Universidad Veracruzana

Guía para detección de Phishing mediante correo electrónico

Ciberseguridad
UV-CSIRT

Información segura... ¡es cultura!®

Guía para detección de Phishing mediante correo electrónico

Introducción

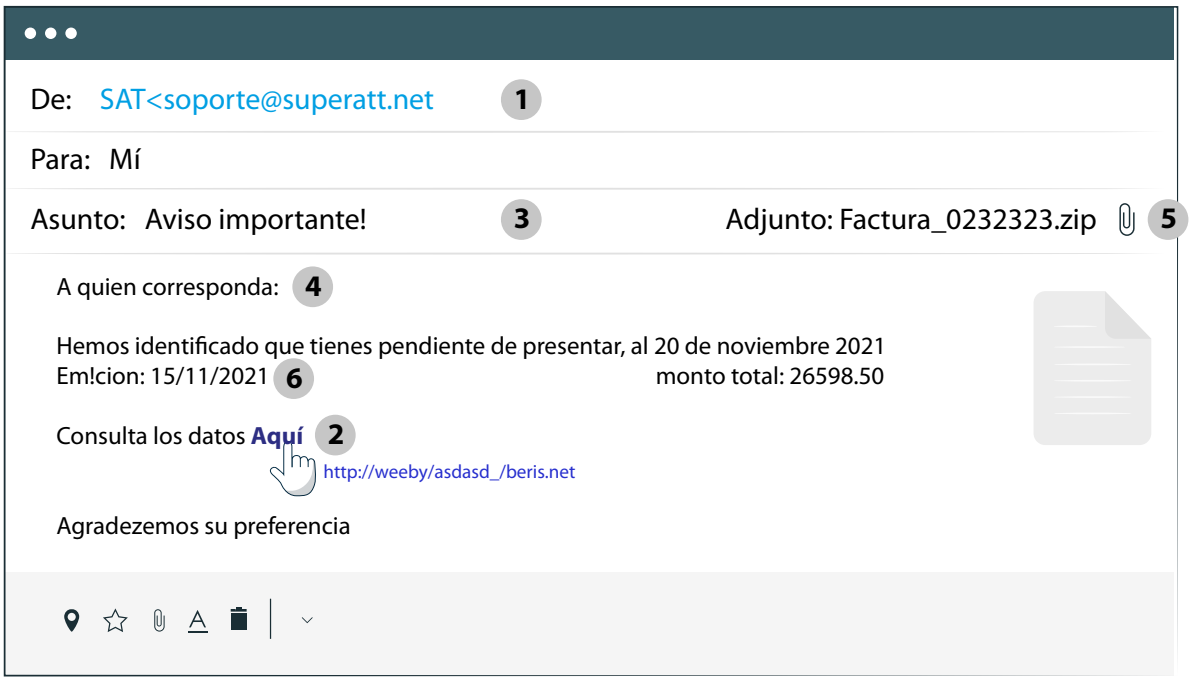
El phishing ha sido uno de los métodos más eficaces de los atacantes que les permite recabar información y engañar al usuario, usando diferentes tácticas de ingeniería social principalmente.
Uno de los medios más utilizados para realizar este tipo de ciberataques es el correo electrónico, aunque también los ciberdelincuentes utilizan otros medios como sitios web falsos, mensajes de texto, llamadas telefónicas.
Sin embargo, esta guía se enfoca en presentar las variantes de correos fraudulentos asi como los elementos que se debe considerar para saber reconocer este tipo de correos.

Objetivo

Proporcionar los elementos que permitan identificar los diversos correos fraudulentos conocidos como phishing y que el usuario reconozca que la concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes.

¿Cómo reconocer un correo fraudulento?

La mayoría de los correos fraudulentos, tienen algunas características que nos permiten estar alerta y reconocer casi de inmediato que se trata de una estafa. Algunos de estas se describen a continuación.



Guía para detección de Phishing mediante correo electrónico

1. Remitente desconocidos o suplantados

En ocasiones se reciben correos electrónicos que no esperábamos, es decir de remitentes desconocidos, o incluso de remitentes que aparentan ser de un empleado de la institución conocida, incluso en la que labora.

2. Enlace a sitios web suplantados

Pueden incluir enlaces a sitios web suplantados que direcciona a una dirección distinta a la que dice ser y que se visualiza igual a la organización real en el que pide datos de acceso.

3. El asunto capta la atención

Estos correos generan un sentido de alerta, urgencia o llaman la atención con un regalo o ganga en el asunto o contenido del correo.

