CONSEJOS FUNDAMENTALES DE

SEGURIDAD

BANCO ATLAS

BUENAS PRÁCTICAS
DE SEGURIDAD

La prevención de fraude debe formar parte integral de tu vida diaria. Te acercamos métodos para proteger tu dinero y tus medios de pago.

1 Los productos bancarios son de uso personal. Te recomendamos que lo **utilice únicamente el titular**, no debe prestarse a terceras personas, ya que será responsabilidad del titular las transacciones realizadas con los mismos.

No compartas con terceras personas los códigos de acceso a los servicios Atlas Online. **2**

3 En todo momento se debe **proteger la información personal**, como también los datos de cuentas y tarjetas ya que las mismas contienen información que deben ser manejados únicamente por el titular.

Las tarjetas de crédito y débito deben contener la **firma en el dorso** y te recomendamos la **destrucción de los plásticos vencidos.** **4**

5 El **control de los extractos** de tarjetas de crédito y cuentas deben ser **realizados periódicamente** y en caso de **transacciones sospechosas dar aviso al banco** inmediatamente.

Si el titular modifica su domicilio laboral o particular, debe informarlo al banco de manera a evitar el envío de extractos o tarjetas donde ya no corresponde. **La información actualizada es vital.** **6**

CONSEJOS DE SEGURIDAD
PARA INTERNET, TELÉFONO Y CORREO

No facilites el número de tarjeta, fecha de expiración, código de seguridad, PIN de Internet u otro dato bajo ninguna circunstancia y por ningún medio, aunque la llamada provenga del banco, empresas de ventas de paquetes, de loterías, caridad y otros servicios de telemarketing.

Banco Atlas no solicita, a través de ningún medio electrónico, **acceso a datos personales** o de los productos y/o servicios bancarios.

En caso de recibir emalis con links adjuntos, te recordamos que **no es difícil crear un sitio web fraudulento o falsear una cuenta de correo electrónico.**

TIPOS DE FRAUDES
PRACTICADOS EN INTERNET

El pishing, suplantación de identidad; es un tipo de fraude por email en el cual se intenta **engañar a los clientes** a través de páginas webs simuladas e ilegítimas con el objetivo de **capturar datos personales y/o financieros**, tales como números de cuenta , números de tarjetas de crédito o débito, claves o PIN de acceso, entre otros. Estas webs pueden aparecer como ventanas emergentes o links en emails de direcciones; pareciendo ser auténticas e inclusive pueden incluir un vínculo falso a supuesto sitio web legítimo que también resulta ser falso.

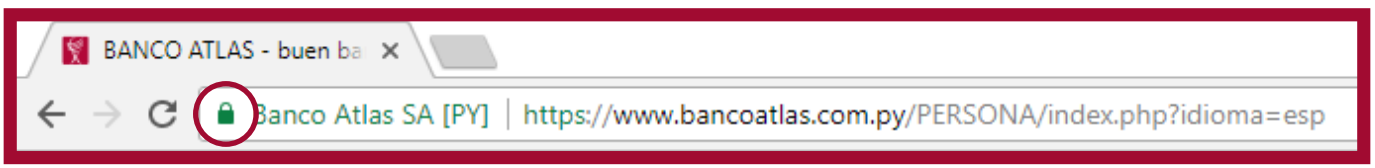
MEDIDAS PREVENTIVAS
CONTRA EL PISHING

1 No respondas y **desconfiá de cualquier solicitud** de información personal financiera.

Verificá la legitimidad del email directamente con la empresa. **2**

3 Para visitar sitios web, introducí la dirección URL en la barra de direcciones y **no hagas clic en un enlace dentro del email**. Ejemplo: Si deseas ingresar a la web de Banco Atlas escribí directamente www.bancoatlas.com.py

Para verificar que el sitio web al cual accedés es seguro, en el explorador que uses, **el icono de candado cerrado** en la barra de estado del navegador te indica que el sitio tiene mecanismo de seguridad de información.



