El regreso a clases será remoto y así es como debes protegerte de ciberataques

CIUDAD DE MÉXICO. 29 de julio de 2020.- La educación remota, debido a la pandemia por el COVID-19, llegó para quedarse. El pasado jueves 23 de julio, el Secretario de Educación Pública de México, Esteban Moctezuma Barragán, anunció de manera oficial que el regreso a clases se realizará mediante un modelo híbrido, en donde habrá tanto clases a distancia como presenciales, de acuerdo a las necesidades de cada uno de los sistemas educativos.

Algo similar sucederá en otros países de la región, en donde con el fin de mitigar los contagios entre alumnado, docentes y personal de las instituciones educativas en general, las clases permanecerán online.

Por lo anterior, antes de retomar las clases es importante cuidar la seguridad de los equipos de cómputo, tanto de las escuelas como de los alumnos, ya que con la educación remota en la 'nueva normalidad' los ciberdelincuentes se han encargado de actualizar sus técnicas y métodos para propagar ataques a este sector.

Es por eso que Sophos, empresa líder en ciberseguridad de última generación, recomienda estar atento en los siguientes aspectos para contrarrestar los riesgos que la educación en línea conlleva:

1. Utiliza una VPN

Tanto el personal de las escuelas como los alumnos necesitan estar conectados a una red escolar para tener acceso a diversas aplicaciones que utilizarán durante su aprendizaje. Estas herramientas están ubicadas principalmente en la nube, tales como apps para compartir archivos, correo electrónico, entre otras. Es por eso que para acceder de manera segura a esas plataformas, el personal de TI de las escuelas debe implementar una VPN para evitar que los ciberdelincuentes se infiltren dentro de esa red local y tengan acceso a la información que en ella se comparte.

La red privada virtual, o VPN, ofrece un acceso remoto seguro a los usuarios y mantiene cifrados y protegidos los datos que fluyen al interior de esa red. Implementarla es importante porque los estudiantes utilizarán equipos de cómputo propios, y para las escuelas es difícil saber si esas computadoras tienen las actualizaciones y parches de seguridad necesarios, para evitar el acceso a los ciberdelincuentes.

Al mismo tiempo, contar con una VPN ayudará a mantener a los estudiantes a salvo de ciberacoso, contenido inapropiado, y otras amenazas en línea como el malware.

2. Controla el acceso a datos confidenciales

Las escuelas tienen información muy valiosa que se puede vender en la *dark web*, como datos personales de los estudiantes, maestros y personal administrativo, además de datos confidenciales relacionados con investigación o propiedad intelectual. Es fundamental, para esas instituciones, que su personal de TI instale herramientas de acceso a esa información en función de la identidad de cada usuario, para que así solo puedan acceder quienes están autorizados y con permisos limitados de forma personalizada. Para proteger los datos confidenciales, se pueden utilizar soluciones de autenticación de dos factores (2FA), claves del sistema incluidos IPsec, SSL y VPN, así como portales de usuario con acceso mediante contraseña.

3. Educación contra el phishing

El *phishing* es actualmente uno de los riesgos más latentes en cuanto a seguridad cibernética. Los estudiantes, maestros y personal en general de las instituciones, están expuestos a ser manipulados para hacer clic en enlaces maliciosos que pueden proporcionar a los ciberdelincuentes acceso a la red de la escuela y a información de valor. La mejor manera de contrarrestar ese tipo de riesgos es a través de la concientización y capacitación de los usuarios.

Educar y realizar ataques simulados a los usuarios ayuda a facilitar una cultura de conciencia en cuanto a ciberseguridad, de igual forma hace que esas personas sean menos propensas a caer en estafas mediante correo electrónico. Los propietarios de escuelas deben asegurarse de que la seguridad en tu red de correo electrónico interna esté actualizada y de que cuente con protección avanzada en todos sus puntos finales, de modo que estén bien protegidos contra malware, ransomware, exploits y otro tipo de amenazas.

4. Seguridad para móviles

Los dispositivos móviles, como teléfonos celulares y otros, son cada vez más utilizados para el aprendizaje remoto. Es por eso que las instituciones deben proteger las redes de acceso locales para esos equipos, ya que un solo dispositivo desprotegido puede comprometer a toda una red escolar. Con la gran mayoría de esos *gadgets* conectados a internet, se requiere de soluciones de seguridad que ayuden a evitar la descarga de archivos riesgosos y que bloqueen el acceso a sitios web inapropiados, siempre que accedan a la red escolar desde esos dispositivos.

Mantener la seguridad de los usuarios dentro de las redes escolares es fundamental, ya que por tratarse de cientos de personas conectadas a una sola red de información y datos, no se sabe en qué momento los ciberdelincuentes pueden aprovechar alguna vulnerabilidad para

inmiscuirse en dichas redes y robar información sensible para las escuelas, además de que se pone en riesgo el prestigio de cualquier institución al ser atacada por ciberdelincuentes.

####

Sobre Sophos

Como líder mundial en seguridad cibernética de última generación, Sophos protege de las amenazas cibernéticas más avanzadas de la actualidad a más de 400,000 organizaciones de todos los tamaños en más de 150 países. Desarrolladas por SophosLabs -un equipo global de inteligencia de amenazas y ciencia de datos-, las soluciones basadas en la nube y en IA de Sophos aseguran endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las técnicas de ciberataque que están evolución, incluyendo ransomware, malware, exploits, extracción de datos, violaciones de adversarios activos, phishing, entre otras. Sophos Central, plataforma de administración nativa de la nube, integra la cartera completa de productos de última generación de Sophos, incluida la solución de endpoint Intercept X y el firewall de próxima generación XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición hacia la ciberseguridad de próxima generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas administradas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 47,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido, y cotiza en la Bolsa de Londres con el símbolo "SOPH". Más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/