El atacante puede usar frases como:

- “Buzón lleno”
- “Actualización de correo”
- “Aviso importante”
- “Esperamos confirmación de pago”
- “Archivos PDF y XML Factura Electrónica Data: 01/02/2021”
- “Comprobante Data: 11/02/2021 994238802”
- “Tu línea de crédito se reducirá”
- “Aviso de comparecencia ante el tribunal”
- “Tu correo ha sido comprometido”

4. Comunicación impersonal

Se refieren al usuario (destinatario) de forma genérica como “usuario”, “cliente” y no con el nombre completo.

5. Archivos adjuntos maliciosos

Algunos correos invitan a abrir un archivo adjunto que puede contener código malicioso y que el usuario no estaba esperando

6. Redacción

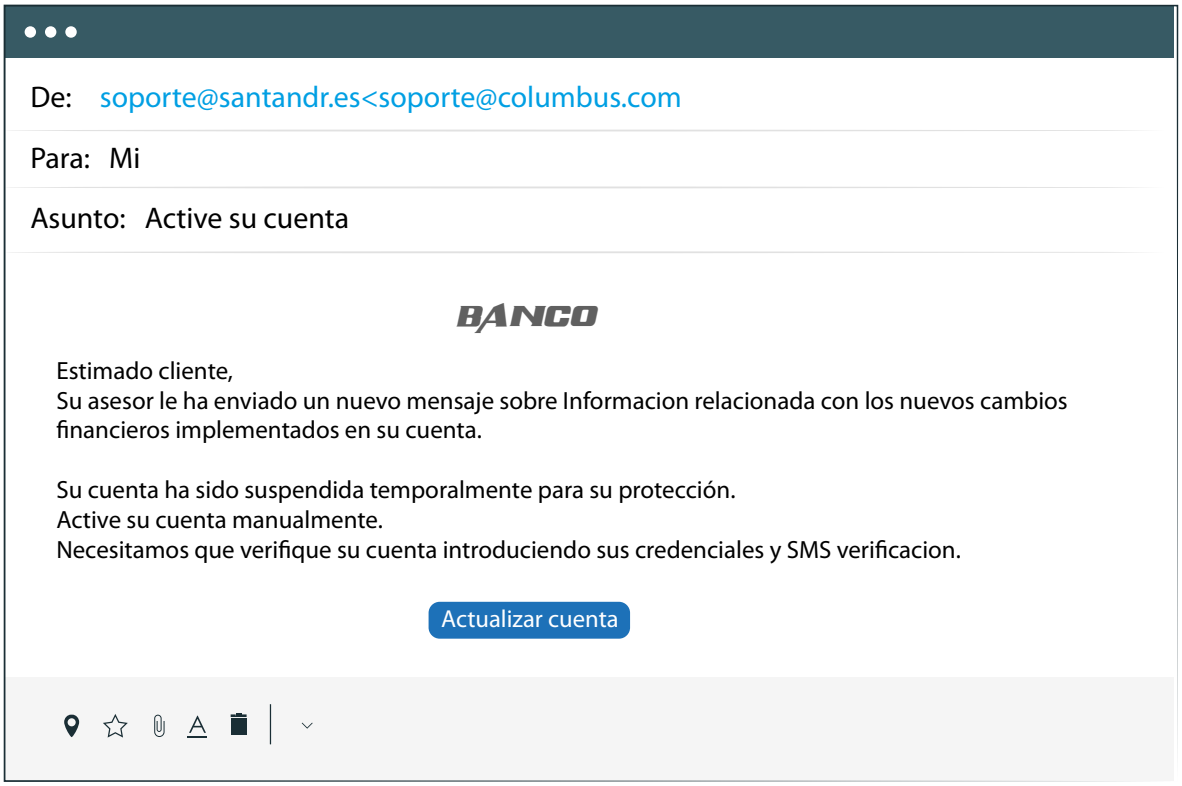
La mayoría de las veces, este tipo de correos, se muestran en su contenido con mala redacción, faltas de ortografía, o incluso parecen una mala traducción a otro idioma.

Guía para detección de Phishing mediante correo electrónico

Tipos de correos fraudulentos

Phishing

Este tipo de correos, suplantan la identidad de alguna institución, tratando de engañar al usuario para que ingrese a un enlace en donde lo vinculará a un sitio web falseado que se visualiza “igual” al de la institución conocida solicitando ingresar datos personales, bancarios o credenciales de inicio de sesión de algún servicio.
En la siguiente imagen se muestra un ejemplo de un correo que aparentemente lo envía una institución conocida.



