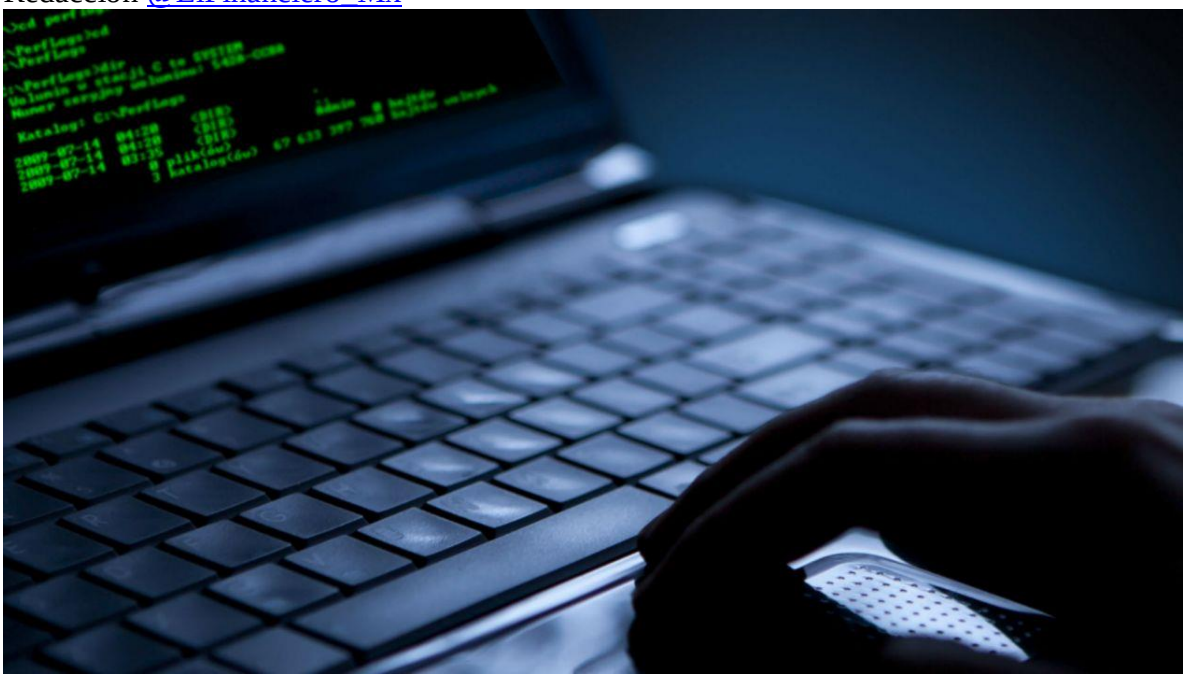
¡Cuidado! No caigas en este correo apócrifo que detectó la Consar

La Consar alertó que diversos usuarios han reportado un correo electrónico que pretende engañarlos al pedirles confirmar un supuesto cambio de Afore.

Redacción @ElFinanciero_Mx



Si en estos días recibes un correo de la **Comisión Nacional del Sistema de Ahorro para el Retiro** (Consar) ten mucha precaución, ya que puede tratarse de un posible esquema de robo de datos, aunque las autoridades aún no han determinado su fin.

A través de un mensaje en su sitio web, la Consar alertó que diversos usuarios han reportado un correo electrónico que pretende engañarlos al pedirles confirmar un supuesto cambio de Administradora de Fondos para el Retiro (Afore) autorizado por el propio trabajador. El *e-mail* incluye una liga para abrir un documento y encontrar detalles de la operación.

“El cambio de institución Afore para administrar su fondo de retiro ha sido ejecutado de manera correcta, recuerde que este cambio debe haber sido realizado y autorizado por usted, en el siguiente documento se encuentran los detalles de la operación”, se lee en el correo.

Enseguida se ve en letras azules y subrayadas la frase “Ver Documento”, en donde los usuarios deben dar click para corroborar la presunta operación.

El correo electrónico exhibe en la parte superior los logotipos de la Consar y la Secretaría de la Función Pública (SFP), dependencia que no tiene ninguna injerencia ni autoridad sobre el tema de los ahorros de los trabajadores.

Algunos bancos que administran recursos de Afores, como Citibanamex, han reenviado en correos electrónicos la alerta de la Consar a sus clientes para que no caigan en el engaño.

En el pasado, la Consar había detectado correos electrónicos apócrifos que pretendían obtener datos personales de las personales, como direcciones, sitios de trabajo y cuentas bancarias y de seguridad social.

Otras instituciones de gobierno que en meses recientes han alertado de la emisión de correos electrónicos falsos han sido la Secretaría de Hacienda y Crédito Público (SHCP) y el Servicio de Administración Tributaria (SAT), que incluso mantiene un registro de más de 100 direcciones de correo de las que han sido emitidos los mensajes de engaño.