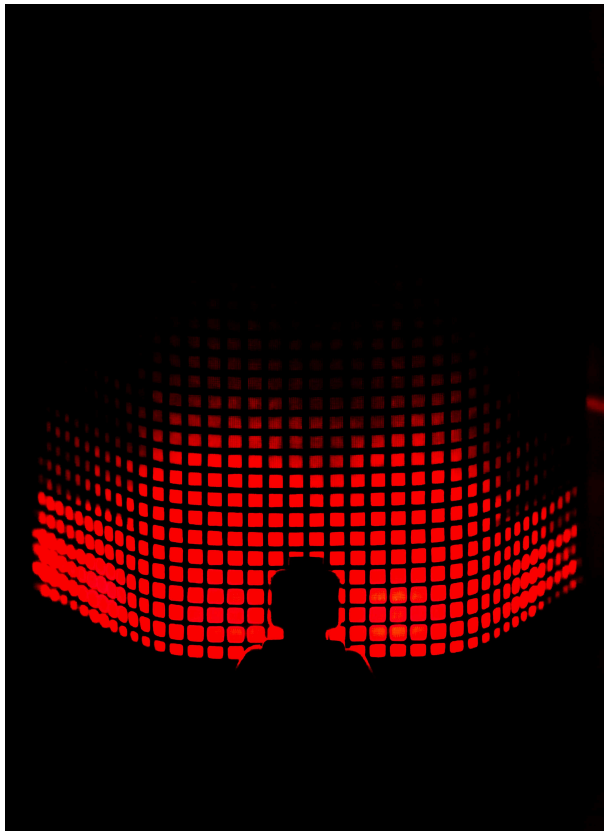

México es el país
en donde se recibieron más
correos maliciosos en 2020
mexis
aggity

El trabajo a distancia contribuyó a que se intentaran los ataques de este tipo

En 2020, año marcado por la pandemia, la transición masiva al teletrabajo y la comunicación en línea, el internet se convirtió en la mejor herramienta para mantener nuestras actividades. Además de un mayor tiempo de conexión, otro de los puntos que demuestran el impacto de conectividad en el mundo es el aumento de campañas de spam y phishing.



Todo el mundo estuvo expuesto a ello pero México destaca en términos de correos maliciosos.

Como era de esperarse, los ciberdelincuentes utilizaron al máximo el tema de **Covid-19** como un cebo para sus campañas, y todo apunta a que esta tendencia se mantenga en 2021. **En ese sentido expertos advierten que es previsible un aumento de ataques dirigidos al sector empresarial este año ya que el teletrabajo genera mayor vulnerabilidad en los empleados.**

Asimismo, la compañía de ciberseguridad alertó que los usuarios de sistemas de mensajería deben mantenerse alerta, ya que es probable que también se incremente la cantidad de spam y phishing dirigido a dispositivos móviles.

México en peligro

De acuerdo con un estudio de Spam y Phishing 2020, México pasó del penúltimo lugar en el Top 10 mundial al séptimo puesto, situándose a la cabeza de los países latinoamericanos receptores de correos maliciosos,

es decir aquellos que contienen archivos adjuntos maliciosos o enlaces a sitios de phishing.

Según la investigación, que toma en consideración los datos anuales, el 3.34% de los usuarios que recibieron este tipo de mensajes en su correo electrónico eran mexicanos. A nivel regional, le sigue de cerca Brasil con **3.33%.** El Top 3 global está encabezado por España **(8.48%),** Alemania **(7.05%)** y Rusia **(5.87%).**

Sin embargo, también destacó que **el año pasado, la proporción de spam sobre el tráfico de correo global disminuyó en comparación con el año anterior** lo que explican debido a la transición hacia el teletrabajo y, en consecuencia, a un aumento en el volumen de correspondencia legítima.

Consejos para mantenerse protegido.

