Diez Consejos para garantizar tu ciberseguridad cuando trabajas en remoto

Nunca antes habíamos dependido tanto de la tecnología, tanto en nuestro trabajo como en nuestra vida personal. Con el aumento de esta dependencia, se incrementan también los riesgos cibernéticos. Además, cuantos más usuarios trabajen o estudien desde casa, mayor es la probabilidad de que se produzcan incidentes cibernéticos.

CHUBB®

Los ciberdelincuentes, son conscientes de que cuando se conectan un gran número de usuarios en red, estos interactúan con la tecnología de diferentes maneras. En ocasiones, para algunos puede ser la primera vez que utilizan un tipo de red o de software. A menudo, los ciberdelincuentes se aprovechan de dichas situaciones, valiéndose del engaño para acceder a todo tipo de información sensible. Al mismo tiempo, los equipos informáticos y operativos de las empresas tienen que dedicar largas jornadas a mantener las redes en continuo funcionamiento, lo que puede afectar a su capacidad de detección de la actividad maliciosa de una forma rápida.

Esto dificulta más que nunca la protección de la información. En Chubb, queremos ir más allá con nuestros clientes y por eso sugerimos posibles maneras de ayudar a prevenir que se produzcan este tipo de problemas. Sigue estos consejos para que tu negocio y tus empleados puedan gozar de la mejor ciberseguridad incluso en épocas de incertidumbre.

Las mejores prácticas para tu empresa

1 Anticípate a problemas de recursos informáticos tanto desde la perspectiva de personal como desde la tecnológica.

Cuando un número elevado de usuarios se conecta en remoto, los servicios de atención al cliente se enfrentan a un volumen enorme de llamadas, por lo que se necesitan más recursos fuera del horario de trabajo habitual. Al mismo tiempo, se ponen a prueba el ancho de banda de la red, la capacidad de almacenamiento de datos y la potencia de procesamiento. A pesar de este aumento de tráfico, la atención a los detalles no puede verse mermada.
Animamos a las empresas a que presten especial atención a este tipo de necesidades, a que preparen un plan para reasignar los recursos en función de la conveniencia, y a que acepten que esta dependencia puede incrementarse con el tiempo.

2 Asegúrate de que tu red, tu software y tus aplicaciones están actualizadas.

Los ciberdelincuentes conocen los puntos débiles de las tecnologías de acceso remoto, y con frecuencia se aprovechan de ellos para acceder a información protegida. Asegúrate de que el software y las aplicaciones están actualizadas y de solventar toda debilidad que estas alberguen.

3 Asegúrate de que los recursos estén en orden antes de que se produzca un incidente.

Las organizaciones deberán asegurarse de que sus planes de continuidad de negocio, sus equipos de recuperación de desastres y sus planes de actuación frente a incidentes cibernéticos estén en orden. Los ciberdelincuentes son conscientes de que la dependencia de la red y su disponibilidad siempre será más vulnerable cuando un gran número de usuarios acceden a ella de forma remota, y lo utilizan a su favor.

4 Comprueba tus políticas actuales y aplica las excepciones de seguridad necesarias.

Cuando los recursos informáticos son insuficientes, es posible que las organizaciones tengan que llevar a cabo determinadas excepciones en políticas, normativas o prácticas de seguridad. Pon en marcha un proceso exhaustivo de comprobación para garantizar que esas excepciones estén minuciosamente controladas y se resuelvan. Por otro lado, las políticas de trabajo utilizadas en remoto, no fueron elaboradas para aplicarse en este tipo de situación de trabajo en remoto, por lo que las organizaciones también deberán comprobar las políticas respecto a esto.

5 Emplea la autenticación de múltiples factores; es el momento de implementarla si aún no lo has hecho.

El inicio de sesión tradicional con usuario y contraseña es un blanco fácil para los ciberdelincuentes. Recurre a la autenticación de múltiples factores para tus cuentas siempre que sea posible. Ello requiere proporcionar al menos dos métodos de autenticación, prueba o identificación, previo acceso a la información protegida, dotándole de una segunda barrera de seguridad frente a la actividad criminal. Dicho nivel de protección adicional resulta especialmente importante cuando un gran número de usuarios se conectan a redes de forma remota, proporcionando a los ciberdelincuentes más puntos de acceso a través de los que vulnerar redes privadas.

Las mejores prácticas para tus empleados

6 Conectarse a Internet únicamente desde una red segura.

Al conectarnos a una red pública, terceras personas pueden acceder a toda la información que compartimos online o a través de una aplicación de móvil. Utiliza siempre una Red Privada Virtual (VPN) para encriptar tu actividad. La mayoría de las organizaciones proporcionan una VPN a sus empleados para garantizar un acceso remoto seguro para uso laboral, y muchos proveedores de servicios ofrecen cuentas de VPN personales.

7 Emplea contraseñas robustas

La mayoría de los usuarios emplean la misma contraseña o una similar para cada cosa, incluso en el trabajo y en casa. Por desgracia, ello implica que, con robar una única contraseña, los hackers podrán reutilizarla en lugares diferentes para acceder a decenas de cuentas. Recordar contraseñas seguras y complejas para cada cuenta puede ser un quebradero de cabeza o una labor imposible. Utiliza un programa de gestión de contraseñas para garantizar contraseñas robustas y diferentes para cada aplicación, ya que las contraseñas conforman la base de las actividades online.

8 Accede únicamente a enlaces, archivos adjuntos y programas descargables de fuentes fiables.

La mayoría de los usuarios quiere estar al día de las novedades, sobre todo en periodos de incertidumbre. Los ciberdelincuentes son conscientes de esto y pretenderán enmascarar enlaces maliciosos bajo material informativo. Una vez que entramos al enlace malicioso, este permite acceder a la información privada del usuario o de la organización y/o paralizar sus ordenadores o redes. Si no estamos seguros de la fuente, accede a la página web de la organización. Si es información relevante, se encontrará publicada allí también.

9 Verifica los enlaces web antes de compartir información confidencial

Los ciberdelincuentes pueden crear sitios web falsos cuyo enlace y página de inicio son significativamente parecidos a la web original, como tu proveedor de servicios sanitarios, tu banco o el correo electrónico. En lugar de acceder al enlace desde tu correo, tecléalo de forma manual. Además, asegúrate de que la web que visitas utiliza el protocolo HTTPS, estos enlaces son más seguros que los que utilizan HTTP.

10 No contestes a solicitudes de información de fuentes desconocidas, especialmente si exigen información identificativa o contraseñas.

Los ciberdelincuentes intentarán incitar a los usuarios a proporcionar información confidencial suplantando la identidad de un conocido o de un compañero de trabajo. Pon especial atención en identificar a quién te está solicitando tus datos, incluso si crees que la solicitud proviene de una organización o fuente fiable. No lo hagas con prisa, tómate tu tiempo para recabar información sobre la solicitud y plantéate si te conviene antes de ofrecer una respuesta.

Minimiza los ciberriesgos y actúa frente a una crisis

Cualquier ciberpolítica comercial de Chubb proporciona acceso a una variedad de recursos para ayudar a tu empresa a anticiparse y a actuar con rapidez frente a incidentes cibernéticos no deseados.

Visita https://www.chubb.com/es-es/ para obtener más información sobre la protección para las empresas.

Chubb. Insured.℠