



Montevideo, Diciembre de 2012

Estimado cliente,

El crecimiento del correo electrónico nos ofrece mayores oportunidades de comunicación e interacción, pero esto también trae consigo nuevos riesgos contra los cuales debemos protegernos.

En esta comunicación le sugerimos algunos controles a realizar en las instrucciones recibidas vía correo electrónico, a efectos de prevenir eventos de suplantación de identidad.

Una suplantación de identidad es un mensaje de correo electrónico que trata de engañar a la persona que lo recibe para que proporcione información valiosa personal/institucional/comercial, a efectos de utilizar la misma para realizar entre otras, transferencias bancarias hacia cuentas no deseadas, divulgación de información confidencial, etc.

Estas instrucciones parecerán provenir de casillas de correo de vuestros proveedores o socios comerciales instruyendo realizar pagos a cuentas específicamente abiertas en el exterior para efectuar este tipo de acciones fraudulentas.

Por lo tanto, le sugerimos, que en el caso de recibir instrucciones vía correo electrónico, verifique previamente la autenticidad de las mismas antes de instruir la realización del pago o transferencia solicitada.

Le sugerimos algunos controles a realizar:

- Ratifique la instrucción recibida **por otro canal** (por ejemplo telefónicamente). **Nunca** utilice para verificar la misma datos o links incluidos en el mensaje en cuestión.
- En el caso haber realizado pagos similares a ese proveedor/socio comercial, **verifique** que los datos correspondientes al destino de los fondos (Banco, Cuenta, Titulares, etc.) **concurden con instrucciones ya procesadas**.
- No ingresar en links adjuntos a mails, a menos que conozca que son genuinos
- Extremar estos controles si las transferencias tienen como destino países de Asia y/o Medio Oriente.

Frente a cualquier duda o consulta al respecto, por favor, diríjase a su oficial de cuenta que con gusto lo asesorará al respecto.

Atentamente,

HSBC Bank Uruguay S.A.