

Consejos para no ser víctima de un ciberataque inesperado

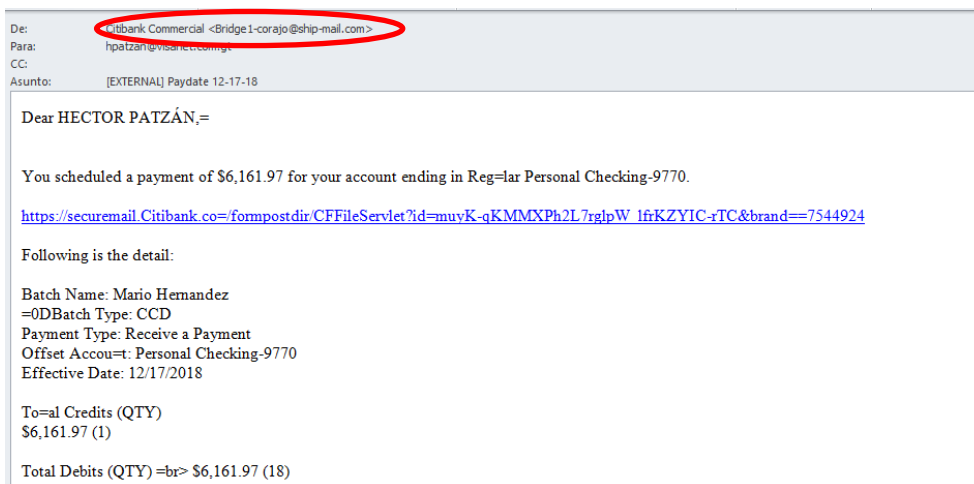
El correo electrónico se ha convertido en una herramienta de trabajo indispensable para el desarrollo diario de cualquier Empresa. Los ciberdelincuentes no dudarán en usarlo para acceder a la información de la Organización.

Por tal razón, queremos ayudarte a identificar los correos falsos denominados **Phishing** en los que los delincuentes **suplantando 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**.

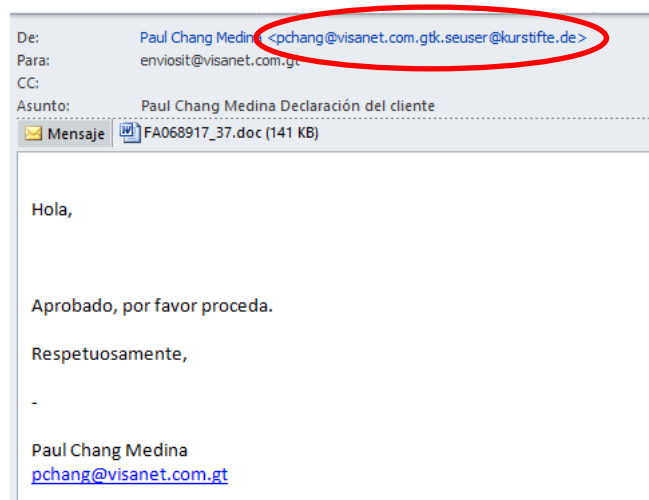


- En otras ocasiones es evidente que la dirección de correo no tiene **nada que ver**

