

# El hackeo a PAMI afecta a millones de usuarios: qué hacer para evitar estafas

9 agosto, 2023



Fue atacada por un virus que cifra la información y luego pide rescate.

Los hackeos a los entes estatales no son una novedad, pero el último, que tuvo como víctima a PAMI, **complica a millones de usuarios de todo el país y no se descartan posibles estafas a partir de la información que fue robada.**

El responsable del daño es el ransomware **Rhysida**, un malware que **cifra los archivos y los vuelve inaccesibles a menos que se pague una suma de dinero para obtener la clave que los descifre.**

Lo importante, además de saber cuándo se va a resolver el problema (hay quienes dicen que la restauración total llevará semanas y hasta meses) es informar que **se pueden haber**

filtrado datos de empleados, prestadores y/o afiliados de la obra social de los jubilados.

Normalmente, el modus operandi de los hackers es poner en venta en foros de ciberdelincuencia o redes sociales los datos robados. Se usan, principalmente, para las campañas de phishing o suplantación de identidad.

Usando los datos de las personas, envían mails ficticios (similares a los oficiales) o hacen llamados haciéndose pasar un banco o prestador donde la víctima tenga algo contratado.

Según publicó el diario *Clarín*, desde PAMI les aseguraron que el hackeo “fue mitigado”, que “no hay amenaza alguna de los datos de los afiliados”, que la atención (turnos, entrega de medicación en farmacias) funcionan “con normalidad”. Sostuvieron que los pagos “están garantizados” y que las licitaciones seguirán los “circuitos de compras normales, publicados en el Boletín Oficial”. Además, afirmaron que ya hicieron la denuncia “ante la UFI PAMI”.

## Qué hacer si sos afiliado a PAMI

Aun sin una comunicación oficial de la obra social de los jubilados, es importante alertar a la población para evitar caer en estafas.

Los afiliados deben estar atentos a los llamados y correos electrónicos o comunicaciones oficiales que puedan recibir por parte del organismo.

Aunque pueda parecer oficial, es de vital importancia chequear todo lo que se reciba en nombre de PAMI.

Por ello, los expertos en ciberdelito recomiendan desconfiar de los llamados que digan ser del PAMI aunque tengan información nuestra. Leer con detalle los correos electrónicos, el remitente debe ser @pami.org.ar.

Ante cualquier duda comunicarse con las vías oficiales de PAMI. Si se recibe un llamado o correo no dar ningún tipo información ni compartir contraseñas.

Los canales habilitados por PAMI son: la línea 138, el número de teléfono 0800-222-7264 y el WhatsApp oficial: 11 4370-3138.

Fuente: El Sol Diario