EL CORREO ELECTRÓNICO

Consejos para no ser víctima de un ciberataque inesperado

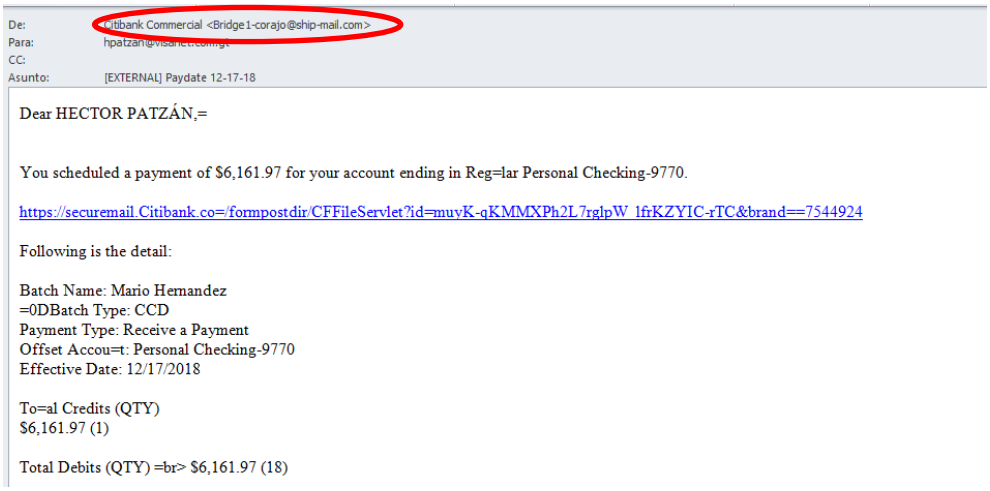
El correo electrónico se ha convertido en una herramienta de trabajo indispensable para el desarrollo diario de cualquier Empresa. Los ciberdelincuentes no dudarán en usarlo para acceder a la información de la Organización.

Por tal razón, queremos ayudarte a identificar los correos falsos denominados **Phishing** en los que los delincuentes **suplantan la identidad** de una Organización con fines maliciosos.

El objetivo de este tipo de correos fraudulentos es muy amplio, pero en su mayoría buscan conseguir información confidencial como **credenciales de acceso o información bancaria**, **infectar dispositivos corporativos** con cualquier clase de malware como el Ransomware o el **ingreso directo en una cuenta bancaria** controlada por los ciberdelincuentes.

A continuación, se detallan algunos ***tips*** para detectar correos maliciosos:

- ¡Fíjate en el **Remitente**!
  - La dirección de correo electrónico del remitente no coincide exactamente con el nombre de la Entidad a la que pretende suplantar, usando en su lugar una dirección muy similar a la legítima.


De: Citibank Commercial <Bridge1-corajo@ship-mail.com>
Para: hpatzan@visanet.com.gt
CC:
Asunto: [EXTERNAL] Paydate 12-17-18

Dear HECTOR PATZÁN,=

You scheduled a payment of $6,161.97 for your account ending in Reg=lar Personal Checking-9770.

https://securemail.Citibank.co=/formpostdir/CFFileServlet?id=muyK-qKMMXPh2L7rglpW_1frKZYIC-rTC&brand==7544924

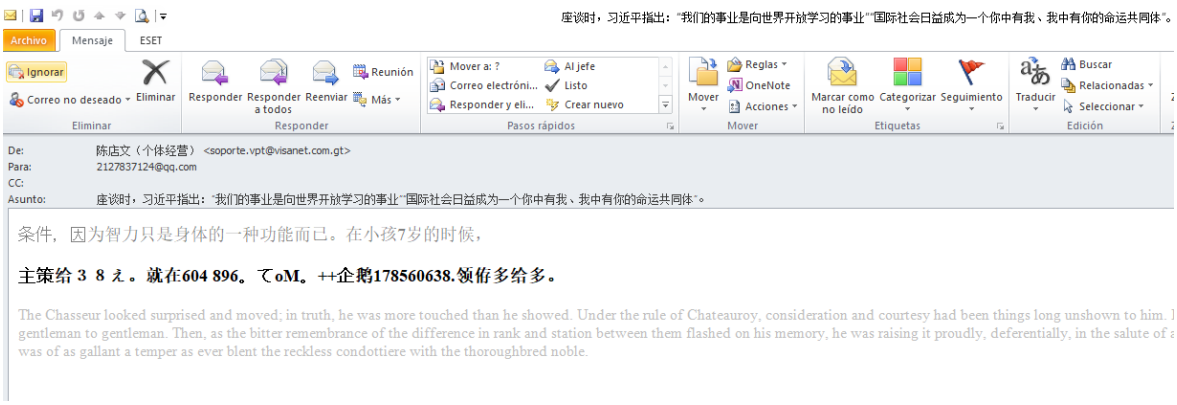
Following is the detail:

