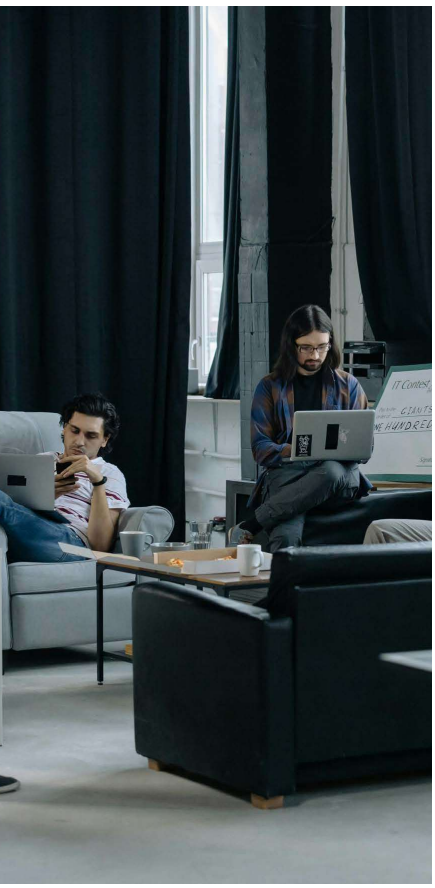
www.mexis.net

RIESGOS CIBERNÉTICOS
DE LOS ESPACIOS DE COWORKING

mexis aggity



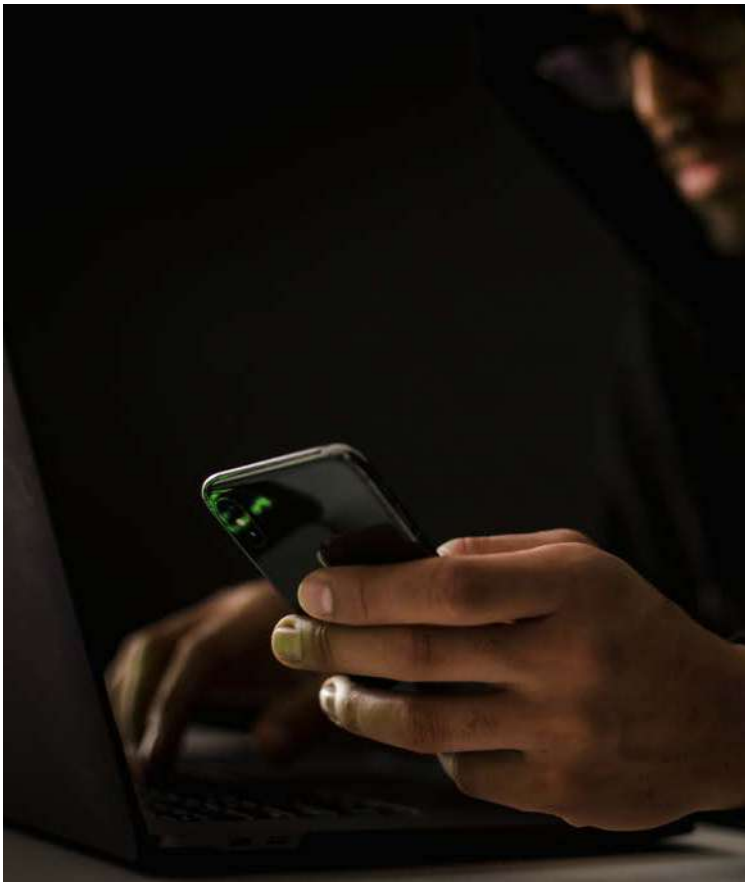
Los espacios de coworking son ambientes muy colaborativos. Lugares donde freelancers, emprendedores, y empleados de grandes corporaciones, encuentran flexibilidad y oportunidades de networking en un entorno compartido y dinámico.

Sin embargo, este mismo diseño abierto y colaborativo, que hace de los espacios de coworking lugares tan atractivos para trabajar, los expone a su vez a una serie de riesgos cibernéticos. Con el acceso libre a las redes Wi-Fi compartidas, las vulnerabilidades son abundantes y los riesgos muy reales.

