OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS

CIRCULAR N°02

PARA: **ESTUDIANTES, DOCENTES Y PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD DE CALDAS.**

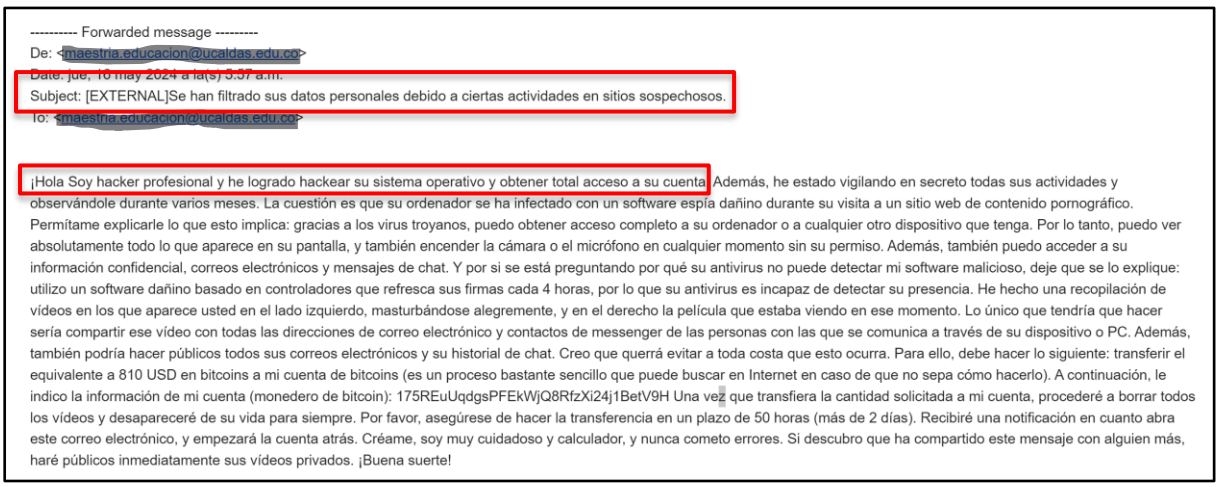
DE: **OFICINA DE SISTEMAS**

ASUNTO: **ALERTA SOBRE CORREOS ELECTRÓNICOS MALICIOSOS**

FECHA: **16 DE MAYO DE 2024**

Cordial saludo,

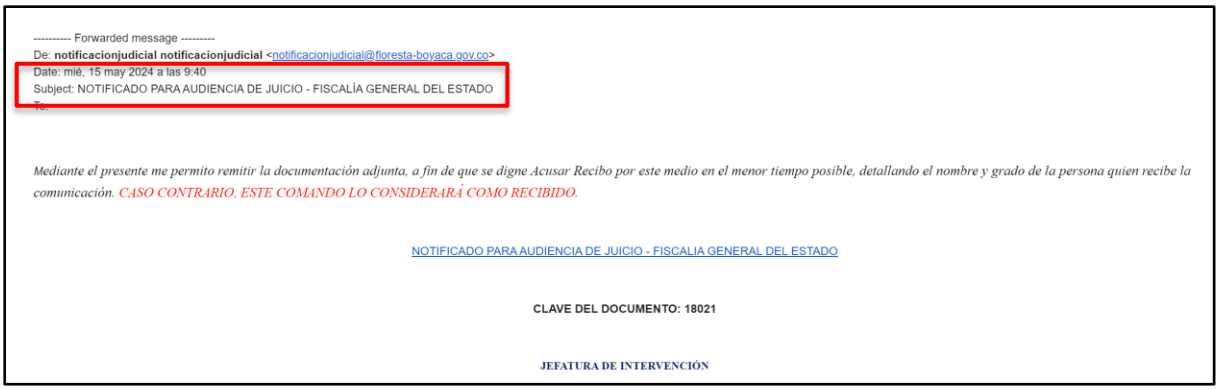
La Oficina Asesora de Planeación y Sistemas alerta a toda la comunidad universitaria sobre la circulación de correos electrónicos con contenido malicioso (phishing), en el cual indican sobre **embargos bancarios**, **notificaciones de demandas**, **reportes DIAN**, **extorciones**, en los cuales incitan a abrir archivos adjuntos con credenciales suministradas, o realizar consignaciones en bitcoints, similares a estas imágenes:



---------- Forwarded message ---------
De: <maestria.educacion@ucaldas.edu.co>
Date: jue, 16 may 2024 a la(s) 3:57 a.m.
Subject: [EXTERNAL]Se han filtrado sus datos personales debido a ciertas actividades en sitios sospechosos.
To: <maestria.educacion@ucaldas.edu.co>