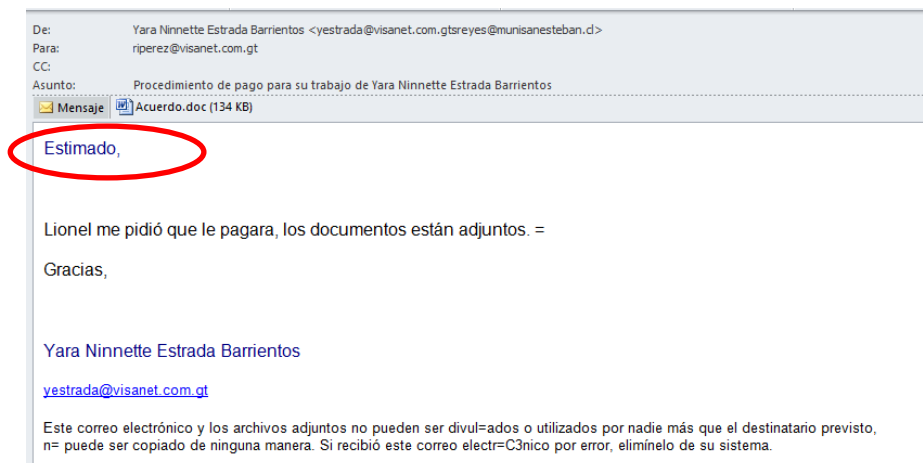


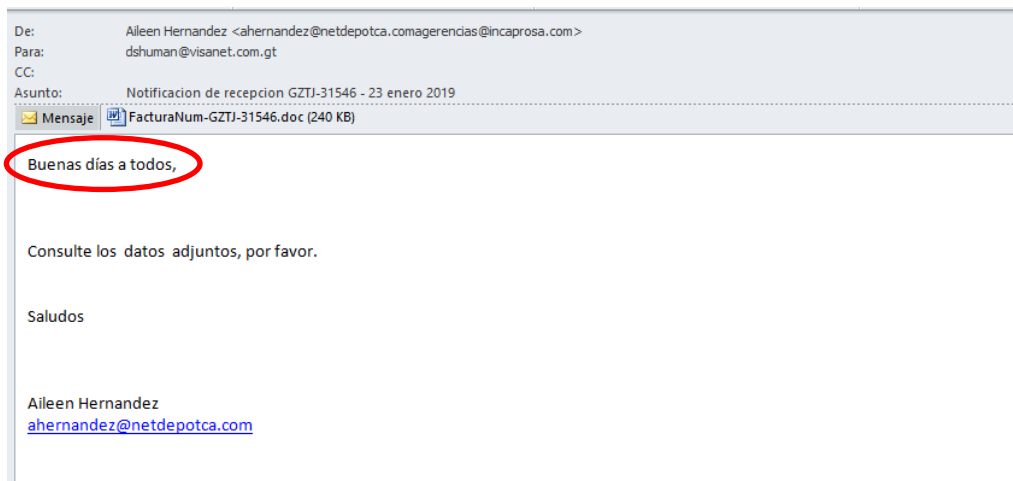
con el contenido:

- 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.

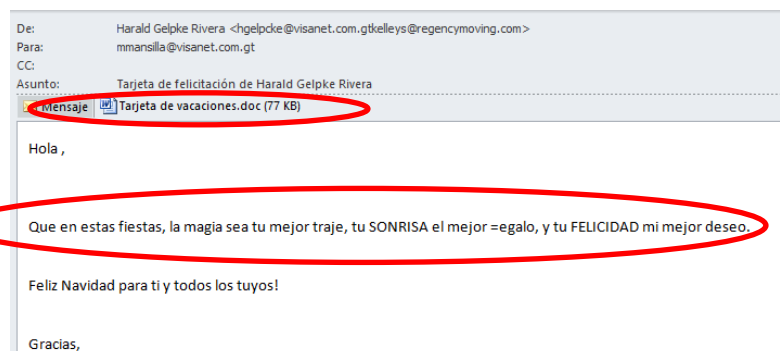


- El mensaje comienza con un **saludo genérico** de tipo “Estimado” o “Buen día a todos”