Batch Name: Mario Hernandez
=0DBatch Type: CCD
Payment Type: Receive a Payment
Offset Accou=t: Personal Checking-9770
Effective Date: 12/17/2018

To=al Credits (QTY)
$6,161.97 (1)

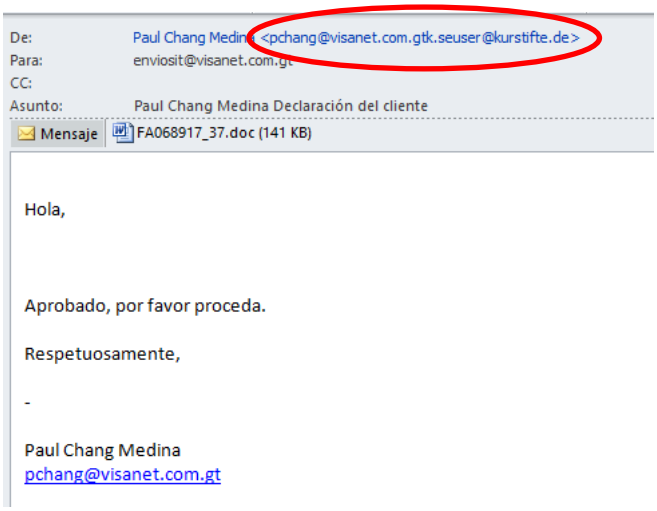
Total Debits (QTY) =br> $6,161.97 (18)

- En otras ocasiones es evidente que la dirección de correo no tiene nada que ver

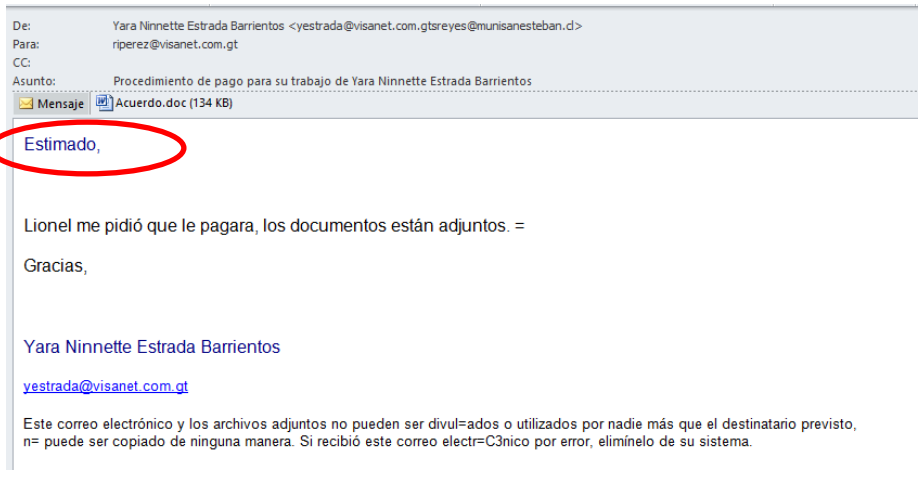


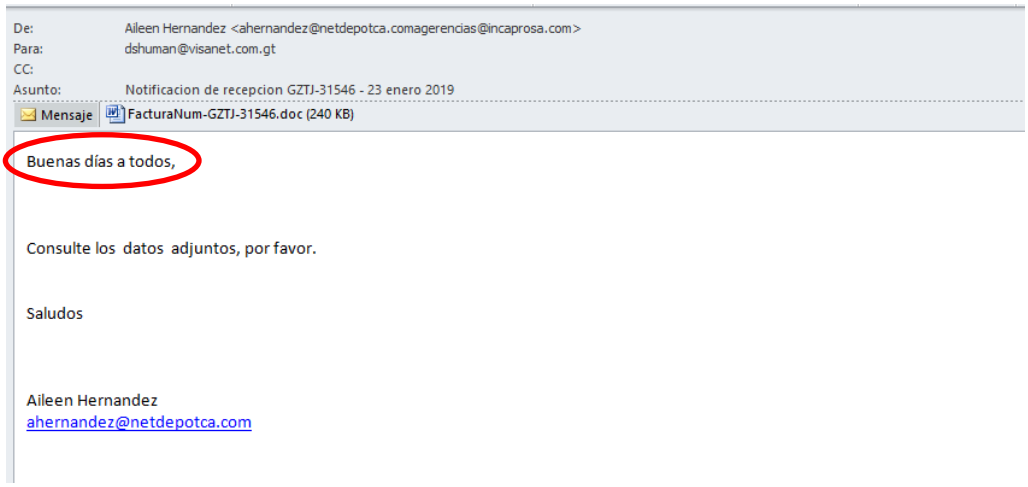
con el contenido:

- Revisa la **dirección** donde recibes el correo y el cuerpo del mensaje
  - El mensaje no tiene nada que ver o no corresponde con el puesto de trabajo del remitente.



