Alerta ID:	0073-CSIRT
Fecha del reporte:	09/02/2026
Entidad:	Todas las Entidades del estado
Título:	Campaña de Phishing desde dominio de Microsoft
Herramienta de detección	N/A
Activo involucrado:	Infraestructura tecnológica y servicios de red de entidades públicas
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Crítico

Resumen ejecutivo

Informar a las entidades del Gobierno sobre la campaña de phishing altamente sofisticada que utiliza cuentas reales de correos electrónicos con dominio.**gov.co** (previamente comprometidas) para enviar mensajes fraudulentos. Los atacantes buscan suplantar la página de autenticación oficial de Microsoft Office 365 para capturar credenciales de acceso de funcionarios y contratistas del Estado.

Descripción:

Esta táctica, conocida como propagación lateral por compromiso de confianza, es particularmente efectiva debido a su naturaleza cíclica: el ataque inicia cuando un funcionario recibe un correo electrónico que aparenta ser una notificación legítima de Microsoft; una vez que la víctima ingresa sus credenciales en el sitio fraudulento, los atacantes toman control total de su buzón institucional. A partir de ese momento, la cuenta comprometida se convierte en un nuevo foco de infección, enviando automáticamente los mismos correos de alerta a todos sus contactos internos y a otras entidades con dominios .gov.co. Esto genera una cadena de engaño donde el receptor confía plenamente en el remitente al tratarse de un compañero o una entidad oficial conocida, lo que facilita que la campaña se extienda rápidamente por toda la red gubernamental.

Modo de explotación y cadena de infección

La campaña comienza cuando un usuario recibe un correo electrónico que parece ser una alerta de seguridad legítima de Microsoft. Este correo utiliza la urgencia y un remitente que parece oficial para engañar al usuario.

El asunto suele referirse a "Verificación de cuenta", "Actualización de seguridad obligatoria" o "Suspensión de servicios de correo".

De: [redacted]@supersalud.gov.co>
Enviado: lunes, 9 de febrero de 2026 5:20 a. m.
Para: [redacted]@cancer.gov.co>
Asunto: Requerimiento de verificación de cuenta.

No suele recibir correo electrónico de [redacted]@supersalud.gov.co. Por qué es esto importante

Microsoft

[redacted]

Estimado/a usuario/a [redacted]@cancer.gov.co

Como parte de nuestros controles de seguridad, es necesario validar la titularidad de la cuenta **jdrodriguezr@cancer.gov.co** mediante un proceso de verificación obligatorio.

Para continuar con el uso normal del servicio, le solicitamos completar el procedimiento a través del siguiente enlace:

👉 [confirmacion-micr0.wixsite.com/login]

La verificación deberá realizarse **antes del 09 de febrero del 2026**. En caso contrario, podrían aplicarse restricciones temporales de acceso por motivos de seguridad.

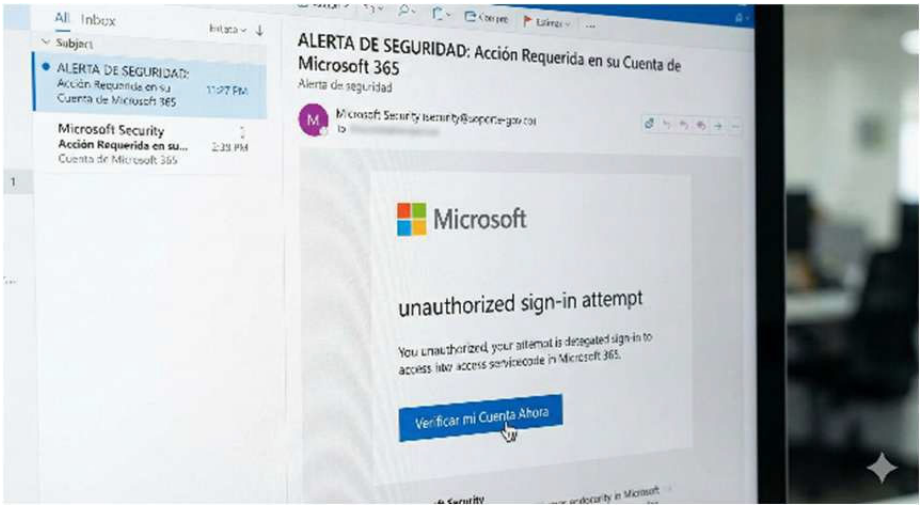
Atentamente,
Área de Seguridad de la Información

Departamento de Soporte Técnico

[redacted]

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Al hacer clic en el enlace del correo (Enlace Malicioso), el usuario es redirigido a una página de inicio de sesión que imita perfectamente la de Microsoft 365. El objetivo es que el usuario ingrese sus credenciales en este sitio fraudulento.



URL detectada: **verificacion-micue[.]wixsite[.]com/login**

Captura de Credenciales: Una vez que la víctima ingresa su usuario y contraseña, los atacantes obtienen acceso inmediato para realizar movimientos laterales dentro de la red institucional.

La Propagación: Con las credenciales robadas, el atacante toma el control de la cuenta de correo de la víctima. Utiliza esta cuenta legítima para enviar automáticamente el mismo correo de phishing a todos los contactos de la víctima, o a otras cuentas del sector gubernamental propagando la campaña y aumentando su alcance.

Recomendaciones para usuarios

- Verificar la URL: Antes de ingresar cualquier contraseña, asegúrese de que la dirección en la barra del navegador sea exactamente **https://login.microsoftonline.com.**
- Desconfiar de la urgencia: Microsoft nunca solicitará cambios de contraseña o verificaciones mediante servicios de hosting gratuitos como Wix, Weebly o Webcindario.
- Reportar: Si recibe un correo sospechoso, incluso si viene de un compañero o entidad conocida, no haga clic y reportarlo al equipo de seguridad de la entidad.
- Mantener MFA activo: Es mandatorio habilitar y mantener la Autenticación de Múltiples Factores (MFA), preferiblemente mediante la aplicación Microsoft Authenticator.
- Esta campaña es especialmente peligrosa porque utiliza la confianza entre entidades del Estado. Si se detecta que un usuario ingresó sus datos en un sitio sospechoso, reportar a la mesa de ayuda de su entidad inmediatamente, y realizar el cambio de la contraseña.