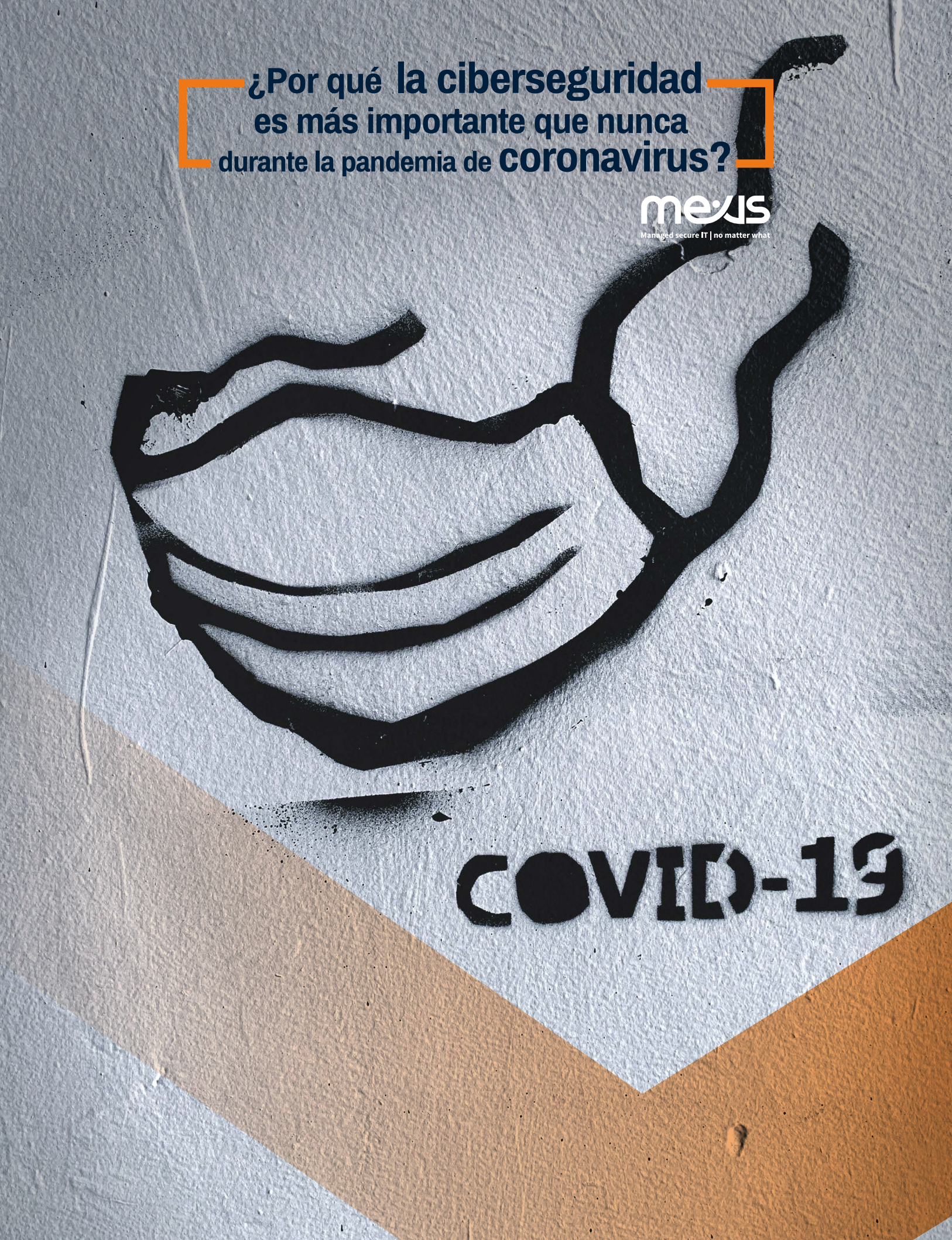
¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus?

mexus®
Managed secure IT | no matter what



¿Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus?

La pandemia COVID-19 plantea el riesgo de un aumento de los ataques cibernéticos.

Los piratas informáticos eligen como blanco la dependencia cada vez mayor de las personas con respecto a las herramientas digitales.

Entre las estrategias para mantener la ciberseguridad se incluyen garantizar continuamente una buena higiene cibernética, verificar las fuentes y mantenerse actualizado sobre las actualizaciones oficiales.

A medida que la pandemia de coronavirus sigue perturbando los sistemas mundiales de salud, económicos, políticos y sociales, hay otra amenaza invisible en aumento en el espacio digital: el riesgo de ataques cibernéticos que se aprovechan de nuestra mayor dependencia de las herramientas digitales y de la incertidumbre de la crisis.

Aquí se enumeran tres razones por las que contar con medidas de seguridad cibernética sólidas es más importante que nunca.

