El riesgo de ver el Mundial 2026 por streaming: alertan por páginas falsas para robar datos

11/06/2026

El comienzo del **Mundial 2026** no solo moviliza a millones de fanáticos alrededor del mundo. También genera una oportunidad para los **ciberdelincuentes**, que aprovechan el interés masivo por los partidos para desplegar campañas de **fraude digital** dirigidas a usuarios que buscan transmisiones gratuitas por Internet.

Especialistas en ciberseguridad advirtieron que durante los grandes eventos deportivos suelen multiplicarse las páginas falsas que imitan plataformas de streaming con el objetivo de obtener información personal, contraseñas y datos bancarios.

Según los expertos, detrás de una supuesta **transmisión gratuita** puede esconderse una operación diseñada para robar

información sensible o infectar dispositivos con **programas maliciosos**.

La advertencia fue difundida por la empresa Kaspersky, que alertó sobre el aumento de este tipo de maniobras en un contexto donde muchas personas intentan acceder a los encuentros mediante enlaces compartidos en redes sociales, aplicaciones de mensajería o sitios web desconocidos.

Cómo funcionan las estafas vinculadas al Mundial 2026

Los ataques suelen comenzar con anuncios patrocinados, publicaciones en redes sociales o mensajes enviados por **WhatsApp**, Telegram y otras aplicaciones.

La búsqueda de partidos del Mundial 2026 en sitios no oficiales puede exponer a los usuarios al robo de datos personales y bancarios.

Los delincuentes crean páginas que imitan la apariencia de plataformas reconocidas de **streaming deportivo** o de servicios que supuestamente cuentan con autorización para transmitir los

partidos del Mundial.

Las promesas suelen ser similares: acceso gratuito, transmisiones en vivo en alta definición, pruebas sin costo o enlaces exclusivos para ver encuentros sin necesidad de pagar una suscripción.

Cuando la víctima ingresa al sitio, se encuentra con **una página que parece auténtica**. Allí se le solicita crear una cuenta, completar formularios o ingresar datos personales para habilitar el acceso al contenido. En algunos casos, también se pide información financiera bajo la excusa de activar una **prueba gratuita** o verificar la identidad del usuario.

El objetivo real es obtener datos bancarios, credenciales de acceso y otra información valiosa que luego puede utilizarse para cometer fraudes.

Existen además campañas que intentan convencer a los usuarios de descargar aplicaciones, reproductores multimedia o extensiones para navegadores. Esos archivos pueden contener **software malicioso**, capaz de recopilar información almacenada en el dispositivo o monitorear la actividad de la víctima.

Por qué estos engaños resultan tan efectivos

Los especialistas explican que buena parte del éxito de estas campañas se basa en la combinación de ingeniería social y diseño visual convincente. Los sitios fraudulentos suelen **copiar logotipos**, colores, imágenes y estructuras similares a las utilizadas por servicios legítimos, lo que dificulta detectar el engaño a simple vista.

Además, muchos usuarios toman decisiones rápidas cuando intentan encontrar una transmisión pocos minutos antes del inicio de un partido.

Según datos difundidos por Kaspersky, el **39% de los latinoamericanos** no sabe identificar correctamente una página web falsa, mientras que otro grupo importante manifiesta dificultades para verificar si un sitio es auténtico incluso cuando sospecha que podría tratarse de una estafa.

Leandro Cuzzo, analista de seguridad del equipo global de investigación y análisis de la compañía, advirtió que durante el torneo millones de personas buscarán transmisiones de último momento, una situación que suele ser aprovechada por los atacantes.

De acuerdo con el especialista, muchas de estas páginas están diseñadas específicamente para recopilar **credenciales de acceso**, información personal o datos financieros, mientras que otras distribuyen programas capaces de comprometer la seguridad de los dispositivos.

Las recomendaciones para evitar caer en la trampa

Frente a este escenario, los expertos recomiendan utilizar únicamente **plataformas oficiales** para acceder a las transmisiones del Mundial. También aconsejan evitar enlaces compartidos por desconocidos o difundidos en redes sociales sin verificar previamente su origen.

Otro aspecto fundamental consiste en **revisar cuidadosamente la dirección web** antes de ingresar información personal. Los sitios fraudulentos suelen modificar una letra, agregar palabras extrañas o utilizar dominios muy similares a los originales para generar confusión.

Si existe alguna duda sobre la autenticidad de una página, lo más recomendable es cerrar el sitio e ingresar manualmente a la plataforma oficial desde el navegador.

Los especialistas también sugieren **no descargar aplicaciones**,

extensiones o reproductores multimedia ofrecidos por páginas desconocidas. Cuando un portal solicita instalar software para desbloquear una transmisión o mejorar la calidad del video, puede tratarse de una maniobra destinada a infectar el dispositivo.

Por último, recomiendan mantener actualizado un **software de seguridad** capaz de detectar intentos de phishing, páginas fraudulentas y otras amenazas digitales antes de que el usuario interactúe con ellas.

Con millones de personas pendientes del **Mundial 2026**, la competencia no solo se jugará dentro de la cancha. En Internet también habrá que estar atentos para evitar que una búsqueda apresurada termine convirtiéndose en **estafas**.

Fuente: La Mañana de Neuquén.