

Píldoras formativas

Declaración Renta

¿Cómo reconocer y defenderse ante los ataques de phishing sobre la renta?

Existen una serie de características en los correos electrónicos y SMS que envían los ciberdelincuentes que hacen que sea fácil reconocerlos como phishing (escritos con faltas de ortografía o con expresiones que no son habituales, así como traducciones literales del inglés.

Se suele hacer **referencia a un reembolso de impuestos inexistente** en el que la persona receptora del e-mail sale beneficiada. Para poder disponer del dinero **hay que acceder a una dirección web o rellenar un formulario** en los que se deben aportar datos de cuentas bancarias o tarjetas de crédito o débito.

El objetivo de los delincuentes es **robar a la víctima datos personales o bancarios**, ya sea remitiéndole a una página web falsa que suplanta a la de la Agencia Tributaria o haciéndole descargar ficheros con virus.



Estafa de la renta a través de pagos por bizum

Una de las últimas estafas de las que muchas personas fueron víctimas en la pasada campaña de la renta tiene que ver con los pagos móviles a través de Bizum. En ella, los cibercriminales se hacen pasar por la Agencia Tributaria informando a la víctima de que su declaración le ha salido a devolver, pidiéndole que acepte el ingreso a través de Bizum. Este trámite no se trata de un pago, sino de una solicitud para reclamar ese dinero.

Ten siempre presente que cualquier trámite de la Agencia Tributaria que implique **un pago se realizará a través de la web de la AEAT y en condiciones de comercio electrónico seguro.**

El término “web de la AEAT” es el sitio web de la Agencia Tributaria y está compuesto por:

Sede electrónica de la AEAT, integrada por los dominios: “sede.agenciatributaria.gob.es” y “*.agenciatributaria.gob.es”.

Otros dominios utilizados por la AEAT: “*.agenciatributaria.es” y “*.aeat.es”.



Cuidado con los perfiles falsos de la agencia tributaria

Otro de los engaños que la Agencia Tributaria ha detectado en las últimas campañas de la renta es el que tiene que ver con perfiles falsos en redes sociales.

El ciberdelincuente crea una cuenta en esta red social haciéndose pasar por Hacienda o la Agencia Tributaria para contactar con las víctimas y solicitarles datos personales, al igual que en otras estafas de Scam.



Para detectar, pon la lupa!!!!

- La AEAT **nunca pide ningún dato confidencial**, ni número de cuenta o tarjeta de crédito por **correo electrónico, llamada o SMS**.
- Hacienda **no hace devoluciones a tarjetas de crédito ni débito**, ni tampoco cobra por ninguno de los servicios que presta, nunca envíes estos datos si te los solicitan en el correo o por mensaje e texto.
- La AEAT utiliza los SMS y los correos electrónicos para informar del estado de tu declaración de la renta o avisarte de que tienes una notificación en la Sede Electrónica, pero **nunca pide que llames a un número de teléfono, ni incluye enlaces ni archivos adjuntos**.
- Debes evitar las apps fraudulentas y descargar las aplicaciones de la Agencia Tributaria desde las tiendas de aplicaciones oficiales. **Nunca instales aplicaciones a través de enlaces por mail o SMS o Redes Sociales**.



iGracias! Thank you!

mastel 
hospitality

mastel 
hospitality
ORACLE Partner

mastel 
hospitality
FREEDOM.PAY

mastel 
hospitality
revo

mastel 
hospitality
CyBERSECURITY



CERTIFICATION AUTHORITY ACCREDITED BY ENAC