Condiciones generales relativas a la comunicación por correo electrónico

Las presentes condiciones generales se aplican a toda comunicación por correo electrónico y forman parte integrante del Acuerdo relativo a la comunicación por correo electrónico celebrado entre el titular o titulares die la cuenta, el cliente o clientes y las partes contratantes (en adelante denominado conjuntamente como el “Cliente”) y Rothschild & Co Bank AG (el “Banco”).

El Cliente y los destinatarios/remitentes aceptan por medio del presente documento la información y las condiciones que se recogen a continuación en comunicarse con el Banco por correo electrónico. El Cliente y los destinatarios/remitentes conocen las amenazas existentes en el entorno actual de comunicaciones a nivel global y saben, por tanto, que es fundamental gestionar de forma segura los datos relativos a cualquier actividad bancaria.

Riesgos

El Cliente y los destinatarios/remitentes están conscientes que las solicitudes, notificaciones o comunicaciones enviadas por correo electrónico pasan por una red abierta, de acceso público y, en ocasiones, transfronteriza, y, si no están encriptadas, pueden ser vistas por terceros, lo que permite deducir a dichas terceros la existencia de una relación bancaria con el Banco. El Cliente y los destinatarios/remitentes están conscientes también que el contenido electrónico y el lenguaje de una solicitud, notificación o comunicación enviada por correo electrónico no cifrado puede ser modificados y manipulados por terceros.

Si la comunicación entre el Banco y el destinatario/remitente está encriptada, el contenido de la comunicación con las direcciones de correo electrónico o el nombre de dominio facilitados quedará protegido. El Cliente y los destinatarios/remitentes toman nota de que sólo estará protegido el contenido, pero no la dirección e-mail del Banco ni las direcciones de correo electrónico o nombre de dominio facilitados, al no ser estas anónimas, siendo por tanto ostensible el hecho en sí de una comunicación con el Banco.

En este sentido, el Cliente y los destinatarios/remitentes liberan expresamente al Banco del secreto bancario y de la protección de datos.

Además, es posible que personas no autorizadas tengan acceso no autorizado a los equipos informáticos (un ordenador personal, por ejemplo) del Cliente o de los destinatarios/remitentes durante la sesión de internet. El Cliente y los destinatarios/remitentes saben y reconocen que tal riesgo puede aumentar al indicar solo, o también, un nombre de dominio. Es por tanto responsabilidad de cada usuario tomar las precauciones técnicas adecuadas para minimizar los riesgos inherentes al uso de Internet y asegurarse de que el sistema informático está equipado con las salvaguardas más recientes frente a programas maliciosos (como virus, gusanos y troyanos) o piratas informáticos (por ejemplo, mediante el uso de un cortafuegos).

El Cliente y los destinatarios/remitentes saben que la transmisión de una solicitud, notificación o comunicación se puede retrasar, interrumpir o totalmente impedida debido a errores de transmisión, defectos técnicos, caídas, averías, intervenciones ilegales, sobrecarga de red o bloqueo intencionado del acceso electrónico por parte de terceros u otros fallos atribuidos a los operadores de la red. Además, también se pueden producir retrasos relacionados con el tiempo que le lleva al Banco procesar un correo electrónico.

Robo de identidad

El robo de identidad es uno de los delitos que más rápido han crecido dentro de la industria financiera y afecta cada año a millones de personas. Consiste en robar la identidad o los datos personales de alguien, como el nombre, la fecha de nacimiento, la dirección, el correo electrónico, etc., y utilizarlos luego para el beneficio financiero de los estafadores. Por ejemplo, los autores del robo pueden utilizar los datos de identidad para ejecutar pagos o hacer transferencias de dinero; o bien utilizar los datos de la tarjeta de crédito para hacer compras a expensas de la víctima del robo de identidad. Una forma habitual para los estafadores de obtener identidades es vulnerar la cuenta de correo electrónico de un individuo y obtener acceso a la correspondencia electrónica, con el fin de identificar las relaciones del individuo e intentar explotarlas.

