Las estafas están a la orden del día en Facebook Messenger

Un tentador mensaje supuestamente llegado de un amigo les está amargando la vida a los Facebook Messenger. “Mira lo que encontré” (“Look what I found”) es el asunto de la comunicación, que no esconde más que el enésimo ataque de phishing o suplantación de identidad.

Lo más peligroso que los ciberdelincuentes consiguen transformar el remitente en contactos de la potencial víctima, que anteriormente han caído en la trampa a través de la misma vía o similares, informó 7News.

Además de la sugerente invitación, los mensajes suelen ir acompañados de uno o varios emojis, además de un enlace. Visitar el link implica la visita a una “página web maliciosa que exige al usuario las credenciales de acceso a Facebook”, detalló la versión. Aparte del intento por obtener la información sensible, también podría intentar instalar malware en el dispositivo.

“La estafa se conoce desde hace varios años, pero recientemente parece estar proliferando de forma exponencial”, complementó la estación televisiva australiana. Algo parecida está ocurriendo con otra comunicación titulada “¿Eres tú la persona del video”, que emplea una estrategia muy similar para hacerse de los datos de la misma red social.

Leslie Sikos, experto en ciberseguridad de la Universidad Edith Cowan, explicó que los mensajes aparentemente provenientes de amigos o contactos de Facebook “tienen muchas más probabilidades” de terminar en un clic, a diferencia de lo que puede ocurrir con un emisor desconocido. “La gente puede centrarse solo o principalmente en el nombre del remitente, en lugar del contenido del mensaje, independientemente de que este parezca sospechoso”, contó.

Por desgracia, hay tantas estafas de este tipo, que es complejo establecer un patrón para evitar caer en el fraude. De todos modos, hay elementos comunes que los criminales suelen demostrar. “No hay un saludo apropiado o una firma que coincida con el estilo del remitente (…) Las estafas suelen tener un uso inapropiado de la gramática o errores tipográficos que también pueden indicar su verdadera naturaleza”, subrayó.

También sugirió observar los nombres de dominios falsos,

analizar si ese contacto en la red social podría en la vida real compartir contenido sensible e incluso la hora en envío.

Con información de Digital Trends