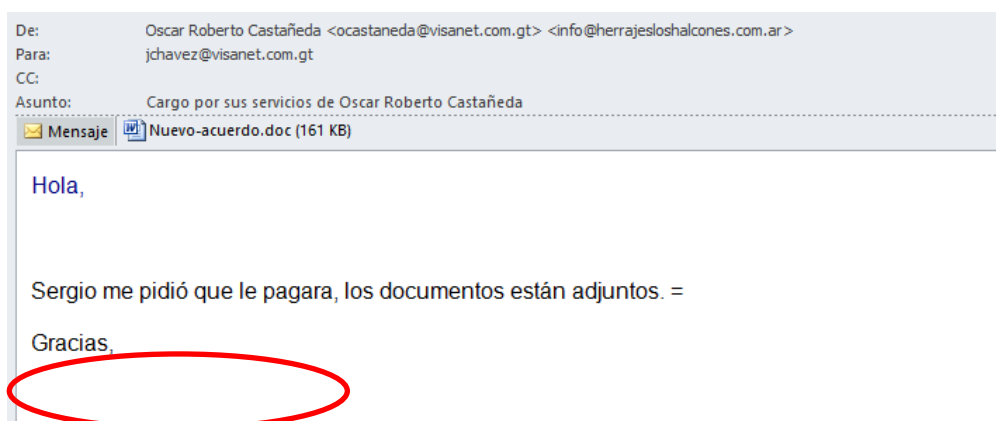




- El **mensaje es distinto** a los que recibes del remitente: se dirige de una forma diferente, en otro idioma, e incluye importe de facturas no habituales para el remitente, hasta cobros que no maneja.

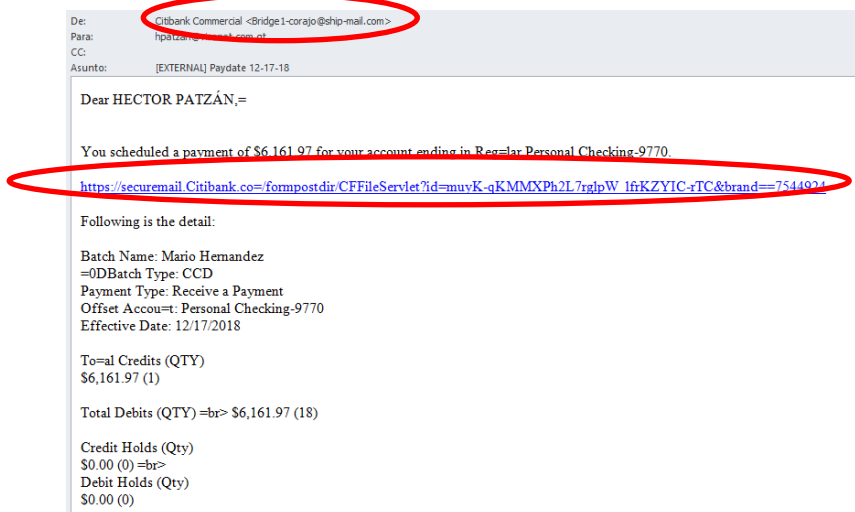


- Lo más común es que en el mensaje, intenten premiarlos con el pago de una factura, y que, al no hacerlo, puede incrementar la cantidad supuestamente que deben, o un fallo reembolso de un supuesto cobro erróneo.



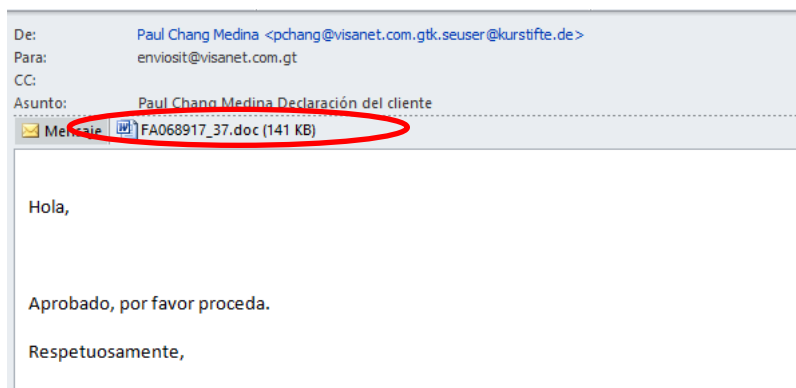
- Revisa los **Enlaces**

- 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.