Ataques cibernéticos: tips para que el trabajo desde casa sea seguro

02/01/2021

Con la cuarentena prolongada y el cambio del trabajo presencial al online muchas personas, a través de sus equipos, se ven amenazadas por la seguridad informática y la información confidencial de sus empresas.

Es necesario proteger, mediante distintas prácticas, nuestros equipos y prevenir intenciones malintencionadas. Los ciberdelincuentes también buscan atacar a otros equipos, sitios web o redes para generar caos, bloquear un sistema informático, propiciar la pérdida de datos o hacer que el servidor falle. Vivimos en una sociedad totalmente dependiente de la tecnología por lo que nuestra información empresarial y personal está expuesta ante posibles ataques cibernéticos. Es por eso que Marcelo Da Cunha, vocero de Visión Tecnológica, comparte 5 tips importantes a implementar para evitar los ataques cibernéticos.

Correos: identificá el correo antes de abrirlo.
Evita abrir correros con remitentes desconocidos. Ante la duda, es recomendable no responder a los mismos y eliminarlos directamente.

Muchos de esos mails vienen con adjuntos y mensajes como “te envío una factura”, “te envío una cotización”. Hay que tener mucho cuidado en cómo vienen los correos, en hacer click en

enlaces sospechosos o descargar documentos.

Estos mails suelen tener distintos tamaños de letra, pueda estar mal traducidos y esto puede ayudar a identificarlos y frenarlos.

Back up: hacé respaldos de la información
Siempre hay que tener la mayor cantidad de respaldos posibles.

Recomendamos que tengan distintos tipos de respaldo: uno local, dentro del equipo para el día a día de trabajo; uno USB, para copiar esta respaldo de día a día y hacer el respaldo de datos, a fin de mantenerlo fuera de la red eléctrica; y un back up en la nube para poder prevenir cualquier tipo de robo, hurto, incendio o cualquier tipo de incidente que pudieran tener en la empresa:

Actualizaciones: mantené tus equipos al día
Actualizar los equipos y dispositivos siempre que sea posible, con software original para que no surjan problemas con actualizaciones fallidas o con problemas de seguridad por fallas con dicho software. Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos. Como contramedida los fabricantes corrigen los programas a través de actualizaciones.

Asimismo, se pueden adquirir hardware y software cortafuegos

para bloquear usuarios no autorizados y evitar que accedan a tus equipos.

Antivirus: contratá un antivirus corporativo
Es necesario que las compañías provean a sus empleados de un antivirus corporativo, no uno gratuito. Los antivirus utilizados para el hogar no garantizan la protección y la barrera contra este tipo de ataques.

Se recomienda contratar antivirus con las reglas de configuración y del sistema adecuadamente definido. Utilizar un antivirus que analice todas las descargas, actualizado al día para que reconozca el mayor número de virus, y además, realizar análisis de forma regular de todo el sistema.

Contraseñas: usá claves seguras
Cuidar las contraseñas y elegir claves grandes y complejas que contengan letras y números ayudará a que no puedan ser descifradas fácilmente.

Al introducir las contraseñas en un sitio se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing).

No se debe utilizar la misma contraseña en diferentes servicios porque si acceden a una cuenta fácilmente podrán acceder al resto.

Capacitaciones: capacitá a tus empleados en las nuevas tecnologías
Los empleados deben estar capacitados en las nuevas tecnologías.

Es necesario tener en cuenta la cultura organizacional de la

empresa ya que debería poder mantener una prevención con respecto a los antivirus y conocer cuáles son las medidas a tomar, cómo poder detectar un correo malicioso para que estén seguros que la información de la empresa está llegando de la mejor forma.

Es necesario estar atento a las señales que la red nos envía, ser precavido antes de hacer click en links o descargar archivos, y al momento de compartir información en línea.

Fuente: Ámbito