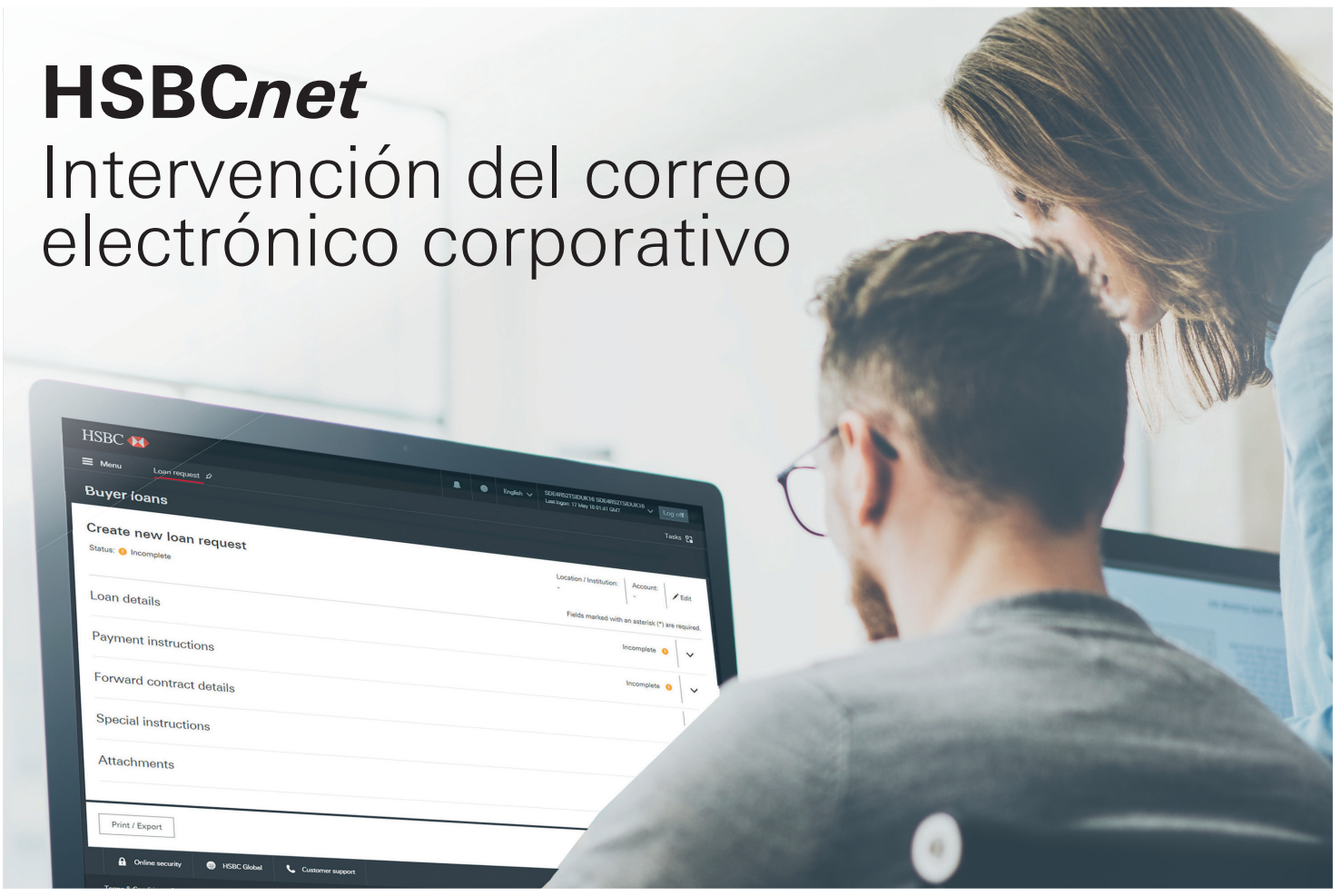
HSBC

Juntos prosperamos

HSBC*net*
Intervención del correo electrónico corporativo



Riesgos para sus negocios: **Pérdidas financieras importantes** | **Daño reputacional**

Los ataques cibernéticos han aumentado constantemente durante los últimos años. Los delincuentes idean nuevas formas de robar información y dinero todo el tiempo, y una de las amenazas más recientes es la intervención del correo electrónico corporativo también conocido como:

- **Fraude del CEO**
- **Fraude del presidente**
- **Redirección de pago**
- **Correo electrónico impostor**
- **Whaling**

Cómo funciona la intervención del correo electrónico corporativo

Un estafador envía un correo electrónico al equipo de pagos de una empresa, en el que se hace pasar por un contratista, proveedor, acreedor o incluso un miembro de la Alta Dirección. El correo electrónico puede parecer ser del CEO, quien pide que se realice un pago urgente, o de un proveedor que solicita que los futuros pagos vayan a una nueva cuenta. A menudo le da instrucciones al destinatario de no conversar sobre el mensaje con nadie.

Ya que el correo electrónico del remitente coincide casi a la perfección con una dirección de correo conocida, este tipo de fraude suele pasar inadvertido hasta que es demasiado tarde. Los criminales cibernéticos pueden incluso acceder ilegalmente a una cuenta de correo electrónico real, lo que dificultará aún más identificar una comunicación fraudulenta.

Su información es muy valiosa

La estafa puede parecer aún más convincente si los ladrones obtienen información acerca de los líderes de una empresa y del equipo de finanzas, por ejemplo, desde del sitio web de la empresa. Las publicaciones en medios sociales también pueden informarles cuando el personal de alto nivel esté fuera de la oficina en reuniones o conferencias. Los estafadores ven esas ocasiones como una oportunidad para enviar correos electrónicos, ya que es difícil que el destinatario verifique si la solicitud es auténtica.

La intervención del correo electrónico corporativo en el mundo real

Caso real de un negocio: Una pérdida de USD 400,000

El equipo de pagos de una empresa recibió un correo electrónico que decía ser el CEO, en el que se pedía que se configuraran los pagos para nuevos beneficiarios. Un miembro del equipo creó y autorizó los pagos. Para cuando el equipo se dio cuenta de que la dirección de correo electrónico del solicitante no coincidía exactamente con la del CEO, habían transcurrido dos días y el delincuente ya había robado casi USD 400,000.

En los **EE. UU.**, el FBI informa pérdidas de **cientos de millones de dólares** cada año.
El **monto promedio** es de alrededor de
USD 140,000

Desde enero del 2015, ha habido un
aumento del 1,300 %
en pérdidas expuestas identificadas,
que ahora llegan a un total de más de USD 3,000 millones

Cómo mantener su negocio seguro:

- Asegúrese de que sus empleados estén al tanto de este tipo de fraude.
- Implemente un proceso de verificación interno de dos pasos para realizar pagos, que incluya una comprobación del solicitante que no sea por medio del correo electrónico.
- **Llame al solicitante utilizando un número de teléfono verificado** para hacer un seguimiento de una solicitud por correo electrónico.
  o NO responda directamente al correo electrónico inicial
  o NO utilice los números de teléfono ni otra información de contacto incluida en el correo electrónico.
- Verifique que las direcciones de correo electrónico coincidan exactamente con sus registros internos.
- Esté alerta con aquellas solicitudes de pago que sean inesperadas o irregulares, sin importar el monto involucrado. En caso de dudas, no realice el pago.

Si sospecha que fue víctima de un fraude, comuníquese con su representante de HSBC inmediatamente.