

# 5

## TIPS PARA PROTEGERNOS CONTRA FRAUDES INFORMATICOS POR COVID-19



**HOY EN DÍA** nuestras actividades en el uso de tecnología se han vuelto más intensas, esto como todos sabemos es en gran medida a la crisis global derivada del COVID-19, durante este tiempo en los usos más intensos en las herramientas tecnológicas se ha incrementado los riesgos de Phishing derivado ganchos como: "promesa en ayuda por el COVID-19", "crédito rápidos por COVID-19", "financiamientos COVID-19", y todos aquellos que podamos imaginar, utilizando este tipo frases para atrapar a posibles víctimas.

Es por lo anterior que nuestro equipo de especialistas sugiere cinco acciones para ser socializado con su personal para mitigar riesgos de fraude y mantenerlos fuera de problemas y a su vez salvaguarda su información personal y de la organización.

- 1. Concientizar del riesgo de fraude (phishing).** Los atacantes utilizarán todos los medios posibles para engañarlos, por eso es importante ser siempre escéptico con la información que reciba, comunicarlo con los diferentes miembros de la organización.
- 2. Detectar correos electrónicos, mensajes de texto, comunicaciones de redes sociales o llamadas telefónicas que reciba que prometan ayudas.** Los correos electrónicos u otra comunicación digital que reciban los miembros con frases relacionadas a "ayuda COVID-19" deben de detectar origen, dar un seguimiento

y comunicarlo a los miembros de la organización, esto nos ayudara a establecer protocolos de actuación y listas negras.

- 3. Nunca debe proporcionar el número de cuenta bancaria, clabe bancaria, nombres de cuentas de usuario – contraseñas, número de seguro social, INE, CURP, otra información personal en respuesta a cualquier solicitud online.**
- 4. Evitar hacer directamente clic en los enlaces enviados por medio de correo electrónico.** Es importante comunicarlo a los miembros especializados de la organización.
- 5. Confirmar y verificar sitio de seguro de las webs.** Cuando se visite un sitio web, el personal de la organización puede confirmar y verificar que el sitio sea seguro, con un click en la imagen del candado a la izquierda de la dirección url en el navegador.

Es sumamente importante mantener una comunicación abierta con los miembros de la organización tanto técnicos – especialistas como operativos, el principal mitigante de este riesgo de fraude denominado Phishing derivado de la ingeniería social siempre será mitigado por establecer acciones tan simples como comunicar y el monitoreo continuo.

**"EL ESCEPTICISMO ES EL PADRE DE LA SEGURIDAD"**