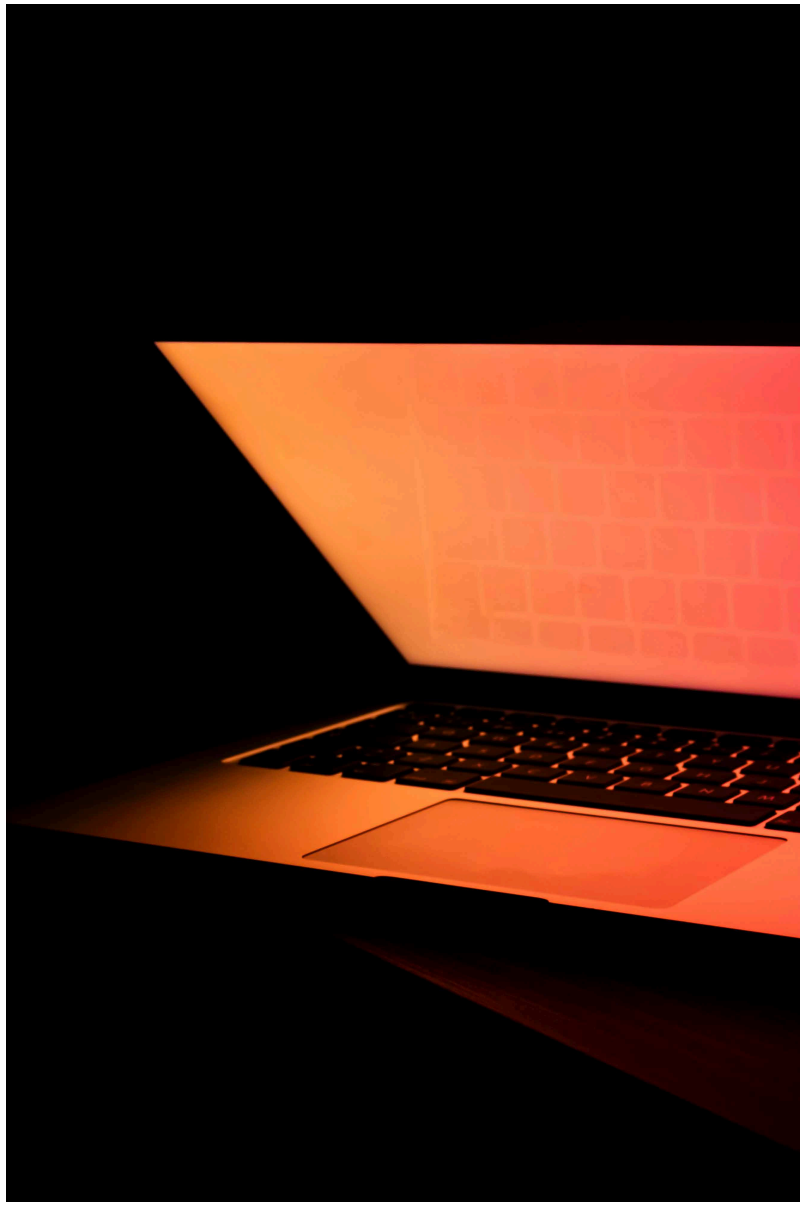
Presta mucha atención y no abras ningún archivo o adjunto sospechoso recibido de fuentes desconocidas. **Revisa el formato de la URL y la ortografía** del nombre de la empresa antes de descargar cualquier archivo. Los sitios web falsos pueden parecerse a los reales, pero habrá anomalías que le ayudarán a detectar la diferencia.

No descargues e instales aplicaciones de fuentes no fiables.
No hagas clic en ningún enlace recibido de fuentes desconocidas y en anuncios online sospechosos.

Crea contraseñas fuertes y únicas, incluyendo una mezcla de letras minúsculas y mayúsculas, números y puntuación, y activa la autenticación de dos factores.

Instala siempre las actualizaciones. Algunas de ellas pueden contener correcciones de problemas críticos de seguridad.
Ignora los mensajes que solicitan la desactivación de los sistemas de seguridad para el software de oficina o el software antivirus.

Utilice una tecnología de seguridad robusta apropiada para tu sistema y dispositivos.



Fuente de información:
Eluniversal.com