¡Hola Soy hacker profesional y he logrado hackear su sistema operativo y obtener total acceso a su cuenta. Además, he estado vigilando en secreto todas sus actividades y observándole durante varios meses. La cuestión es que su ordenador se ha infectado con un software espía dañino durante su visita a un sitio web de contenido pornográfico. Permítame explicarle lo que esto implica: gracias a los virus troyanos, puedo obtener acceso completo a su ordenador o a cualquier otro dispositivo que tenga. Por lo tanto, puedo ver absolutamente todo lo que aparece en su pantalla, y también encender la cámara o el micrófono en cualquier momento sin su permiso. Además, también puedo acceder a su información confidencial, correos electrónicos y mensajes de chat. Y por si se está preguntando por qué su antivirus no puede detectar mi software malicioso, deje que se lo explique: utilizo un software dañino basado en controladores que refresca sus firmas cada 4 horas, por lo que su antivirus es incapaz de detectar su presencia. He hecho una recopilación de vídeos en los que aparece usted en el lado izquierdo, masturbándose alegremente, y en el derecho la película que estaba viendo en ese momento. Lo único que tendría que hacer sería compartir ese vídeo con todas las direcciones de correo electrónico y contactos de messenger de las personas con las que se comunica a través de su dispositivo o PC. Además, también podría hacer públicos todos sus correos electrónicos y su historial de chat. Creo que querrá evitar a toda costa que esto ocurra. Para ello, debe hacer lo siguiente: transferir el equivalente a 810 USD en bitcoins a mi cuenta de bitcoins (es un proceso bastante sencillo que puede buscar en Internet en caso de que no sepa cómo hacerlo). A continuación, le indico la información de mi cuenta (monedero de bitcoin): 175REuUqdgsPFEkWjQ8RfzXi24j1BetV9H Una vez que transfiera la cantidad solicitada a mi cuenta, procederé a borrar todos los vídeos y desapareceré de su vida para siempre. Por favor, asegúrese de hacer la transferencia en un plazo de 50 horas (más de 2 días). Recibiré una notificación en cuanto abra este correo electrónico, y empezará la cuenta atrás. Créame, soy muy cuidadoso y calculador, y nunca cometo errores. Si descubro que ha compartido este mensaje con alguien más, haré públicos inmediatamente sus vídeos privados. ¡Buena suerte!

Para este caso en particular sugerimos ELIMINAR el correo (el remitente aparece también como destinatario).



---------- Forwarded message ---------
De: **notificacionjudicial notificacionjudicial** <notificacionjudicial@floresta-boyaca.gov.co>
Date: mié, 15 may 2024 a las 9:40
Subject: NOTIFICADO PARA AUDIENCIA DE JUICIO - FISCALÍA GENERAL DEL ESTADO
To:

Mediante el presente me permito remitir la documentación adjunta, a fin de que se digne Acusar Recibo por este medio en el menor tiempo posible, detallando el nombre y grado de la persona quien recibe la comunicación. CASO CONTRARIO, ESTE COMANDO LO CONSIDERARÁ COMO RECIBIDO.

NOTIFICADO PARA AUDIENCIA DE JUICIO - FISCALIA GENERAL DEL ESTADO

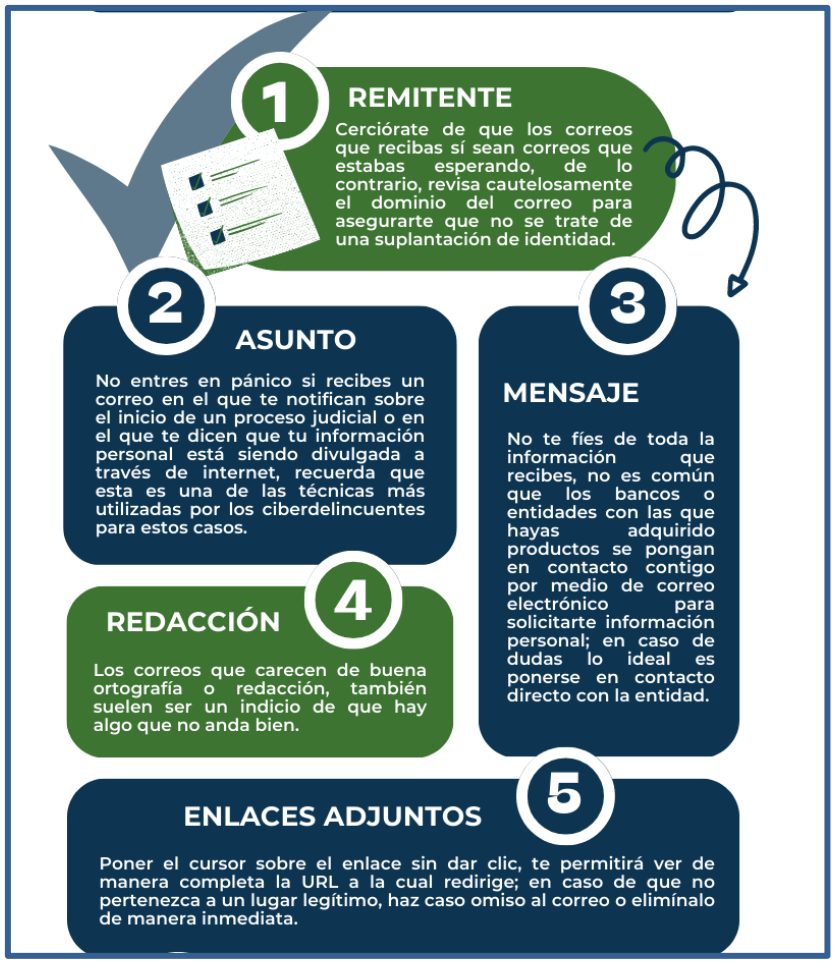
CLAVE DEL DOCUMENTO: 18021

JEFATURA DE INTERVENCIÓN

Ante estos casos las instrucciones a seguir son:

- NO intentar abrir los archivos adjuntos
- NO acceder a links suministrados
- Marcar el correo como “Denunciar suplantación de identidad”
- Eliminar el correo

Por último, compartimos algunos tips para identificar correos maliciosos, con el fin de evitar robo de información personal y financiera por medio de correos electrónicos:



Por favor compartir esta información.

Atentamente,

HECTOR FABIO TORRES MARTINEZ
Líder Oficina de Sistemas