**Directrices para protegerse contra el fraude de suplantación de identidad**

- De conformidad con las Políticas de finanzas y control del Grupo Sidel, la empresa opera un sistema de doble autorización, incluso para cualquier cambio de instrucción de pagos. Cualquier cambio de este tipo debe ser aprobado de antemano, por escrito, por dos personas autorizadas por una entidad legal de Sidel. Dichos cambios de instrucción de pagos son muy poco comunes. Sidel casi nunca pide que se cambie el pago de un banco a otro, especialmente a un tercer país.
- Para todas las solicitudes de pago, Sidel siempre adjunta una factura. Por lo tanto, sospeche de inmediato de cualquier solicitud de este tipo que no contenga una factura correcta.
- Para todos los recordatorios o solicitudes de seguimiento relativos a los pagos, se incluye sistemáticamente una referencia de la solicitud y la factura originales. Por lo tanto, sospeche de inmediato de cualquier solicitud que no contenga una referencia que coincida con la solicitud y la factura iniciales.
- En caso de cualquier cambio en sus solicitudes de pago e instrucción de pago normales de las entidades o agentes legales de Sidel, aunque pueda parecer que Sidel sea el remitente, le recomendamos que siempre confirme verbalmente las instrucciones mediante una llamada telefónica a su contacto Sidel de confianza utilizando su número de contacto habitual con Sidel. **No** utilice los datos de contacto proporcionados por el remitente que aparecen en las solicitudes de pago y en los cambios de instrucción de pagos. En su lugar, llame su contacto Sidel de confianza utilizando su número de contacto habitual con Sidel. Esto es especialmente importante si recibe una solicitud para transferir fondos o suministrar información comercial confidencial a partir de una dirección de correo electrónico que parezca diferente al formato nombre.apellido@sidel.com.
- Sidel solo se comunica desde una dirección de correo electrónico sidel.com, como nombre.apellido@sidel.com. Sidel no utiliza ninguna otra dirección de correo electrónico que finalice, por ejemplo, en sidel.net, side1.com, sidei.com, etc.
- No abra ni responda a correos electrónicos basura (*spam*) de terceras partes externas.
- No responda a llamadas o mensajes de correo electrónico que soliciten información personal o comercial confidencial. Siempre verifique la fuente (anotando los datos de la solicitud inicial y, después, devolviendo la llamada telefónica a la persona mencionada en un número de contacto comprobado).
- Cuando envíe información comercial confidencial por correo electrónico, considere codificar el mensaje.
- Cuando acceda a sitios web utilizando motores de búsqueda populares, recuerde comprobar la URL que el motor de búsqueda suele mostrar para asegurarse de que el sitio que esté contactando sea legítimo.
- Siempre verifique la identidad de cualquier persona con la que se comunique mediante una comunicación electrónica (como el correo electrónico), así como la finalidad de su solicitud, si tiene alguna sospecha.

- Sospeche siempre de los mensajes de correo electrónico externos que contengan enlaces para acceder a sitios web, independientemente de lo legítimo que parezca el mensaje de correo electrónico.
- Nunca haga clic en un hipervínculo (como un enlace a una página de Internet) de un correo electrónico si sospecha del mensaje o el remitente. Si un correo electrónico lo dirige a un sitio web de Sidel, no olvide comprobar que la dirección del sitio web sea una dirección sidel.com válida.
- Los principales sitios web utilizados por Sidel para las comunicaciones externas son www.sidel.com, www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr y www.sidel.ru. Si en un correo electrónico le piden que ingrese a otro sitio Sidel, no acceda al enlace y, en su lugar, compruebe primero que sea correcto mediante una llamada telefónica a su contacto Sidel correspondiente.
- Actualice siempre las computadoras con los últimos parches de seguridad. A menudo, los proveedores de los sistemas operativos (como Windows) ofrecen mejoras de seguridad para perfeccionarlos. Por ejemplo, Windows permite que los usuarios instalen automáticamente parches de seguridad a través de http://windowsupdate.microsoft.com.
- Los navegadores de Internet (tales como Internet Explorer, Mozilla Firefox, Google Chrome y Safari [Apple], entre otros) ahora ofrecen protección contra los sitios web fraudulentos y cuentan con funcionalidades contra el *phishing* (suplantación de identidad) en sus menús. Asimismo, conviene actualizar regularmente los navegadores en su computadora con la última versión.
- Todo el software de las computadoras debería actualizarse con regularidad. Los proveedores a menudo envían mensajes emergentes para proponer actualizaciones de su software.
- Considere instalar un software antivirus y contra el software espía (*spyware*), muchas veces disponibles en el mismo producto, y asegúrese de que esté actualizado. También es conveniente actualizar dicho software con regularidad.
- La mayoría de los software antivirus cuentan con una base de datos de virus, que puede actualizarse hasta varias veces al día. El software antivirus puede configurarse para que instale automáticamente dichas actualizaciones de bases de datos para garantizar la máxima protección. Para comprobar cualquier posible infección, es conveniente que examine su computadora después de instalar o actualizar el antivirus.
- Considere activar un cortafuegos (*firewall*) personal. Así podrá proteger la computadora contra intrusiones y controlar el tráfico entrante y saliente.
- Proteja el correo electrónico. El software del correo electrónico debería estar equipado con filtros anti-*spam*. El acceso al correo electrónico debería estar protegido con inicio de sesión y una contraseña segura.
- Si sospecha que su dirección de correo electrónico ha sido pirateada, considere utilizar una nueva dirección de correo electrónico y comuníquelo adecuadamente a todos los contactos comerciales.

Por último, recuerde comprobar siempre dos veces cualquier solicitud de cambio de fondos o datos bancarios y verificar la identidad del remitente autorizado. Confirme la solicitud

llamando al número del remitente a través de sus datos de contacto normales (es decir, no utilice los datos de contacto suministrados en el correo electrónico).

Para más información, incluido el asesoramiento y las directrices, consulte los sitios web de soporte internacional http://www.stopthinkconnect.org/ y http://www.antiphishing.org/.