

Boletín de Ciberseguridad

Septiembre 09 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	no se evidencia
Cuenta de correo del remitente:	rogermop1@hotmail.com
TLP:	BLANCO

Registro grafico relacionado con el Phishing

Cuenta Microsoft

Estimado Usuario: rogermop1@hotmail.com

Lamentablemente le informamos que su cuenta de correo electrónico esta apunto de ser bloqueada debido al uso inadecuado de la bandeja de entrada

Si quiere seguir usando nuestros servicios y beneficios debe hacer una validación de datos.

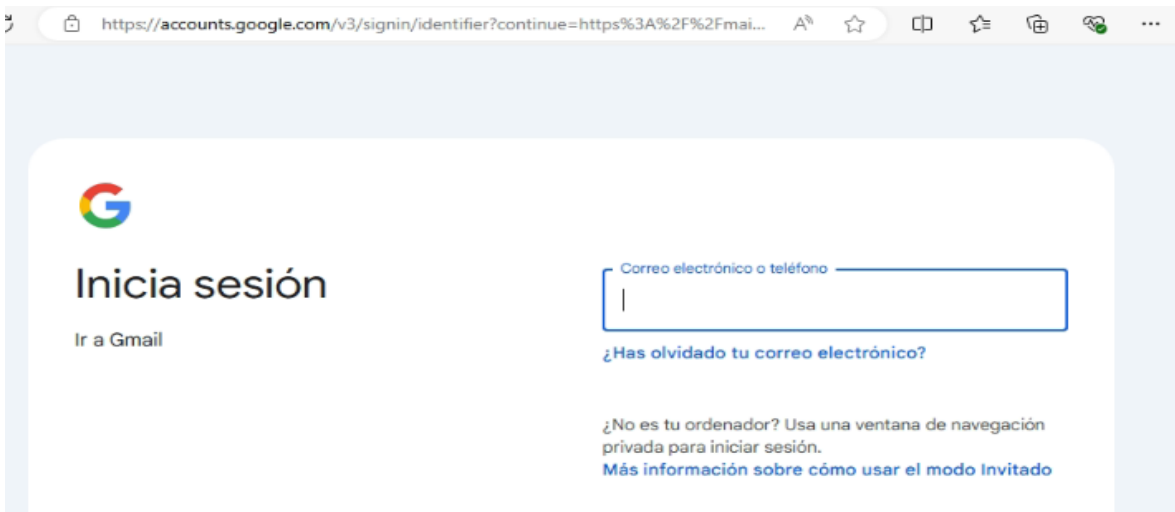
En el siguiente enlace ingrese su dirección de correo electrónico y contraseña de seguridad actual para seguir con los beneficios.

validmymail8.webcindario.com

Usted cuenta con 12 horas para la verificación de su correo electrónico, si ignora este comunicado se le bloqueara definitivamente su correo electrónico sin su consentimiento.

Gracias

El equipo de cuentas de Microsoft 2024@.



El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, bajo la modalidad de Smishing, donde se recibe un correo, para que el receptor tome contacto con una supuesta entidad con el fin de obtener contraseñas, números de tarjetas de crédito o información personal.

Boletín de Ciberseguridad

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Por lo cual se recomienda no ingresar sus Credenciales, cuando lleguen mensajes de una supuestamente **Asesor Digital Ordonez** donde adjuntan unas imágenes las cuales redirigen.

Pero esta te redirecciona a esta página

<https://accounts.google.com/v3/signin/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3D2%26ik%3D4a5f54ecae%26attid%3D0.1%26permmsgid%3Dmsg-f%3A1809728434583561841%26th%3D191d726c4346e671%26view%3Datt%26disp%3Dsafe%26realattid%3D191c23cd0174cff311&emr=1&ifkv=Ab5oB3q2mYcgLTwCjuHzmjAZMPKogYJIE-mBw-8f5gV980xohT1TwvJcOPZ408XbNy0SlaDZza7vYw<mpl=default<mplcache=2&osid=1&passive=true&rm=false&scc=1&service=mail&flowName=GlifWebSignIn&flowEntry=ServiceLogin&dsh=S-1038038591%3A1725898140361951&ddm=0>

como se ve en la imagen la cual es completamente diferente. La cual pide credenciales de GMAIL con el fin de poder robar su información.

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

Correo electrónico: csirt@unad.edu.co

(+57 1) 344 37 00 Ext. 1042516