Guía del colaborador remoto: Parte 4

Soporte técnico: ¿A quién debo contactar si algo sale mal?

A diferencia del soporte presencial, donde suele ser más rápido y sencillo resolver un problema con acceso directo al equipamiento necesario, el soporte remoto tiende a implicar dificultades y riesgos, a los que los empleados deben estar atentos.

Por empezar, los empleados deben tener los datos de contacto de la persona a la que deben dirigirse cuando necesitan reportar un problema o pedir asistencia. Es importante tener esa información almacenada en varios dispositivos. De esta forma, si alguno no estuviera disponible, los datos de contacto seguirían siendo accesibles.

Lo mismo aplica a los detalles de contacto para reportar un incidente de seguridad, como puede ser el robo o pérdida de un equipo. En este caso, es de especial importancia notificar a su empleador lo más pronto posible. Esto permitirá que el equipo de IT tenga tiempo suficiente para responder rápidamente y ejecutar los protocolos de seguridad correspondientes para prevenir que la información se vea comprometida.

Muchas compañías utilizan protocolo de escritorio remoto (RDP, por sus siglas en inglés) para dar a los técnicos informáticos acceso remoto a los dispositivos de la empresa. Varias herramientas RDP están disponibles para el público de forma gratuita, es decir, pueden ser utilizadas por cualquiera. Es importante estar al tanto de que existen múltiples engaños de RDP, en los que los atacantes buscan convencer a los usuarios de que existe un problema con su equipo, que requiere soporte técnico y acceso al RDP. Esto no es así.

Por eso, sin importar cuál sea la situación, siempre contacta al equipo de soporte técnico de la compañía y asegúrese de que realmente son ellos quienes

quieren acceder a su dispositivo. No le permita acceso remoto a cualquier persona desconocida o sospechosa.

Es también recomendable prestar atención a las acciones llevadas adelante por la persona de soporte en su equipo, aún si no cuenta usted con conocimiento técnico, porque es responsabilidad suya asegurarse de que no accedan a información confidencial en el proceso. De ser necesario, puede desenchufar su router hogareño – una solución rápida para desconectar el RDP.

Buenas prácticas

Durante estos tiempos de auge del teletrabajo, la seguridad de la información de los negocios depende más que nunca del cuidado de los empleados. Para mitigar los riesgos de la mejor manera, las empresas deberían seguir las siguientes prácticas:

- Cifre la información almacenada en equipos de trabajo
- Instale un software de seguridad endpoint en los equipos y manténgalo actualizado
- Mantenga los dispositivos (también) actualizados, incluyendo el sistema operativo y las aplicaciones
- Asegure y configure de forma correcta las redes hogareñas
- Al conectarse a una red pública o a un hotspot Wi-Fi, utilice siempre una VPN y evite acceder a información sensible
- Respalde la información periódicamente
- Proteja los dispositivos con contraseñas y evite dejarlos desatendidos una vez que se haya iniciado sesión
- Habilite la protección antirrobo en sus equipos
- Utilice doble factor de autenticación para proteger sus cuentas críticas
- Tenga siempre a mano los datos de contacto de soporte técnico y reporte cualquier incidente de seguridad lo más pronto posible
- Manténgase al día con los últimos engaños y amenazas siguiendo las noticias de WeLiveSecurity

Conclusión

A lo largo de esta guía hemos repasado los riesgos que implica el trabajo remoto y las maneras en que los negocios pueden optimizar significativamente el comportamiento de los empleados para mitigar dichos riesgos y mejorar la seguridad de las comunicaciones realizadas en redes remotas.

Tomando en consideración el avance del 5G, los dispositivos IoT y otras tecnologías – sumado al impulso del COVID-19, el acceso remoto a la información por parte de los empleados que trabajan desde sus hogares es sin duda una preocupación central de las empresas.

El empleado remoto se ha convertido en una pieza fundamental en la gestión de la seguridad de la información y los procesos de su negocio. Para afrontar los nuevos desafíos, las organizaciones deben tener políticas claras para administrar la información y herramientas adecuadas para permitir a los empleados llevar adelante sus actividades de forma segura.

Modificar el modo de trabajo dentro de una compañía debe involucrar a toda su fuerza de trabajo, y eso lleva tiempo. Pero con el correcto entrenamiento, los empleados pueden comprender rápidamente los riesgos del trabajo remoto y saber cómo evitarlos o contraatacarlos. Confiamos en que esta guía ha impulsado ese objetivo.