30/03/2020

Envío de correos fraudulentos que suplantan a Caixabank



Recursos afectados:

Cualquier empleado, autónomo o empresa que sea cliente de CaixaBank y realice, habitualmente, operaciones de banca electrónica.

Descripción:

Se ha detectado una campaña de envío de correos electrónicos fraudulentos que suplantan a CaixaBank, cuyo objetivo es dirigir a la víctima a una página web falsa (*phishing*) para robar sus credenciales de acceso e información bancaria.

Solución:

Como en cualquier otro caso de phishing, extrema las precauciones y avisa a tus empleados para que estén alerta de los correos que reciban de origen sospechoso, especialmente, si contienen archivos adjuntos o como en este caso, enlaces externos a páginas de inicio de sesión.

Si algún empleado ha recibido un correo de estas características, ha accedido al enlace e introducido las credenciales de acceso a la cuenta bancaria, deberá modificar lo antes posible la contraseña de acceso a la banca online, así como contactar con la entidad bancaria para informarles de la situación. Además, se recomienda modificar la contraseña de todos aquellos servicios en los que se utilice la misma.

Como pautas generales, para evitar ser víctima de fraudes de este tipo, se recomienda:

- No abrir correos de usuarios desconocidos o que no haya solicitado: hay que eliminarlos directamente.
- En caso de que el correo proceda de una entidad bancaria legítima, nunca contendrá enlaces a su página de inicio de sesión o documentos adjuntos.

- No contestar en ningún caso a estos correos.
- Tener precaución al seguir enlaces o descargar ficheros adjuntos en correos electrónicos, SMS, mensajes en WhatsApp o redes sociales, aunque sean de contactos conocidos.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus comprobar que está activo.
- Asegúrate de que las cuentas de usuario de tus empleados utilizan contraseñas robustas y sin permisos de administrador.

Además, para prevenir y reforzar estos consejos, es importante realizar acciones de concienciación en ciberseguridad entre los empleados.

Detalle:

La campaña maliciosa detectada suplantando a CaixaBank tiene como asunto “Nuevo protocolo de acceso a oficinas CaixaBank” o similar. En la comunicación se informa al usuario que con motivo del estado de alarma han actualizado los protocolos de actuación en las oficinas, han mejorado sus procedimientos de seguridad en banca online y para evitar que su cuenta sea suspendida, debe acceder al enlace y seguir los pasos que se indican con un límite de tiempo de 24 horas.

El enlace tiene la apariencia del oficial, pero redirige a una web fraudulenta y no a la legítima de la entidad.

El correo recibido es similar al que se muestra en la siguiente imagen:

Haciendo clic en el enlace del correo, el usuario accederá a la página web fraudulenta que suplanta a la de CaixaBank.
Tras introducir las credenciales de acceso, será enviado a una sección donde se solicita información referente a la tarjeta de crédito.
A continuación el número de teléfono.
Por último, se solicita dos veces un código de verificación SMS.
Una vez introducidos los datos el usuario, será redirigido a la página web legítima de CaixaBank.
Fuente: INCIBE https://www.incibe.es/content/envio-correos-fraudulentos-suplantan-caixabank