- El mensaje comienza con un saludo genérico de tipo “Estimado” o “Buen día a todos”




De: Aileen Hernandez <ahernandez@netdepotca.comagerencias@incaprosa.com>
Para: dshuman@visanet.com.gt
CC:
Asunto: Notificacion de recepcion GZTJ-31546 - 23 enero 2019
Mensaje | FacturaNum-GZTJ-31546.doc (240 KB)

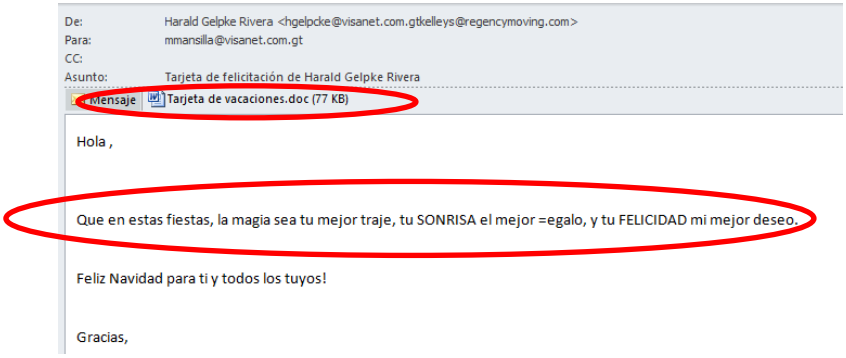
Buenas días a todos,

Consulte los datos adjuntos, por favor.

Saludos

Aileen Hernandez
ahernandez@netdepotca.com

- El mensaje es distinto a los que recibes del remitente: se dirige de una forma diferente, en otro idioma, e incluye importe de facturas no habituales para el remitente, hasta cobros que no maneja.


De: Harald Gelpke Rivera <hgelpcke@visanet.com.gtkelleys@regencymoving.com>
Para: mmansilla@visanet.com.gt
CC:
Asunto: Tarjeta de felicitación de Harald Gelpke Rivera
Mensaje | Tarjeta de vacaciones.doc (77 KB)

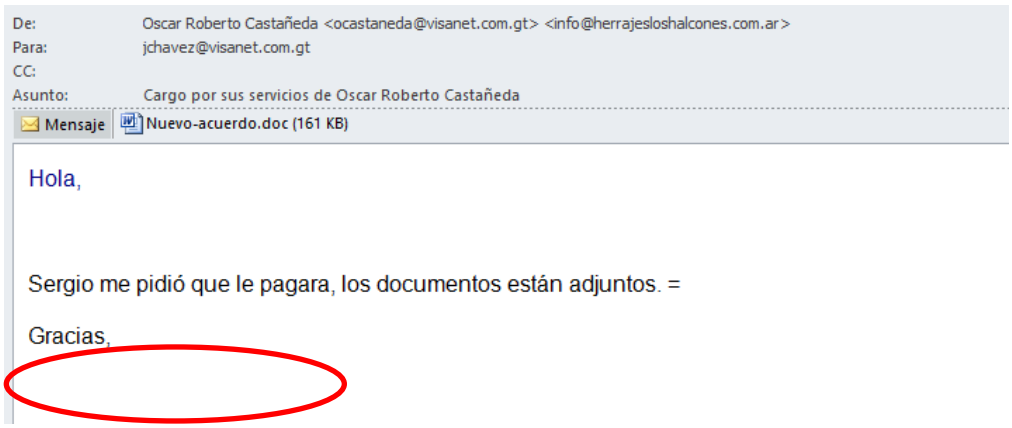
Hola ,

Que en estas fiestas, la magia sea tu mejor traje, tu SONRISA el mejor =egalo, y tu FELICIDAD mi mejor deseo.

Feliz Navidad para ti y todos los tuyos!

Gracias,

- Lo más común es que en el mensaje, intenten premiarlos con el pago de una factura, y que, al no hacerlo, puede incrementar la cantidad supuestamente que deben, o un falto reembolso de un supuesto cobro erróneo.

