# ¡Cuidado con las estafas financieras digitales!


SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

## *CUIDADO CON LAS ESTAFAS FINANCIERAS DIGITALES*

*Es parte de una serie de cartillas elaboradas por la Superintendencia de Banca, Seguros y AFP y tiene como finalidad contribuir al desarrollo de capacidades financieras en jóvenes y adultos. En esta cartilla aprenderás sobre las diferentes modalidades de fraudes financieros que existen, cuándo y cómo nos pueden robar la identidad y cómo evitarlo.*

**Cuidado con las estafas financieras digitales**
"Esta es una obra colectiva"
Editado por:
Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones
Los Laureles 214 San Isidro - Lima
1ª. Edición Diciembre 2022
Depósito Legal N° 2022 - 12980

**En la actualidad, gracias a la tecnología podemos realizar compras y pagos**, abrir cuentas en una entidad financiera, realizar transferencias o hasta pedir delivery a través de un app utilizando tu tarjeta.

*La tecnología simplifica la vida, pudiendo realizar transacciones financieras ahorrando de esta manera tiempo y dinero.*

Sin embargo, el auge de la era digital; ha provocado que los llamados **"hackers"** usen sus conocimientos de informática con intenciones maliciosas para realizar el robo de identidad y los fraudes financieros a través de canales digitales. Por eso debemos tener **CUIDADO.**

---

**El robo de identidad o suplantación de identidad es un delito que consiste en que una persona se haga pasar por ti,** valiéndose de tu información personal y financiera para obtener beneficios de manera fraudulenta o para cometer otros delitos. Cuando esto sucede, no solo pierdes dinero, también se daña tu reputación financiera.

---

Tu identidad se compone de todos tus datos personales como tu: **nombre, teléfono, domicilio, huellas dactilares, imagen, información financiera, etc.**

# ¡CUIDADO! El robo de identidad puede ocurrir en cualquier momento si no somos precavidos.

A continuación, conoceremos algunos ejemplos de operaciones que podría realizar un delincuente si suplanta nuestra identidad:

**Realizar transferencias:** Tan solo iniciando sesión en tu cuenta, podría realizar trasferencias hacia sus cuentas personales o a las de terceros.

**Comprar por internet** usando la información de tu tarjeta (número, nombre, fecha de vencimiento y código de seguridad, entre otros).

**Abrir cuentas:** Con la identidad robada, pueden crear cuentas para "lavar" dinero, recibir dinero robado o de otras actividades a tu nombre.

**Solicitar créditos a tu nombre:** Tan solo ingresando a la página web o app de tu entidad financiera, podrían solicitar un préstamo a tu nombre.

**Crear perfiles falsos:** Pueden crearte un perfil falso en redes sociales para relacionarse con tus contactos y solicitarles depósitos de dinero.

**Al obtener tu información personal,** pueden suplantarte y reponer el chip asociado a tu número de celular para ingresar a tu cuentas vía web o por aplicativos.

Como verás, los ciberdelincuentes pueden perjudicarte de distintas maneras lanzando "anzuelos" para obtener tu información. Nuestra intención no es que te estreses o que sufras de insomnio pensando que tu dinero o tus datos no están a salvo; queremos prevenirte para que protejas tu identidad y tu dinero.

*En la mayoría de los casos, la información que roban es para contratar productos y servicios financieros a nombre de la víctima, pudiendo hasta dañar tu calificación crediticia en las centrales de riesgo.*

# ¿Cómo pueden obtener tu información para cometer fraudes?

**A continuación te presentamos las formas más comunes utilizadas por estos delincuentes para robar tu información y qué puedes hacer para evitarlas.**

