Recomendaciones para la Ciberseguridad en el Teletrabajo

CSIRT-CR

En Costa Rica estamos ante una alerta amarilla por la propagación del Coronavirus, por lo cual, se está impulsando a que tanto las empresas públicas como privadas realicen teletrabajo.

Trabajar desde la casa no es complicado, y la mayoría de nosotros lo hacemos de vez en cuando. Pero sabemos que la mayor parte de las organizaciones no habrán preparado a tantos empleados para trabajar de manera remota, es por esto por lo que es muy probable que los propios empleados no conozcan las mejores prácticas de seguridad cuando trabajan desde casa.

Es normal que desde casa trabajemos más relajados, especialmente cuando se trata de seguridad, ya que nos sentimos cómodos con la seguridad de nuestros hogares, pero desafortunadamente, los ciberdelincuentes aprovechan estas situaciones con ataques y amenazas de phishing muy bien diseñadas.

Los actores cibernéticos pueden enviar correos electrónicos con archivos adjuntos maliciosos o enlaces a sitios web fraudulentos para engañar a las víctimas para que revelen información confidencial o donen a organizaciones benéficas o causas fraudulentas.

Es por esto que recomendamos tener cuidado al manejar cualquier correo electrónico con una línea de asunto, archivo adjunto o hipervínculo relacionado con COVID-19, y desconfíe de las súplicas, textos o llamadas de las redes sociales relacionadas con COVID-19.

Si desea obtener información actualizada y basada en hechos sobre COVID-19, utilice fuentes confiables, ingresar a los sitios web legítimos del gobierno.

Mejores prácticas para que los empleados puedan trabajar de forma segura desde sus hogares

Asegure las redes a las que se conecta

- Resultará útil una Red Privada Virtual (VPN), la cual crea una red privada partiendo de una red pública. Así sus actividades en línea serán encriptadas y su información personal o la de su empresa no serán vulnerables para que cualquiera pueda interceptarlas.

Las contraseñas son importantes

- Se deben de revisar y fortalecer las contraseñas que utiliza para iniciar sesión, por ejemplo, correo electrónico o aplicaciones de trabajo.

Tenga cuidado con la suplantación de identidad (phishing)

- Si ve un enlace sospechoso No de clic y si va a descargar contenido, hágalo de fuentes confiables que puedan verificarse. Recuerde que las campañas de phishing son una forma de ingeniería social, por lo que, si recibe un correo electrónico con una solicitud inusual, verifique cuidadosamente los detalles del remitente para asegurarse de que se está comunicando con colegas, no con delincuentes.

Elija su dispositivo con cuidado

- Al realizar teletrabajo, la mayoría de los empleados usan la portátil de su empresa, lo que puede crear un riesgo de seguridad. Pero es mayor el riesgo si utiliza un portátil personal para fines laborales. Es recomendable hablar con su equipo de TI sobre cómo fortalecer la seguridad si tiene que usar su portátil para el trabajo.

La red Wifi de su hogar

- Asegúrese de que la contraseña de su Wifi sea segura, y que esté protegido contra cualquier persona dentro del alcance que pueda acceder y conectarse a la red. Las redes no seguras facilitan el acceso de los ciberdelincuentes a correos electrónicos y contraseñas.

Resguarde sus documentos en la nube

- Algunas empresas trabajan almacenando sus documentos y archivos en una nube y no en un dispositivo, es por esto que también se deben de tomar medidas de seguridad para que la información almacenada permanezca segura. Por ejemplo, una opción es activar una verificación, para que cada vez que quiera acceder a la nube, sea enviado a su celular un mensaje de texto que contendrá un código que deberá ingresar en el acceso a la nube.

Firmado digitalmente por JORGE EMILIO MORA FLORES (FIRMA)
Fecha: 2020.03.12 15:54:50 -06'00'

Jorge Mora Flores

Director de Gobernanza Digital

RAQUEL JAZMIN CANTILLO GAMBOA (FIRMA)
2020.03.12 15:48:32 -06'00'

Raquel Cantillo Gamboa

Analista en Ciberseguridad