1. Una mayor dependencia de las infraestructuras digitales aumenta el coste del fracaso.

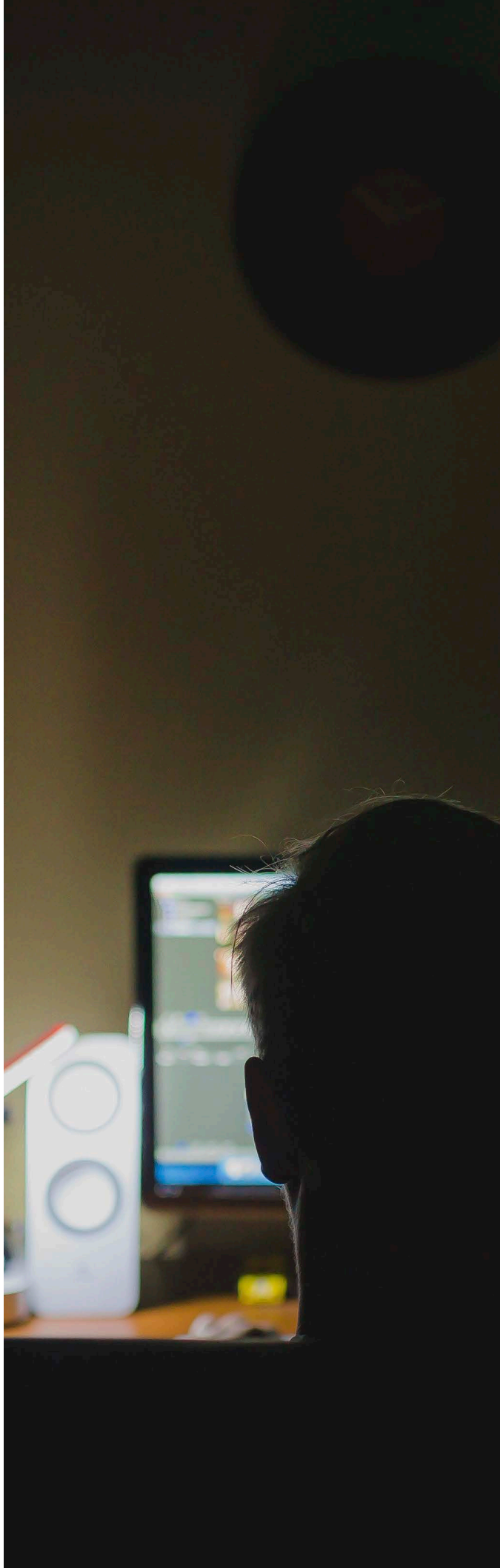
En una pandemia de esta escala, con casos de coronavirus registrados en más de 150 países, la dependencia de las comunicaciones digitales se multiplica. Internet se ha convertido casi instantáneamente en el canal para la interacción humana efectiva y la forma principal en que trabajamos, nos contactamos y nos apoyamos mutuamente.

LAS EMPRESAS Y LAS ORGANIZACIONES DEL SECTOR PÚBLICO ESTÁN OFRECIENDO O APLICANDO CADA VEZ MÁS POLÍTICAS DE (TELETRABAJO), Y LAS INTERACCIONES SOCIALES SE ESTÁN LIMITANDO RÁPIDAMENTE A LAS VIDEOLLAMADAS, LAS PUBLICACIONES EN LAS REDES SOCIALES Y LOS PROGRAMAS DE CHAT.

Muchos gobiernos están difundiendo información a través de medios digitales. Por ejemplo, el Reino Unido ha hecho de la comunicación digital el modo predeterminado de comunicación, instruyendo a los ciudadanos a confiar en los sitios web oficiales para obtener actualizaciones con el fin de evitar inundar los servicios de información telefónica con solicitudes.

En este contexto actual sin precedentes, un ataque cibernético que priva a las organizaciones o familias del acceso a sus dispositivos, datos o Internet podría ser devastador e incluso mortal: en el peor de los casos, los ataques cibernéticos de base amplia podrían causar fallos de infraestructura generalizados que desconecten a comunidades o ciudades enteras, poniendo obstáculos a los proveedores de atención médica, los sistemas públicos y las redes.

Solo en los últimos días, el sitio de estadísticas de Coronavirus Worldometers.info y el Departamento de Salud y Servicios Humanos de EE. UU. han sido objeto de ataques cibernéticos con intención de interrumpir las operaciones y el flujo de información.



2. El delito cibernético se aprovecha del miedo y la incertidumbre.

Los ciberdelincuentes se aprovechan de la debilidad humana para penetrar en las defensas sistémicas. En una situación de crisis, especialmente cuando se prolonga, las personas tienden a cometer errores que de otro modo no habrían cometido. En Internet, cometer un error en cuanto al enlace en el que se hace clic o a la persona a la que confía sus datos puede costarle muy caro.

La gran mayoría de los ataques cibernéticos según algunas estimaciones, el 98% aplica métodos de ingeniería social. Los ciberdelincuentes son extremadamente creativos al idear nuevas formas de aprovecharse de los usuarios y la tecnología para acceder a contraseñas, redes y datos, a menudo sirviéndose de temas y tendencias populares para tentar a los usuarios a tener comportamientos inseguros en línea.

El estrés puede incitar a los usuarios a realizar acciones que se considerarían irracionales en otras circunstancias. Por ejemplo, un ciberataque global reciente se dirigió a personas que buscaban imágenes de la propagación de COVID-19. El malware se ocultó en un mapa que muestra estadísticas de coronavirus cargadas de una fuente en línea legítima. Se pidió a los espectadores que descargaran y ejecutaran una aplicación maliciosa que ponía en peligro el ordenador y permitía a los piratas informáticos acceder a las contraseñas almacenadas.

3. Más tiempo en línea podría ocasionar un comportamiento más peligroso.

Un comportamiento arriesgado en Internet que se tiene de forma inadvertida aumenta si se pasa más tiempo en línea. Por ejemplo, los usuarios podrían caer en el acceso (gratuito) a sitios web oscuros o programas pirateados, abriendo la puerta a posibles ataques y malware.

Del mismo modo, podría haber riesgos ocultos en las solicitudes de información de la tarjeta de crédito o la instalación de aplicaciones de visualización especializadas. Hacer clic en el enlace equivocado o ampliar los hábitos de navegación puede ser extremadamente peligroso y salir muy caro siempre, y especialmente durante la pandemia.

Fuente de información:
https://es.weforum.org/