HSBC

Juntos prosperamos

HSBC*net*
Ingeniería social

Riesgos para sus negocios: Robo de datos | Pérdida financiera | Redirección fraudulenta de banca por Internet

¿Sabe con quién conversa por teléfono? ¿El correo electrónico o mensaje de texto parece verdadero? Manténgase alerta. Ahora, los ladrones tienen muchas formas ingeniosas de robar información con fines fraudulentos.

Estas tácticas se conocen como ingeniería social y están en aumento.

Cómo funciona la ingeniería social

Correos electrónicos fraudulentos
Correos electrónicos

Los correos electrónicos pueden crear una sensación de miedo, urgencia o de oportunidad para alentar a los destinatarios a hacer clic en un link o abrir un archivo adjunto que luego infecta su equipo con un virus o malware. Más tarde, esto les permite a los delincuentes robar información o dinero, o interrumpir el sistema de la computadora.

Si bien muchos estafadores actúan de forma aleatoria, algunos tienen como objetivo a grupos específicos de empleados o clientes. Esta técnica se denomina "spear phishing" (correos electrónicos fraudulentos focalizados). Un ejemplo es el fraude del CEO, en el que los delincuentes suplantan a los altos ejecutivos e instruyen a sus colegas para que les transfieran dinero.

Otra táctica es el fraude a través del desvío de pagos. Los delincuentes envían un correo electrónico en el que afirman ser un proveedor. Este correo indica que su información bancaria cambió, por lo que los fondos deben transferirse a otra cuenta.

No responda estos correos electrónicos.

Conversaciones telefónicas fraudulentas
Llamadas telefónicas

Los estafadores a menudo crean una sensación de pánico para obtener una respuesta rápida por teléfono. Cuando su objetivo es una organización, pueden fingir ser un colega sénior o un cliente que se encuentra en apuros o que requiere ayuda urgente.

Los estafadores también pueden llamarlo y fingir que pertenecen a HSBC. Es posible que intenten indicarle que realice operaciones que permitan el envío de pagos no autorizados a los delincuentes. Esto podría incluir la entrega de códigos de seguridad generados a partir de su token.

Muchas campañas de conversaciones telefónicas fraudulentas se escuchan con un volumen alto, ya que utilizan llamadas automáticas o de banda ancha para comunicarse con miles de posibles víctimas por hora.

Si recibe una llamada sospechosa, no proporcione información.

Mensajes de texto fraudulentos
Mensajes de texto

Los mensajes de texto fraudulentos intentan persuadir a su objetivo para hacer clic en links maliciosos, activar un troyano que pueda robar contraseñas y otros datos de gran valor.

Los mensajes de texto pueden afirmar que su banco sospecha que su cuenta estuvo expuesta a actividades fraudulentas, que se encuentra en problemas con las autoridades fiscales o que ganó dinero.

Los mensajes de texto fraudulentos normalmente solicitan una acción urgente, que se refiere a hacer clic en un link malicioso, lo que a su vez permite el robo de datos. Los filtros de correo no deseado evitan que los correos electrónicos fraudulentos lleguen a las bandejas de entrada, pero aún no existe ninguna solución general para evitar que los mensajes de texto lleguen al objetivo deseado.

No responda a esos mensajes ni haga clic en los links que contienen.

Si sospecha de una llamada telefónica, un mensaje de texto o un correo electrónico que afirmen ser de HSBC, llame a su representante de HSBC para obtener verificación adicional.

En qué debe fijarse

Los estafadores pueden usar una o más de las siguientes tácticas para intentar atacar a su organización:

Señales de advertencia	Acción recomendada
Recibe una llamada de un número de larga distancia desconocido o una llamada redirigida por un operador.	Pregunte por la identidad de quien llama (p. ej. quién es, de dónde es y por qué necesita la información). Confirme la identidad de quien llama a través del proceso de verificación de su organización.
Personas muy amigables o intimidantes que afirman que algo es muy urgente o importante y que, incluso, amenazan con quejarse. Estas personas pueden citar información familiar, como el nombre de su departamento o de su gerente para presionarlo para que divulgue información.	Confíe en su instinto. Si recibe una llamada sospechosa en la que le solicitan información del banco o del personal, no la proporcione. Informe sobre la llamada a través de los procesos internos de su organización.
Solicitudes que parezcan inusuales o que requieran que omita pasos o haga excepciones a procedimientos establecidos.	En caso de dudas, haga preguntas que lo ayuden a verificar si la solicitud es verdadera o no. Comuníquese con su gerente o administrador de sistemas de HSBCnet para obtener una segunda opinión antes de realizar cualquier otra acción.
Recibe un correo electrónico que parece ser de un colega de su organización. Cuando responde, la dirección de correo electrónico del destinatario cambia a la de una empresa externa.	Si cree que recibió un correo electrónico sospechoso, no responda, no haga clic en ningún link ni abra archivos adjuntos. Informe sobre el correo electrónico a su administrador de sistemas de HSBCnet y reenvíe el mensaje a hsbcnet.phishing@hsbc.com. Luego, elimine el correo electrónico de su bandeja de entrada.
Llega un mensaje de texto inesperado a su teléfono móvil que dice ser de HSBC. En este le piden que haga clic en un link para realizar una acción urgente. No haga clic en ningún link que venga en un mensaje de texto que no esperaba recibir. No responda el mensaje con la información de contacto suministrada en el mismo.	No haga clic en ningún link que venga en un mensaje de texto que no esperaba recibir. No responda el mensaje con la información de contacto suministrada en el mismo. En caso de duda, verifique el mensaje de texto mediante los contactos conocidos de HSBC.

Cómo mantener su negocio seguro:

- Cree conciencia sobre las posibles consecuencias que la ingeniería social puede tener en su organización e implemente una política para informar sobre los casos sospechosos.
- Nunca comparta información financiera o de su empresa con gente que no conozca.
- No tome decisiones apresuradas.
- Nunca haga clic en los links que contienen los mensajes de texto o correos electrónicos ni abra o descargue los archivos adjuntos, a menos que tenga la certeza de que son seguros.
- Tenga cuidado con la información que comparte en las redes sociales, ya que puede suministrar pistas a los estafadores, que al final crean un panorama general.
- Siempre realice llamadas a números de teléfono que conozca y que haya verificado. Si alguien afirma ser un colega, compruebe que su nombre aparece en el directorio del personal de la organización y vuelva a llamarlo a su número de teléfono interno.
- Reenvíe los correos electrónicos sospechosos a **hsbcnet.phishing@hsbc.com**