⚠ ALERTA DE SEGURIDAD INSTITUCIONAL

Campaña de extorsión por correo electrónico en circulación

Tipo de alerta	Nivel de riesgo	Fecha
Ingeniería social / SPAM	BAJO (amenaza falsa)	Mayo 2026

> Se han detectado correos con asunto "Su cuenta ha sido hackeada" llegando a buzones institucionales. El asunto del correo varia para evitar la contención de estos mensajes. Estos mensajes son FALSOS. Nadie ha accedido a su equipo ni a su cámara o su equipo. No realice ningún pago solicitado en Bitcoins.

¿DE QUÉ SE TRATA?

Esta campaña se denomina sextorsión falsa. Los atacantes envían correos masivos afirmando haber instalado un troyano en su computador, haber grabado video comprometedor a través de la cámara y tener acceso a todos sus contactos y correos. Todo es mentira. El objetivo es generar pánico para que la víctima pague un rescate en criptomonedas. Esta táctica no requiere ningún conocimiento técnico del atacante: basta con enviar el mismo mensaje a millones de personas.

TEXTO DEL DE CORREO

Subject: [SPAM] Su cuenta ha sido hackeada. He robado sus datos. Averigüe cómo recuperar el acceso.

Hola,

Soy hacker y he conseguido acceder a su sistema operativo.
También tengo total acceso a su cuenta.

Llevo varios meses vigilándole.

La cuestión es que su ordenador se infectó con un malware cuando usted visitó un sitio para adultos.
Por si no sabe a qué me refiero, se lo explicaré.
Se trata de un virus troyano que me permite controlar por completo cualquier ordenador o dispositivo.
Esto significa que puedo ver todo lo que hay en su pantalla, y también encender la cámara y el micrófono sin que usted se dé cuenta.
También tengo acceso a todos sus contactos y correos electrónicos.

¿Por qué su antivirus no detecta el malware?
Respuesta: el malware que he utilizado está basado en controladores y actualizo sus firmas cada 4 horas.
De ahí que su antivirus sea incapaz de detectar su presencia.
He creado un vídeo donde aparece usted satisfaciéndose a sí mismo en la mitad izquierda de la pantalla,
y el vídeo que estaba viendo en ese momento en la mitad derecha.

Con solo hacer clic, puedo enviar el vídeo a todos sus contactos de correo electrónico y a sus redes sociales.
También puedo hacer públicos sus mensajes de correo electrónico y el historial de chat de los messengers que utiliza habitualmente.

Si no quiere que ocurra esto, transfiera el equivalente a 750 USD en bitcoins a mi dirección bitcoin
(si no sabe cómo hacerlo, busque "comprar bitcoins" en Google).

Mi dirección bitcoin (monedero de bitcoin) es:13EHaj6UjpA4yen32k5gyWceRpXRUTXxPG

En cuanto haya realizado el pago, borraré el vídeo inmediatamente, y listo. No volverá a saber nada más de mí.
Le daré 50 horas (más de 2 días) para pagar. Recibiré una notificación en cuanto abra este correo electrónico y empezará la cuenta atrás.
No tiene sentido presentar una denuncia en ningún sitio porque este correo electrónico no se puede rastrear, ni tampoco mi dirección bitcoin.

Nunca cometo errores.
Si descubro que ha compartido este mensaje con otra persona, el vídeo se distribuirá inmediatamente.

Saludos cordiales.

SEÑALES QUE CONFIRMAN QUE EL CORREO ES FALSO

✗ El remitente y el destinatario son la misma dirección institucional — técnica de spoofing para aparentar acceso a la cuenta.

✗ No adjunta ningún video ni muestra prueba real de acceso al equipo o a la cámara.

✗ El propio servidor de correo clasificó el mensaje como [SPAM] antes de entregarlo al buzón.

✗ Exige pago en bitcoin e impone un plazo artificial de "50 horas" — presión psicológica.

✗ El texto es genérico y traducido al español: se envía simultáneamente a miles de personas sin datos reales de ninguna.

¿QUÉ DEBE HACER SI RECIBE ESTE CORREO?

✓ HAGA ESTO

- Mantenga la calma: es una amenaza vacía.
- Si el correo ya fue marcado como Spam, no solicite recuperar el correo.

Elimine el correo sin responder.

- Si el correo llego a su bandeja de entrada marque el mensaje como spam o phishing.
- Notifique a la mesa de ayuda y Seguridad.

✗ NO HAGA ESTO

- No responda el correo bajo ninguna circunstancia.
- No realice ningún pago en bitcoin ni en efectivo.
- No haga clic en enlaces ni descargue adjuntos.
- No comparta sus datos personales ni contraseñas.

NOTA TÉCNICA: ¿CÓMO FUNCIONA ESTE ATAQUE?

La técnica usada se llama email spoofing: el atacante falsifica el campo "De:" para que el correo parezca provenir de la propia cuenta del destinatario. Esto NO implica acceso real al buzón ni al dispositivo. Los filtros anti-spam del INC detectaron y marcaron correctamente este mensaje. El malware descrito en el correo no existe: es una amenaza completamente fabricada.

REPORTE Y CONTACTO

Si recibió este correo o uno similar, repórtelo a la **mesa de ayuda** para registrar el incidente y bloquear variantes adicionales. Su reporte contribuye a proteger a otros funcionarios.

Canal de reporte	Clasificación sugerida
Mesa de Ayuda TI — ticket de incidente	Incidente de seguridad — phishing/spam

Dirección de Tecnologías de la Información y Seguridad

Instituto Nacional de Cancerología | Bogotá, mayo de 2026