| MODALIDAD | EJEMPLO | ¿CÓMO EVITARLO? |
|---|---|---|
| **PHISHING**<br>Es un delito cibernético en el que delincuentes simulan comunicaciones de empresas para obtener nuestra información como datos personales o financieros. | Te llega un mensaje falso como este:<br>"Hemos detectado una actividad sospechosa en su cuenta, ingrese aquí" | No ingresar al link de preferencia llamar a la entidad financiera para verificar este mensaje. No brindar tu información personal. |
| **SMISHING**<br>El atacante utiliza mensajes de texto (SMS) para tratar de que la víctima le revele sus datos o para instalar un software malicioso en su celular sin que se dé cuenta. | Te llega un mensaje de texto de tu entidad financiera al celular diciendo:<br>"Estimado cliente su cuenta ha sido deshabilitada: Reactívala ingresando tu celular aquí: (pondrán un link falso) | No ingresar al link. No ejecutar ningún archivo adjunto o enlace si desconocemos el remitente. |
| **VISHING**<br>Mediante el uso de llamadas telefónicas engañan a las personas para obtener información delicada. | Mediante una llamada y grabación te alertan de un fraude; luego te dan un número al que debes llamar y cuando llamas te responde otra grabación pidiendo que ingreses los datos de tu tarjeta a través del uso del teclado. | Es mejor colgar. Ante la duda, contacta a tu entidad financiera a través de los canales oficiales de atención. |
| **PHARMING**<br>Te llega un correo electrónico, que al momento de abrirlo instala un código en tu equipo, este hará que cuando ingreses a la web de tu entidad financiera te dirija a páginas web falsas. | Abres un correo electrónico que es parecido al portal web de tu entidad financiera pero es falsa. | Escribir directamente la dirección de la página web de la entidad financiera. Comprobar la URL (dirección electrónica) de los sitios que ingresas y que tengan el protocolo https y el candado en la barra de direcciones. Asimismo, es recomendable instalar un antivirus. |

# Otros consejos importantes a considerar

**USA** contraseñas seguras, es decir que sean difíciles de adivinar, monitorea tus cuentas y cambia tus claves o contraseñas con frecuencia.

**CONTROLA** tus movimientos bancarios y de ser posible, guarda por un tiempo prudente los comprobantes de tus consumos para poder reclamar en caso corresponda.

**DESCONFÍA** de avisos o llamadas que te generen dudas. Ante la duda contacta a tu entidad financiera a través de los canales oficiales de atención.

**MANTÉN ACTIVO** el servicio de notificaciones inmediatas, a fin de que tu entidad financiera te alerte cada vez que realizas una transacción.

**BLOQUEA** tu celular en caso de robo o pérdida.

**CIERRA** la sesión cada vez que dejes de usar tu correo electrónico o redes sociales y no publiques información personal.

**DESHABILITA** la opción de realizar operaciones con tus tarjetas por internet como realizar compras, en caso no las necesites. Recuerda que puedes deshabilitar o habilitar dicho servicio en el momento que desees, en los canales puestos a disposición por tu entidad financiera.

**SI ERES VÍCTIMA DE FRAUDE...**

✔ **Reporta el robo de tu celular,** en especial si tienes instalados aplicativos de tus entidades financieras.

✔ **Informa a tu entidad financiera** de manera inmediata en caso de que hayas perdido tu tarjeta o si no reconoces algún consumo realizado.

"Algunas entidades suelen solicitar información por teléfono para validar tu identidad al momento de realizar operaciones por dicho canal, utilizando mecanismos para no exponer la información. Cuando una entidad se comunique contigo, NUNCA te pedirá que le brindes tus contraseñas, números de tarjetas o datos personales de tus cuentas".

## PARA MAYOR INFORMACIÓN

**puedes contactar a la**
**Superintendencia de Banca, Seguros y AFP.**

## LLAMADA GRATUITA A NIVEL NACIONAL 0800-10840

**DESDE UN TELÉFONO FIJO O**
**VÍA INTERNET EN**
**www.sbs.gob.pe/contacto**

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

**Este material fue desarrollado por la Superintendencia de Banca, Seguros y AFP. Programa de Educación Financiera.**

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

*Si quieres más información sobre*
*educación financiera entra a nuestra página*

www.sbs.gob.pe/educacionfinanciera

*Donde encontrarás otros materiales educativos*
*sobre los temas presentados en esta cartilla.*

Accede a través
de este código al
**Portal de Educación**
**Financiera de la SBS**