El Pishing Laboral consiste en la captación de información de clientes por medio de emails, anuncios en webs de búsqueda de trabajos, chats y otros. **Empresas ilegítimas te ofrecen trabajar cómodamente desde tu casa y cobrando beneficios muy altos.** Sin saberlo, la víctima es utilizada para blanquear dinero obtenido por medio del Pishing. Generalmente solicitan que tengas o habilites una cuenta bancaria en la cual recibirás transferencias bancarias para que te encargues de debitar dinero y enviarlo a otros países.

MEDIDAS PREVENTIVAS
CONTRA EL PISHING LABORAL

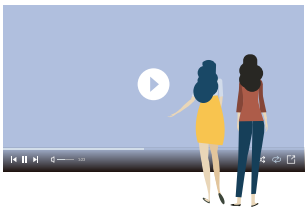
1 **No aceptes ninguna oferta de trabajo recibida por email.** El defraudor podría llegar a mandarte un contrato (falso) para hacer más creíble la oferta y una vez que este obtenga los datos de la víctima y esta no colabora, es amenazada.

2 **No proporciones tus datos personales ni financieros** y desconfiá de todas las propuestas laborales recibidas por email. Estas son algunas de las preguntas más frecuentes: ¿Estas desempleado y con ganas de trabajar?, ¿Querés obtener dinero extra?, ¿Querés trabajar cómodamente en tus horarios desde tu casa?, ¿Querés tener buenos beneficios y de forma rápida?.

Los sorteos falsos son un tipo de fraude en el cual recibis un email que notifica que **has ganado un premio de una lotería o sorteo el cual es falso**, si un usuario contesta ese correo le solicitará a continuación datos bancarios para un falso ingreso de premio y realizará fraudes con la información que fue provista.

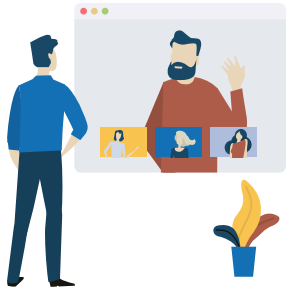
Sitios web falsos: Los fraudes vía email están frecuentemente relacionados con el uso de sitios webs falsos; personas malintencionadas crean una página web o sitio web que es similar al de la compañía legítima y **usan una dirección URL similar a la de la empresa acreditada.**

MEDIDAS PREVENTIVAS
CONTRA SITIOS WEB FALSOS



Podés identificar si la dirección del sitio web o página web falsa usa un **error tipográfico común del nombre de la compañía** o agrega una palabra, símbolo o número antes o después del nombre. La presencia de un símbolo de **arroba "@"** en alguna parte de la URL de la página normalmente indica que se trata de un sitio web fraudalento.

Robo de identidad: Este robo implica **obtener información de la identidad de una persona sin su consentimiento**, con el propósito de hacerse pasar por el titular y cometer fraude. Los ladrones podrán abrir cuentas bancarias y girar cheques, solicitar tarjetas de crédito, o modificar la dirección para recibir la renovación de su tarjeta, obtener préstamos personales, obtener incluso empleo y comprar inmuebles.



MEDIDAS PREVENTIVAS
CONTRA EL ROBO DE INDENTIDAD

1 Mantené tu **documentación personal** y tus comprobantes bancarios de tarjetas en un **lugar seguro.**

Si vas a tirar algún documento que contenga información personal o financiera, **trituralo antes de hacerlo.** **2**

3 Informá al banco cada vez que cambias de domicilio, o teléfono. **Actualizar los datos es vital.**

Revisá y conciliá mensualmente tus extractos de cuenta y **vigilá tu información** crediticia y calificación comercial. **1**

BANCO ATLAS

www.bancoatlas.com.py | Quesada esq. Tte Zotti - Edificio Atlas Center