La necesidad de contar con seguridad informática, se hace más fuerte que nunca.

A medida que los días avanzan, percibimos cómo la tecnología se incorporó definitivamente en nuestras vidas, este tiempo de teletrabajo nos ha permitido desarrollar mayores conocimientos en los sistemas electrónicos, mejorando de esta forma el acercamiento con esos productos o servicios que antes no frecuentábamos en estos medios. Pero esto trae consigo un aspecto que hoy más que nunca debemos evaluar, nos referimos a los fraudes cibernéticos a los que se exponen tanto las empresas como las personas en su día a día.

Definamos al crimen cibernético, como el robo o manipulación de información confidencial o privada con riesgo financiero; podemos representarlo de varias formas, todas llegan a ser percibidas como crímenes deliberados o maliciosos. Pero

también suceden cosas como el daño de archivos de computadoras por algún virus que afecta las operaciones de un negocio, que puede ser causado por un simple error humano.

Lo cierto es que las transacciones en línea crecen y los riesgos incrementan, no importa en qué momento de vida esté tu negocio, si tu página web no está bien protegida, tu sistema es vulnerable de ser hackeado y las pérdidas en la imagen corporativa y seguridad de tu empresa pueden llegar a ser irreparables. En un mundo donde cada día más profesionales llegan a la palestra de la sociedad, profesionales de los robos de datos se capacitan para mejorar su sistema de ataque.

Te compartimos ciertas recomendaciones para evitar que una persona o una empresa se vea afectada con esta modalidad de robo:

- **Comprueba la procedencia de correos electrónicos**
  Solicitar información en un correo electrónico es el sistema de ataque más común. Asegúrate siempre de confirmar la identidad de quien envía y responde los mails.
- **Construye contraseñas apropiadas**
  Además de cambiarlas cada cierto periodo, para evitar riesgos e inconvenientes innecesarios.
- **Respaldo de archivos**
  El común de los factores cuando alguien pierde información, básicamente se comprueba cuando no existe la data de respaldo. Es obligación de las compañías contar con un centro de almacenamiento de datos con un proveedor o servicio de una nube.

Chema Alonso, uno de los hackers más influyentes a nivel mundial, conocido también como “El Hacker bueno”, nos recomienda ponerle mucho más asunto del que creemos. Para entender más sobre materia de seguridad hay que leer mucho, practicar y ser constante, ya que la búsqueda de vulnerabilidades de los usuarios y empresas cada día crece

más.

Para finalizar tenemos que entender que todos somos propensos de sufrir un *cyber* ataque. Un claro ejemplo es lo que nos dice el experto en riesgos cibernéticos, Mauricio Silva Granda de GRB Corredores de Reaseguros, quien recomienda tener contratado planes de seguridad para las páginas web, además de contar con accesos robustos, inclusive las computadoras del personal de una empresa deben contar con las restricciones y herramientas necesarias para evitar ataques cibernéticos.

Es cierto que existen sistemas de seguridad gratuitos, pero pensemos un instante en aquella posibilidad: ¿Dejarías la seguridad de tu empresa bajo este sistema? En el fondo todos conocemos la respuesta, es preferible pagar por una buena protección.

No hay oportunidades para jugar con este tipo de riesgo, muchas aseguradoras ofrecen pólizas contra el crimen cibernético o *cyber risks* y éstas están a tu alcance.

Instrúyete con más consejos sobre seguridad digital en este link que te dejamos a continuación: https://bit.ly/2YJnkGS .

Redactado por: *Diego Mendoza*

Bibliografía:

https://www.youtube.com/watch?v=5zlzdQe7nig
https://reportedigital.com/seguridad/ataque-cibernetico-empresa-consejos/
https://www.marsh.com/ar/es/services/cyber-risk.html
https://www.forbes.com.mx/riesgos-de-fraude-electronico-en-el-e-commerce/