Guía para detección de Phishing mediante correo electrónico

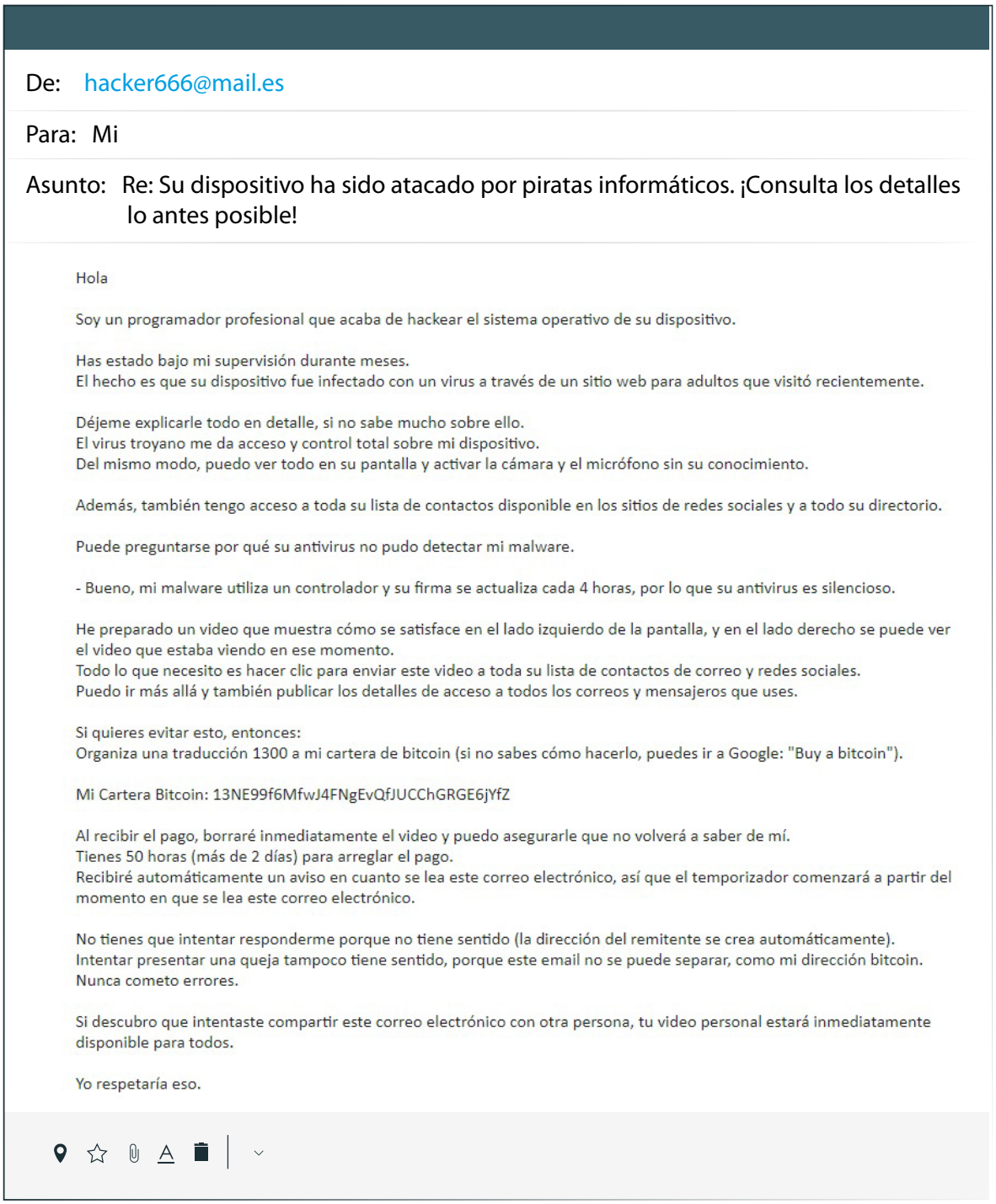
Scam

Este tipo de correos tienen el objetivo de engañar a los usuarios, haciendo creer que han ganado un premio, la lotería, celular, oferta de empleo, prestamos, etc. para obtener información bancaria o personal y así realizar una estafa.

Guía para detección de Phishing mediante correo electrónico

Sextorsión

El objetivo de estos correos es extorsionar a los usuarios destinatarios con un supuesto video de contenido sexual. Este tipo de fraude recibe el nombre de sextorsión. En el contenido se amenaza al usuario con el envío del vídeo entre su red de contactos por lo que le solicita que deposite dinero para que no sea distribuido.



