Tendencias del Fraude

Controles de Seguridad en Línea de HSBC*net*

HSBC*net*

HSBC

Contenido

- Tipos de Fraude
  - Ataques de Malware
  - Intercepción del Correo Electrónico Corporativo
  - Phishing de Voz (“Vishing”)
  - Phishing de Servicio de Mensajes Cortos (SMS) (“Smishing”)
- Cómo Evitar Convertirse en Víctima
- Seguridad Adicional de la Banca por Internet de HSBC*net*.

Ataques de Malware

- Malware es un software que se utiliza para interrumpir el funcionamiento de un computadora, recopilar información confidencial o acceder a sistemas informáticos privados

- El sistema del cliente corre el riesgo de verse involucrado en operaciones fraudulentas

- Los clientes experimentarán lentitud en sus computadoras, pantallas inusuales que solicitan códigos y otras que indican que el usuario debe esperar un tiempo antes de iniciar sesión otra vez

- El Malware puede descargarse de manera involuntaria cuando hace clic en vínculos de correos electrónicos fraudulentos, sitios web sospechosos y cuando se descargan software no originales o piratas

HSBC

Ataques de Malware

Ejemplos:

- Durante el inicio de sesión, los clientes pueden recibir la pantalla "***Please Wait*** (Espere)"

- Es posible que la computadora se vuelva muy lenta

- Las pantallas emergentes le solicitarán ingresar el código de seguridad y otras le solicitaran presionar el botón amarillo
  (reclamaciones de validación del token, problemas de seguridad o resincronización)

- Pueden aparecer pantallas que soliciten que un segundo usuario inicie sesión en el mismo equipo para la validación

HSBC

Intervención del Correo Electrónico Corporativo

- Método de estafa a través de la identificación de clientes de instituciones financieras

- Se produce cuando los estafadores suplantan a contratistas, proveedores, acreedores o incluso a personas de alta dirección para pedirle a una empresa que cambie su pago

- Entonces, los pagos legítimos posteriores se redirigen a la cuenta del estafador

¿Por qué este tipo de ataque es difícil de detectar?

- Los ataques se producen en todas las instituciones financieras y no se limitan a ningún país o región
- Los estafadores se preparan muy bien antes de efectuar el ataque y realizan algún tipo de reconocimiento (ingeniería social) para asegurarse de que la información y los nombres son correctos
- Las direcciones de correo electrónico que utilizan para solicitar los cambios en la cuenta del beneficiario son idénticas o muy similares a las de los proveedores o distribuidores originales, lo cual dificulta la detección del fraude
- Los estafadores son conocidos por acceder ilegalmente a la cuenta de correo electrónico de un acreedor para enviar la solicitud de cambio de beneficiario y, de este modo, una solicitud parece ser legítima
- A través del servicio de correo tradicional, se enviaban cartas falsificadas que parecían ser del acreedor
- Se aprovechan de una conducta o respuesta humana que la tecnología no puede prevenir

Intervención del Correo Electrónico Corporativo

Ejemplos:

- Correos electrónicos de los proveedores existentes o nuevos que indiquen que los números de cuenta se cambiaron y solicitan que los pagos se envíen a una nueva cuenta y ubicación
- Proveedores que soliciten que los pagos ahora deben dirigirse a una empresa matriz en otro país
- Empleados que reciben un correo electrónico de su CEO o CFO en el que se solicita que realicen los pagos, pero más adelante se descubre que se intervino el correo electrónico del CEO o CFO
- El correo electrónico puede provenir de un dominio que es similar a una fuente legítima

Phishing de Voz ("Vishing")

- Vishing es el término utilizado para describir las tácticas utilizadas por los estafadores para "capturar" información personal (como las claves de seguridad de la banca en línea) a través del teléfono.
- Los estafadores pueden fingir que pertenecen a HSBC para comunicarse con los clientes. Pueden llevarlo a realizar acciones 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.

HSBC nunca le solicitará información por teléfono que pudiera utilizarse para realizar un pago, como pedir códigos generados por un dispositivo de seguridad o divulgar alguno de sus datos de seguridad.

HSBC

Phishing de SMS ("Smishing")

- El smishing es una variante del Phishing que utiliza mensajes SMS en vez de correos electrónicos
- Los estafadores pueden fingir que pertenecen a HSBC para comunicarse con los clientes mediante mensajes de SMS. Pueden llevarlo a realizar acciones 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.

HSBC nunca le solicitará información que pudiera utilizarse para realizar un pago, como pedir códigos generados por un dispositivo de seguridad o divulgar alguno de sus datos de seguridad.

¿Cómo Puede Evitar Convertirse en Víctima?

- Desconfíe de las solicitudes que piden cambiar la información del beneficiario: cuestione todos los cambios y valide cualquier solicitud de cambio mediante los canales adicionales
  (es decir, devuelva la llamada y no responda directamente al correo electrónico)

- Establezca los procedimientos de control internos para las solicitudes de cambio de datos del beneficiario

- Si aparecen pantallas emergentes poco usuales o la respuesta de la computadora es más lenta que de costumbre, cierre por completo la sesión de HSBC*net* y analice el equipo con la versión más actualizada del software de protección contra virus. Si tiene dudas, comuníquese con el equipo de TI o con el equipo o el Gerente del Servicio al Cliente de HSBC.

- Haga que el personal se comprometa con el aprendizaje y la importancia del fraude

¿Cómo puede evitar convertirse en una víctima?

- Nunca revele los datos de seguridad por teléfono cuando reciba llamadas no solicitadas (es decir nombre de usuario, información del token, datos de pago)

- Cuando reciba una llamada no solicitada de HSBC, consulte los datos de contacto de la persona que llama y valide la información con el Gerente del Servicio al Cliente o las mesa de ayuda de HSBC

- No modifique información de pago a menos que esté seguro de que esta es legítima

- Informe los intentos de fraude a su banco y revise la configuración del correo electrónico (por ejemplo, cambie la contraseña)

Seguridad Adicional de la banca por internet de HSBC*net*

- No presione el botón amarillo del dispositivo de seguridad, a menos que esté firmando una operación que creó: HSBC nunca solicita una respuesta relacionada con el botón amarillo al iniciar sesión
- Use Doble Control:para las operaciones y derechos (*es decir. Se requiere un mínimo de dos personas para cualquier actividad*)
- Descargue el software *SecureAnywhere* de Webroot en: www.hsbcnet.com sin costo alguno para usted
- Establecer Límites de Firma
- Bloquee todos los inicios de sesión que no provienen de una lista aprobada de direcciones IP
- Actualice el software que no es compatible con los proveedores *(por ejemplo, Internet Explorer 7)*
- Solo acceda a HSBC*net* mediante la dirección de la página web desde la barra de direcciones de su navegador
- No acceda mediante hipervínculos incorporados en un correo electrónico y no confíe solo en la apariencia o aspecto de un sitio web cuando use HSBC*net*