La privacidad de datos, la protección contra el acceso no autorizado, y la integridad de la información se convierten en preocupaciones para los usuarios de los espacios de coworking. Por lo tanto la ciberseguridad debe ser una prioridad en la infraestructura de cualquiera de estos espacios. Pero también es importante proteger nuestros equipos, por ejemplo, **con el uso de herramientas como una VPN prueba gratis que cifran la comunicación de datos, y garantiza que la información sensible permanezca inaccesible para los ciberdelincuentes.**

Vulnerabilidad a ataques cibernéticos en espacios de coworking

En un espacio de coworking típico, encontramos todo tipo de personas. Desde emprendedores tecnológicos que podrían estar desarrollando software avanzado, hasta creativos que quizás no tengan un conocimiento técnico profundo en seguridad informática. **Estos usuarios pueden además utilizar una variedad de dispositivos y sistemas operativos.** Lo que complica aún más la gestión y protección de la red, ante la falta de estándares uniformes en cuanto a la seguridad.



El uso de redes Wi-Fi compartidas, común en los espacios de coworking, es particularmente problemático. Estas redes son susceptibles a una variedad de ataques, incluidos aquellos que interceptan los datos transmitidos entre los usuarios y el punto de acceso, **como los ataques de «man-in-the-middle«.**

Principales riesgos cibernéticos

En los espacios de coworking, el acceso físico suele ser menos restringido en comparación con entornos de oficina tradicionales, lo que permite un flujo constante de personas. La falta de control en estos casos puede llevar a situaciones donde los dispositivos no supervisados se conviertan en puntos de entrada para ataques de seguridad. **Permitiendo a los piratas informáticos acceder a sistemas desprotegidos o dejar hardware de vigilancia, como USBs con malware.**

La naturaleza abierta de los espacios de coworking también puede comprometer la privacidad de los datos. Por ejemplo, si un freelancer utiliza una impresora compartida para imprimir documentos confidenciales, podría dejar inadvertidamente información sensible a la vista de otros.

Entonces las amenazas a la seguridad en espacios de coworking pueden originarse tanto interna como externamente:

- **Amenazas internas:** Incluyen empleados o usuarios regulares que pueden, intencionalmente o por negligencia, comprometer la seguridad de la red o los datos.
- **Amenazas externas:** Como hackers y phishers que se dirigen a redes de coworking para explotar vulnerabilidades y obtener acceso no autorizado.

Tecnologías y estrategias para mitigar riesgos

Tomarse en serio la seguridad y mitigar riesgos en los espacios de coworking, es una necesidad si las empresas quieren defender a los usuarios, y las propias instalaciones, contra cualquier tipo de amenaza cibernética y/o física. Y para ello, algunas de las soluciones más efectivas que se pueden adoptar son:

Reconocimiento de huellas dactilares y facial

Los sistemas biométricos ofrecen métodos de autenticación más seguros y personales que las contraseñas tradicionales o las tarjetas de acceso. El reconocimiento de huellas dactilares y facial proporciona un control de acceso robusto y difícil de falsificar, ya que cada individuo posee características únicas e intransferibles. **Estos sistemas previenen el acceso no autorizado a los espacios de coworking.** Y a la vez, permiten mantener un útil registro detallado de quién entra y sale.

Vigilancia y monitoreo mejorados por IoT

El Internet de las Cosas (IoT) ha introducido una nueva dimensión en la vigilancia y el monitoreo de seguridad. **A través del desarrollo de cámaras inteligentes y sensores distribuidos estratégicamente, es posible mantener una vigilancia constante de cualquier espacio físico.** Estos dispositivos son capaces de detectar movimiento inusual, acceder a registros de tiempo real y enviar alertas automáticas a los administradores en caso de actividades sospechosas. A su vez, la integración con análisis avanzados permite que estos sistemas analicen los eventos grabados, **siendo capaces de identificar patrones de comportamiento inusuales o potencialmente peligrosos.**

Asegurando el futuro de los espacios de coworking

Es innegable que los espacios de coworking ofrecen beneficios a sus usuarios, pero es igual de cierto que los expone a riesgos cibernéticos. Esta situación pone a estos espacios en una situación complicada, pero por suerte, no es insuperable. L**os gestores deben implementar estrategias de seguridad avanzadas y adaptables, como el reconocimiento biométrico, y sistemas mejorados de vigilancia para proteger los datos y la privacidad de los usuarios, sin olvidar fortalecer la integridad física del espacio.**

La inversión en tecnologías de seguridad y la implementación de prácticas de gestión robustas son la base para cultivar un ambiente de coworking donde la seguridad y la colaboración se complementen mutuamente.

Fuente de información: revistabyte