Correos electrónicos fraudulentos

Los estafadores suelen utilizar los mensajes electrónicos como vía para recabar información personal. En estos mensajes se le puede pedir al destinatario que actualice o verifique su información personal y financiera, incluida la fecha de nacimiento, los datos de acceso, los detalles de la cuenta, los números de la tarjeta de crédito, etc. Tales mensajes afirman provenir de un organismo legítimo, como puede serlo un banco o algún establecimiento en línea. El correo electrónico en cuestión contiene un enlace que le dirige a una web falsa, pero que, sin embargo, parece calcada o muy similar al verdadero sitio web del establecimiento. El estafador puede así hacerse con datos personales como las contraseñas, al introducirlas, o bien pueden descargar programas maliciosos en su ordenador.

Si un Cliente o los destinatarios/remitentes reciben un correo electrónico con una solicitud bancaria específica y sospechan que no sea realmente el Banco quien lo envía, deberán ponerse en contacto por teléfono con su asesor para asegurarse. Si el Cliente y los destinatarios/remitentes sospechan de una posible vulneración de la cuenta de correo desde la que vienen comunicándose con el Banco, el Cliente y los destinatarios/remitentes deberán informar de inmediato al Banco.

Protección

Para reducir el riesgo de que su cuenta de correo se vea expuesta, así como para evitar ser víctima de un robo de identidad, se ruega al Cliente y a los destinatarios/remitentes que observen las siguientes medidas de seguridad:

- Estar alerta en Internet y tener bien en cuenta a quién y dónde se revelan datos personales.
- No enviar contraseñas por correo electrónico ni compartirlas con terceros. El Banco no solicitará nunca una contraseña.
- No contestar a correos no solicitados o no deseados; no facilitar cuentas bancarias ni datos personales cuando se lo soliciten si no está seguro del destinatario. El Banco se comunica con los Clientes o los destinatarios/remitentes únicamente a través del respectivo asesor de clientes.
- No pinchar en enlaces sospechosos dentro de un mensaje electrónico. Si pincha un enlace de este tipo se podrían descargar programas maliciosos o virus en el ordenador, lo que puede conllevar que un estafador acceda a información personal.
- Utilizar contraseñas complejas con el fin de proteger las cuentas de correo electrónico. Una contraseña segura debe constar de al menos ocho caracteres e incluir mayúsculas, números y caracteres especiales como / $ _ # - + etc. Se recomienda, además, utilizar contraseñas diferentes para las distintas aplicaciones y cuentas.
- Utilizar programas antivirus en el ordenador personal y mantenerlos actualizados con las nuevas versiones.
- Revisar y cotejar periódicamente los saldos para asegurarse de que todas las transacciones son legítimas. Revisar del mismo modo los extractos de cuenta para comprobar que no haya transferencias no autorizadas.
- Utiliser un anti-virus sur l'ordinateur personnel, et le mettre à jour en chargeant les nouvelles versions.
- Vérifier et rapprocher régulièrement les relevés de compte afin de s'assurer que toutes les transactions sont bien légitimes. De même, toujours vérifier les relevés de compte afin de contrôler s'il y a eu des transferts non autorisés.

La solución del Banco para una comunicación segura

El Banco ofrece *Secure Email*, un entorno seguro para comunicar con el Banco por correo electrónico. *Secure Email* proporciona las siguientes ventajas al Cliente:

- La comunicación electrónica con Rothschild se mantiene separada del resto del correo personal y el acceso al correo requiere, además, un nombre de usuario y una contraseña adicional. De esta forma, si un estafador accediera a su cuenta personal, no tendría conocimiento de sus correos ni de la información intercambiados con Rothschild.
- Los correos del Cliente o de cualquier destinatario/remitente se almacenan exclusivamente en los sistemas del Banco, sin salir nunca de las instalaciones del Banco.
- Los sistemas del Banco son seguros y están sujetos a revisiones periódicas de seguridad por parte de empresas especializadas en ciberseguridad.
- *Secure Email* es fácil de usar y puede utilizarse en la mayoría de los dispositivos.