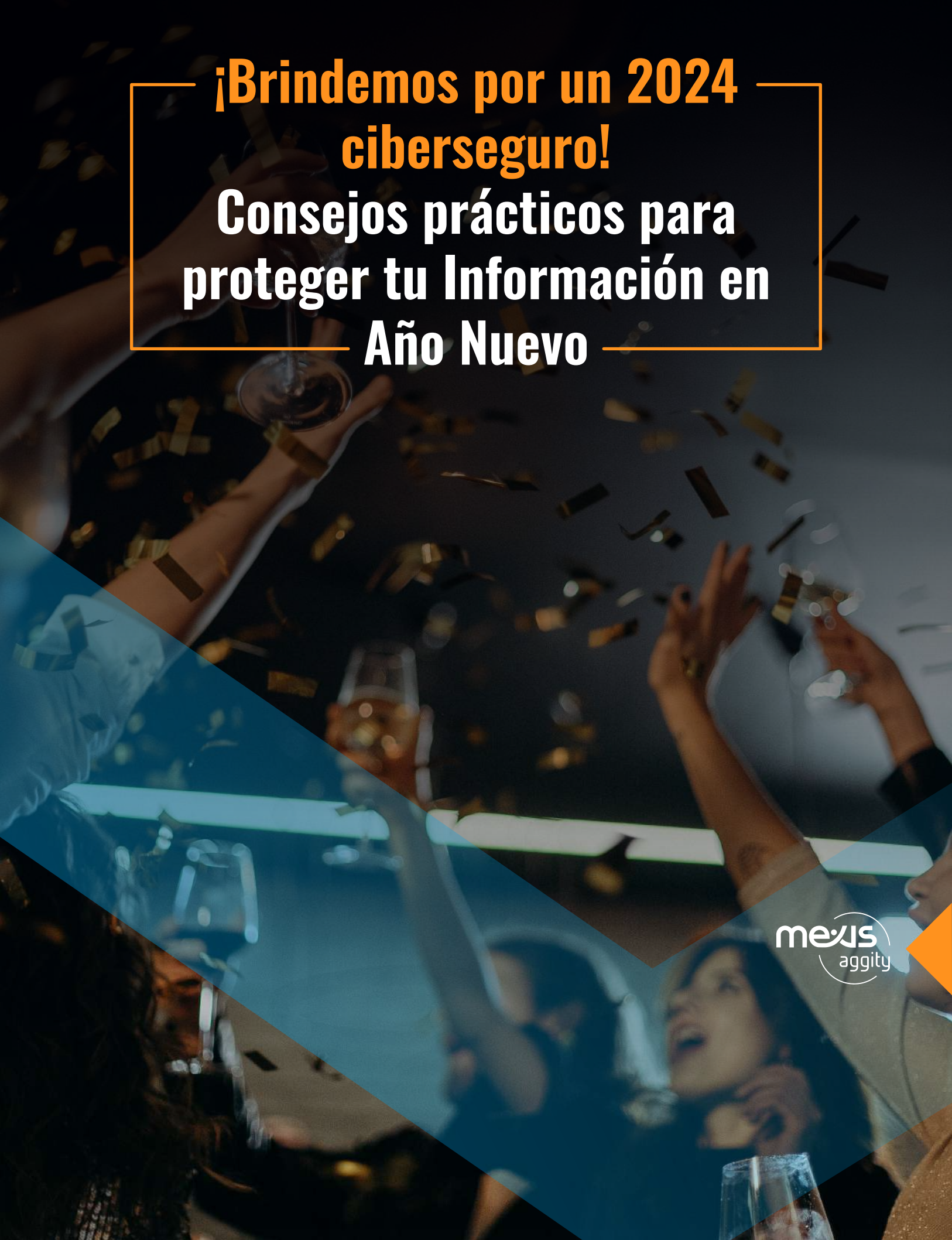

¡Brindemos por un 2024 ciberseguro!

Consejos prácticos para proteger tu Información en Año Nuevo

mexis aggity

Para el año que llega, el compromiso de mejorar nuestra ciberseguridad debería ser una meta necesaria y realizable.

Como sucede cada diciembre, se va acercando el Año Nuevo y **todos hacemos un balance del año que dejamos atrás, pero también nos planteamos una serie de metas que queremos cumplir** en el que está por arrancar: mejorar nuestros hábitos alimenticios, ir al gimnasio, estrechar nuestros vínculos familiares o pasar más tiempo al aire libre. La lista es larga. Aunque no tan recurrente ni tan glamorosa como las anteriores, **el compromiso de mejorar nuestra ciberseguridad debería ser una meta necesaria y realizable en este inminente 2024.**

Seguramente habrás escuchado de algún conocido -si no es que te sucedió a vos mismo- al que le hackearon el teléfono este año o al que le llegaron en el resumen de la tarjeta compras que nunca realizó.

¿Qué podemos hacer para arrancar el año protegidos?

Aunque en principio parece difícil e incluso costoso, la realidad es que nuestra seguridad digital depende de que mantengamos ciertos hábitos sencillos pero constantes a través del tiempo. ¿Cuáles son?

El primer hábito es el más conocido de todos: establecer contraseñas que sean seguras. Esto quiere decir que contengan letras mayúsculas, minúsculas, números y símbolos. Pero sobre todo, y esto es muy importante: que no se repita en más de una cuenta.

El segundo tiene que ver con el doble factor de autenticación. Esto quiere decir que debemos adoptar una verificación de al menos dos pasos siempre que sea posible, ya sea un pin numérico, huella digital u otra autenticación biométrica. Aunque parece engorroso, es increíble lo que podemos proteger nuestra identidad digital agregando un solo paso más.

La tercera recomendación requiere realmente la incorporación de un hábito y tiene que ver con el compromiso de no compartir información innecesaria por correo electrónico o chat, especialmente archivos o links. Esta es la mejor manera de cortar una cadena de desinformación que puede terminar derivando en un ataque malicioso hacia nosotros mismos o terceros. **La clave: revisar y validar la procedencia y veracidad de los hipervínculos o archivos que estamos por reenviar.** Si al hacer esto dudamos, la mitad del trabajo ya está hecho.

La cuarta pauta tiene que ver con proteger nuestra información en internet. Evitemos en la medida de lo posible llenar encuestas gratuitas o formularios para obtener algo que es supuestamente sin costo, porque la moneda de cambio en esos casos son siempre nuestros datos personales.

Por último, evitemos la tentación de colgarnos de redes de wifi públicas. Y si estamos de viaje y no tenemos servicio, que es la situación más común, informémonos previamente sobre el uso de una VPN que proteja nuestra conexión.

Dicho todo esto, **¡alcemos nuestras copas y brindemos por un 2024 más seguro y libre de fraudes informáticos!**

Fuente de información: www.infobae.com