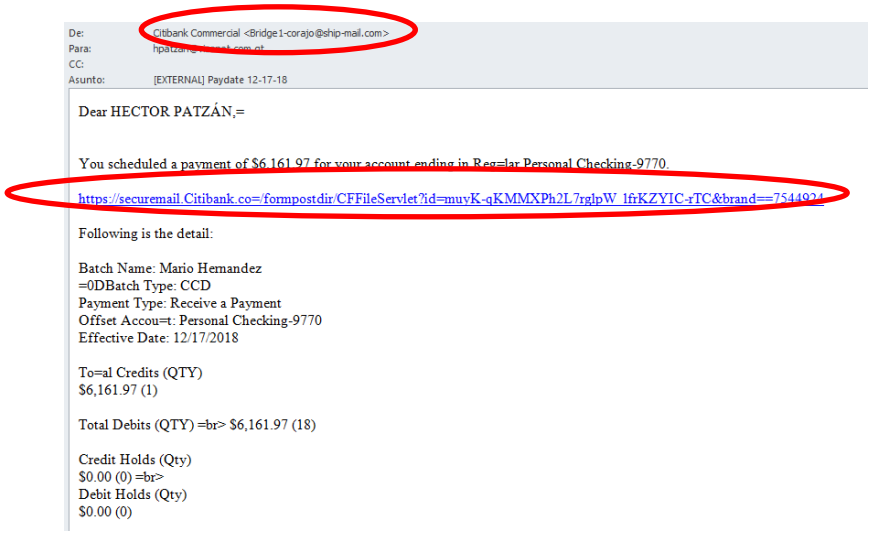

De: Oscar Roberto Castañeda <ocastaneda@visanet.com.gt> <info@herrajesloshalcones.com.ar>
Para: jchavez@visanet.com.gt
CC:
Asunto: Cargo por sus servicios de Oscar Roberto Castañeda
Mensaje | Nuevo-acuerdo.doc (161 KB)

Hola,

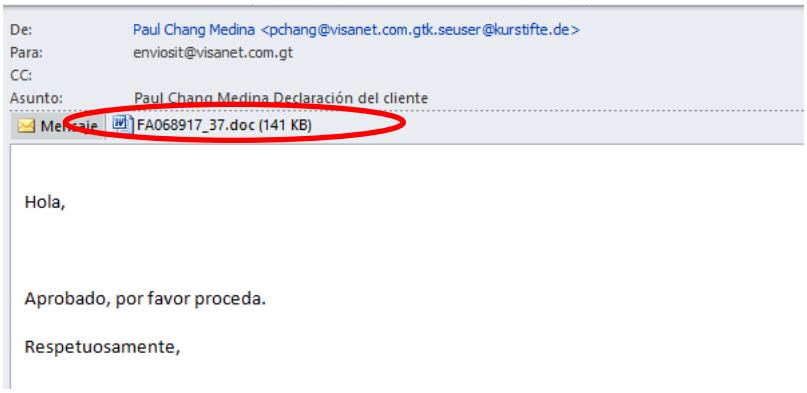
Sergio me pidió que le pagara, los documentos están adjuntos. =

Gracias,

- Revisa los **Enlaces**
  - El enlace que recibes en el correo es falso, pero algunas veces pareciera ser legítimo, por lo que hay que fijarse en la URL. En algunos casos, la dirección de la web falsa es muy parecida a la legítima. Si hay duda, no presionar en el enlace del correo y reportarlo al Área de Seguridad o Tecnología.



- ¡No confíes en los Archivos adjuntos!
  - Es común que diariamente recibamos documentos, informes o facturas adjuntas. **Sospecha** cuando el remitente sea desconocido o no hayas solicitado dicha información. Estos adjuntos contienen códigos maliciosos que se ejecutan al abrirlos y pueden dañar el equipo, red y/o robar información.



Además de conocer estos modelos de correos maliciosos, ten siempre en cuenta lo siguiente:

1. Escribe directamente la URL de la Empresa que tu conoces en el navegador, nunca llegues a ella a través de los enlaces adjuntos en correos electrónicos o desde páginas de terceros.
2. No accedas a sitios web bancarios desde computadoras públicas, no confiables o que estén conectados a redes Wifi Públicas. En caso de tener urgencia en esto, usa la cobertura 4G de tu dispositivo móvil.
3. En caso de acceder desde tu computadora en la Empresa a sitios conocidos que siempre utilizas, revisa que sean sitios legítimos, mira el certificado de cada sitio Web al que accedes.
4. Si tienes sospecha por alguna anomalía que veas, repórtalo inmediatamente.