De: hacker666@mail.es

Para: Mi

Asunto: Re: Su dispositivo ha sido atacado por piratas informáticos. ¡Consulta los detalles lo antes posible!

Hola

Soy un programador profesional que acaba de hackear el sistema operativo de su dispositivo.

Has estado bajo mi supervisión durante meses.
El hecho es que su dispositivo fue infectado con un virus a través de un sitio web para adultos que visitó recientemente.

Déjeme explicarle todo en detalle, si no sabe mucho sobre ello.
El virus troyano me da acceso y control total sobre mi dispositivo.
Del mismo modo, puedo ver todo en su pantalla y activar la cámara y el micrófono sin su conocimiento.

Además, también tengo acceso a toda su lista de contactos disponible en los sitios de redes sociales y a todo su directorio.

Puede preguntarse por qué su antivirus no pudo detectar mi malware.

- Bueno, mi malware utiliza un controlador y su firma se actualiza cada 4 horas, por lo que su antivirus es silencioso.

He preparado un video que muestra cómo se satisface en el lado izquierdo de la pantalla, y en el lado derecho se puede ver el video que estaba viendo en ese momento.
Todo lo que necesito es hacer clic para enviar este video a toda su lista de contactos de correo y redes sociales.
Puedo ir más allá y también publicar los detalles de acceso a todos los correos y mensajeros que uses.

Si quieres evitar esto, entonces:
Organiza una traducción 1300 a mi cartera de bitcoin (si no sabes cómo hacerlo, puedes ir a Google: "Buy a bitcoin").

Mi Cartera Bitcoin: 13NE99f6MfwJ4FNgEvQfJUCChGRGE6jYfZ

Al recibir el pago, borraré inmediatamente el video y puedo asegurarle que no volverá a saber de mí.
Tienes 50 horas (más de 2 días) para arreglar el pago.
Recibiré automáticamente un aviso en cuanto se lea este correo electrónico, así que el temporizador comenzará a partir del momento en que se lea este correo electrónico.

No tienes que intentar responderme porque no tiene sentido (la dirección del remitente se crea automáticamente).
Intentar presentar una queja tampoco tiene sentido, porque este email no se puede separar, como mi dirección bitcoin.
Nunca cometo errores.

Si descubro que intentaste compartir este correo electrónico con otra persona, tu video personal estará inmediatamente disponible para todos.

Yo respetaría eso.

Guía para detección de Phishing mediante correo electrónico

Malware

Estos correos incluyen archivos adjuntos que contienen código malicioso y cuya intención es que el usuario descargue y/o abra el documento para infectar el equipo. Estos correos suelen estar con una extensión ejecutable como .exe, sin embargo, también se puede observar con archivos conocidos como .pdf o imágenes.

Recomendaciones para evitar caer en estafas por correo electrónico.

- ¡Sea precavido!, lea atentamente el remitente, si no espera recibir un correo de dicho remitente, **use el sentido común.**
- No confíe únicamente en el nombre del remitente, verifique que el propio dominio del correo recibido es de confianza.
- Si sospecha que el correo es fraudulento **no abra los enlaces.**
- Analice el enlace, sitúa el cursor encima del enlace para ver la URL real a la que dirige. Si no coincide con el dominio de la institución que supuestamente te envía el correo, o es una web sin certificado de seguridad, no de clic.
- **No descargue ni abra los archivos adjuntos de correos que parezcan sospechosos.**
- Puede crear filtros para aquellos correos que desconozca, así la próxima vez que lo vuelva a recibir, no estará en la bandeja de entrada.
- Revise la redacción y busque errores de ortografía, gramaticales, si no está personalizado, está en un idioma distinto al de su país que no esperaba o parece una mala traducción, sospeche.
- Mantenga **actualizado su equipo de cómputo, así como el antivirus.** Las versiones más recientes de Windows 10 traen incorporado un antivirus “Windows Defeder” o “Microsoft Defender” que se actualiza diariamente.
- Si recibe un correo sospecho de un remitente con dominio de una institución conocida, repórtelo directamente al área de seguridad de su institución.

En ese sentido, es importante considerar: **ninguna institución financiera o publica solicitará datos personales o datos asociados a su cuenta institucional como usuario o contraseña o datos financieros como números de tarjeta a través del correo electrónico o algún otro medio.**

Por último, si has recibido en tu **cuenta institucional** correos con las características mencionadas o si has sido víctima de alguno, repórtalo a la cuenta de correo: reportaspam@uv.mx

¡NO caigas en el PHISHING!

#InformaciónSeguraEsCultura