia para evitar cualquier perjuicio y, más si cabe, en el actual contexto en el que ha sido eliminada la atención presencial temporalmente y la comunicación se realiza de forma telefónica o a través del correo electrónico.

El objetivo de este tipo de correos de suplantación es robar datos personales y bancarios. En este sentido cabe recordar que Hacienda Foral de Navarra nunca realiza devoluciones a tarjetas de crédito o débito.

Le aconsejamos que siga los siguientes consejos del Centro Criptológico Nacional para evitar ser víctima del phishing:



Cómo evitar ser víctima del phishing

- Compruebe el dominio del correo remitente y que su nombre coincida con su cuenta de correo electrónico (nombre y dominio).
- Desconfíe de los correos electrónicos cuyo texto esté mal redactado o con faltas de ortografía.
- Evite abrir archivos adjuntos si se desconoce al remitente o no se espera el documento.
- Preste atención a la sintaxis de los enlaces a páginas web que le lleguen por correo electrónico. Una letra puede marcar la diferencia.
- Si accede a páginas web a través de buscadores, antes de introducir datos personales, compruebe siempre que se trata de la página web oficial y no una página secundaria que recaba la información de su interés.
- Si observa alguna anomalía en un correo electrónico, contacte con el remitente a través de otro canal (ej. Teléfono) para comprobar la autenticidad del mensaje.
- Habilite el segundo factor de autenticación en todos los medios digitales que dispongan de él (aplicaciones bancarias, redes sociales, correo electrónico, etc.).
- No introduzca datos personales en páginas web cuyo enlace haya llegado acordado (cort.as, bit.ly, etc.).
- Utilice un navegador para las gestiones bancarias y oficiales, y otro distinto para la navegación habitual.
- Mantenga actualizado el navegador, así como sus extensiones y complementos (Flash, Java, etc.).

Si desea más información sobre la materia, puede consultar los siguientes enlaces del INCIBE (Instituto Nacional de Ciberseguridad) y de la OSI (Oficina de Seguridad del Internauta) o acudir a sus páginas web:

- Enlace INCIBE: [Distribución de malware vinculado a Covid-19 suplantando varias empresas](#)
- Enlace OSI: [Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes](#)
- Página Web INCIBE: <https://www.incibe.es/>
- Página Web OSI: <https://www.osi.es>

