¿Cómo concientizar a los trabajadores en ciberseguridad?

Managed secure IT | no matter what

Cuando un dispositivo personal de cualquier empleado es comprometido, éste se convierte en un gran riesgo para su empresa. De acuerdo a un estudio el cual indica que el malware basado en Android actualmente representa el **14% de todas las ciberamenazas,** además los ataques dirigidos, las campañas de phishing y los puntos de acceso maliciosos continúan creciendo exponencialmente.

Por ello es fundamental que se establezca un programa de concientización sobre ciberseguridad que le brinde a los empleados información sobre cómo mitigar y evadir estos riesgos.

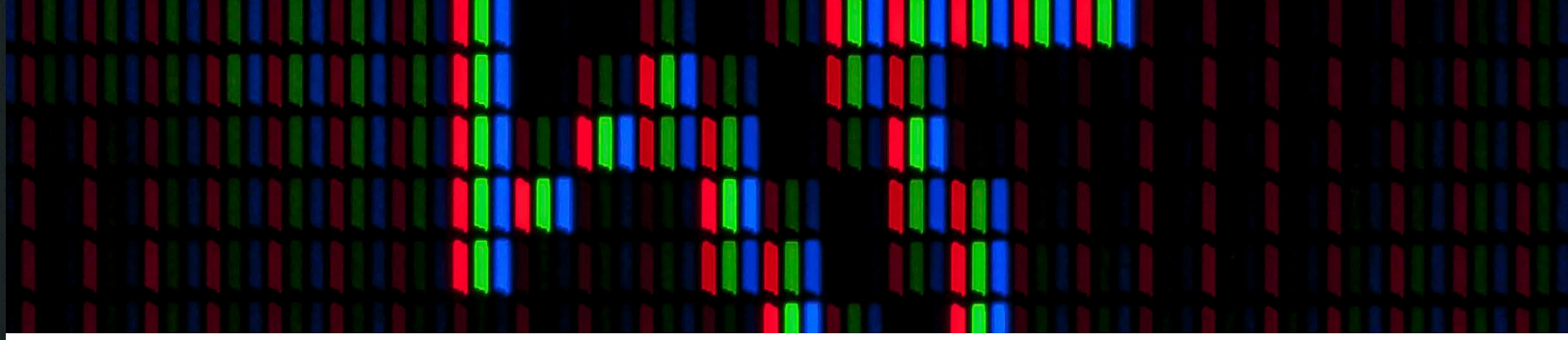
Primero, deben tener cuidado de las redes WiFi públicas debido a que los delincuentes a menudo utilizan sus dispositivos como puntos de acceso públicos en lugares comunes. Cuando un usuario se conecta, el delincuente puede interceptar todos los datos trasmitidos entre la víctima y su sitio de compras en línea o su banco.

Muchos dispositivos inteligentes también buscan automáticamente puntos de conexión conocidos, como el **WiFi** de casa. Los ataques más recientes observan este comportamiento y simplemente preguntan al dispositivo qué está buscando. Para evadir este problema, es una buena práctica que los usuarios desactiven su conexión de **WiFi** y Bluetooth hasta que la vuelvan a necesitar.

Otro punto clave que debe integrar el programa es el uso de la misma contraseña para todas las cuentas en línea. El problema con esta tendencia es que si un delincuente logra interceptar esa contraseña, tendrá acceso a todas las cuentas del usuario. La mejor opción es utilizar un sistema de gestión de contraseñas que solicite al usuario solo tener que recordar una contraseña para acceder a las demás. Por lo tanto, es muy importante garantizar que esta contraseña sea especialmente segura y fácil de recordar.

También es importante reconocer los ataques de phishing que llegan por correos electrónicos o publicados en sitios web ya que siempre habrá un usuario que no podrá resistirse a abrir un correo, descargar un archivo o hacer clic en un enlace de un sitio web. Cualquier iniciativa educativa debe complementarse con soluciones eficaces de seguridad para **correo electrónico y firewall** de aplicaciones web que puedan detectar spam y phishing, validar enlaces y ejecutar archivos en un sandbox.

Los usuarios también deben tener un sistema de seguridad aprobado por su empresa, instalado en cualquier dispositivo con acceso a recursos corporativos y actualizado con frecuencia. Además es importante mantener constante monitoreo de las redes sociales y activar rigurosos controles de privacidad para evitar ser víctima de un ciberataque.



Aunque es esencial desarrollar una estrategia de seguridad completa y eficaz para los usuarios que tienen dispositivos personales conectados a la red, es importante no agobiar a los empleados con grandes cantidades de información.

Se debe dividir la información en secciones digeribles, dar un consejo de seguridad diario, publicar mensajes alrededor de la oficina como en los pasillos o en los espacios comunes, permitir que el comité ejecutivo lo mencione en las reuniones internas, y por último, realizar comprobaciones o inspecciones, así como sus propios correos de phishing, para identificar a los usuarios que puedan necesitar asistencia adicional.

Fuente de información:
www.infochannel.info