



© 18 agosto 2021, 08:25 (CEST)

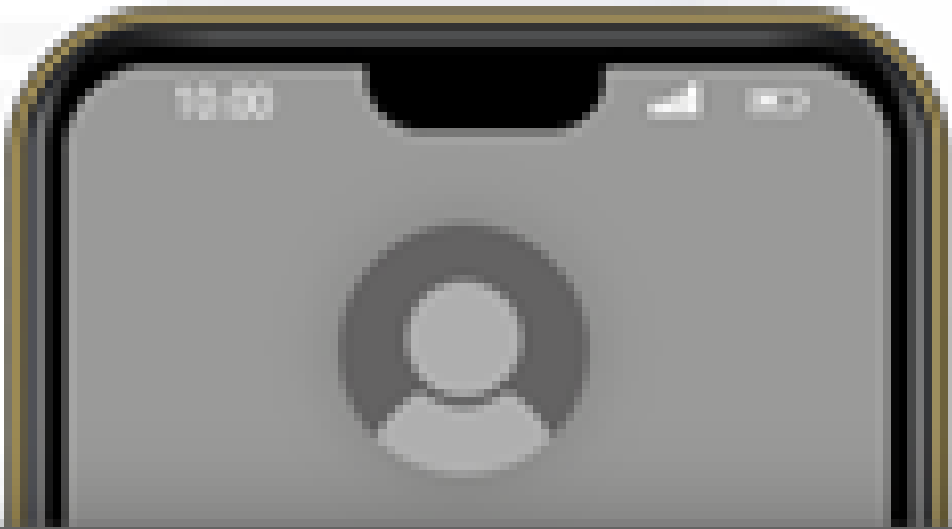
## 5 consejos para evitar ser víctima de los ciberdelincuentes

Durante los últimos días, afiliados a las diferentes AFP han reportado intentos de fraude por parte de ciberdelincuentes, quienes envían mensajes de texto, correos y enlaces de páginas falsas para que las personas ingresen sus datos personales y, de esta forma, puedan robarles sus fondos de pensiones.

Las dos modalidades bajo las cuales actúan estos ciberdelincuentes se llaman *phishing* y *smishing*. El primero consiste básicamente en enviar correos electrónicos con supuestas “páginas oficiales” de las AFP y entidades financieras; sin embargo, son clonadas a fin de no crear sospechas, captar la atención de los afiliados y que éstos puedan registrar sus datos confidenciales. Por otro lado, en la modalidad *smishing* el ciberdelincuente envía mensajes de texto para que el afiliado ingrese a una página web también falsa, en donde les solicitan sus datos personales.

Este sistema de estafa se viene desarrollando en medio del proceso de retiro de hasta 4UIT o S/17,600 de los fondos de pensiones; por ello, Profuturo AFP recomienda tener en cuenta los siguientes consejos para evitar ser víctima de un robo cibernético:

1. En caso reciba un mensaje de texto de parte de su AFP o entidad financiera solicitando información confidencial, no responda y elimine de inmediato el mensaje. Profuturo AFP informa que no solicita datos personales a sus afiliados mediante mensajes de texto. Todas las comunicaciones las realizan a través de sus canales oficiales, los cuales podrás encontrarlos en el siguiente enlace: <https://www.profuturo.com.pe/canales-de-atencion>.

A smartphone is shown with a notification overlay. The notification text is as follows:

Estimado Cliente,  
La solicitud de retiro de sus  
Fondos AFP ha sido  
OBSERVADA, más información  
<https://consultasretiroafp.com>

**FALSO**

2. No brindes información personal a través de una llamada telefónica. Profuturo no realiza llamadas a sus afiliados solicitándoles actualizar sus datos personales o para pedirles información adicional que sea útil para el proceso de retiro de hasta 4UIT. Recuerda que podrás hacer seguimiento a tu solicitud de retiro de pensiones ingresando a la web [www.consultaretiroafp.pe](http://www.consultaretiroafp.pe) que es administrado por la Asociación de AFP, en donde deberás hacer clic al botón ¿Cómo va mi solicitud?

3. Evita realizar transacciones en línea utilizando un wifi público, sobre todo cuando debes ingresar datos bancarios o contraseñas. La mayoría de estas redes públicas son vulnerables a hackers y podrían obtener fácilmente toda tu información registrada. En estos casos, si te encuentras fuera de casa, se recomienda compartir los datos móviles a la laptop; es decir, conectarte desde tu laptop al internet de tu celular para poder realizar de forma segura tus transacciones personales.

4. Para una mayor seguridad, si deseas ver el estado actual de una solicitud de trámite o realizar una nueva solicitud, lo ideal es ingresar de forma directa a la web oficial de Profuturo AFP <http://www.profuturo.com.pe/>, y nunca hacerlo a través de un enlace que fue enviado por correo, mensaje de texto o, incluso, desde el buscador de Google. Asimismo, para realizar el trámite de retiro de hasta 4UIT deberás ingresar al enlace oficial <https://www.consultaretiroafp.pe/>, el cual también podrás encontrarlo en la página oficial de Profuturo o en las notas publicadas por medios de comunicación de confianza que hayan informado al respecto.

5. Si te encuentras en una página web y sospechas de su veracidad, una forma de verificar si es segura o no es identificando errores gramaticales y/o que las direcciones o enlaces te lleven a la página oficial de la empresa. Una vez en la página, comprueba si al dar clic en otros enlaces te derivan a la información indicada. Por ejemplo, si ingresas a la opción “sobre nosotros” en la página web de Profuturo <http://www.profuturo.com.pe/>, este enlace deberá direccionarte hacia dicha información; de lo contrario, podría tratarse de una página clonada por ciberdelincuentes.

PERSONAS | EMPRESAS | SOBRE NOSOTROS | PREGUNTAS FRECUENTES

Buscar 



¡REALIZA EL RETIRO DE  
HASTA S/17,500 DE TU FONDO!  
Retiro de hasta 4 UIT

RECUERDA QUE NO NECESITAS UN  
CRONOGRAMA DE REGISTRO

HAZLO AQUÍ >





Ingresar a tu  
**Zona Privada**

Ingresar

▶ Genera tu Clave Web

Recuerda, si sospechas haber sido víctima de fraude por *phishing* o *smishing*, por cuestiones de seguridad bloquea de inmediato tus tarjetas bancarias y comunícate de inmediato con tu entidad financiera. Cabe señalar que solo entre enero y abril del presente año, la División de Investigación de delitos de Alta Complejidad (Diviac) de la Policía Nacional del Perú recibió 1,188 denuncias por delitos cibernéticos y 600 casos fueron sobre fraudes informáticos.



## Descarga

los adjuntos de la Nota de Prensa





**Astrid Balarín**

Consultora de Proyectos, APOYO Comunicación S.A.

[abalarin@apoyocomunicacion.com](mailto:abalarin@apoyocomunicacion.com)

981346535



---

#### ACERCA DE APOYO COMUNICACIÓN

Somos una consultora de **comunicación**, que busca ser aliada de sus clientes, ofreciendo servicios integrados a través de cuatro grandes disciplinas: **comunicación externa, comunicación interna, insights y transformación digital**, para contribuir con los objetivos de comunicación y reputación de nuestros clientes y que éstos a su vez se vean reflejados en los resultados de negocio.

---

 pr.co



APOYO Comunicación