#AsegúrateDeHacerTuParte

SEGURIDAD **INFORMÁTICA**

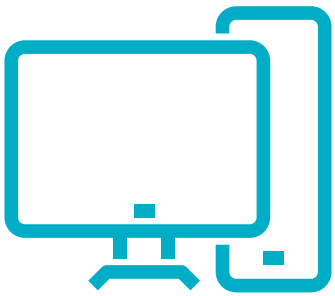
Mientras los estados y las empresas están haciendo frente a la pandemia con medidas que buscan minimizar la exposición al COVID-19, como el teletrabajo, los ciberdelincuentes aprovechan esta coyuntura valiéndose de la descentralización del acceso a la información, para lanzar ataques contra las personas y organizaciones.

Estos delincuentes se aprovechan de la vulnerabilidad de las personas frente a ataques de ingeniería social y de la poca madurez en la seguridad de la información de las organizaciones cuando alguno de sus colaboradores accede a información sensible fuera de los ambientes tecnológicos corporativos, lo cual aumenta la probabilidad de éxito de que un ataque cibernético dirigido.

INGENIERÍA SOCIAL

Los ciberdelincuentes aprovechan los temas de interés y el alto flujo de búsqueda de información para incluir archivos maliciosos que tienen alta probabilidad de descarga por su apariencia de contenido de temas de actuales. Además, según el estudio publicado la BBC el 13 de marzo de 2020, se están enviando correos electrónicos masivos maliciosos usando el miedo a la enfermedad COVID-19 que incluyen, por ejemplo, asuntos e información sobre la vacuna, pautas para evitar el virus o procedimientos para donar recursos para investigación o ayuda para atender los contagiados.

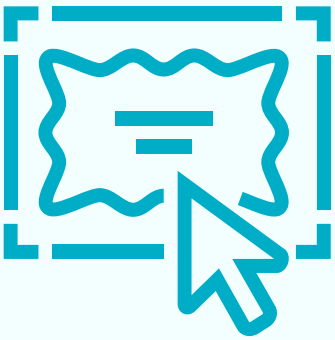
Estas acciones aumentan la exposición ante la estrategia de teletrabajo adoptada por las organizaciones que tienen bajos sistemas de protección fuera de sus plataformas corporativas, que pueden llevar a que los ataques no sean filtrados a tiempo y en muchos casos efectivos. Todo esto para obtener la información que tienes guardada en tus dispositivos personales, dispositivos compartidos y dispositivos asignados por tu empresa que tienen un alto valor en el mercado negro.



Adicional, otra de las amenazas a las cuales nos vemos enfrentados actualmente son las noticias falsas que llegan por las aplicaciones de mensajería instantánea como WhatsApp, Telegram, Messenger y redes sociales. Estos son los medios más usados para difundir rumores como testimonios de supuestos profesionales del sector sanitario que informan de noticias que los medios no se atreven a contar y que pueden generar pánico, llevándonos a acceder a páginas suplantadas e inseguras.

A continuación, te presentamos una guía de buenas práctica para proteger la información personal y empresarial de un ciberataque mientras estás fuera de tu lugar habitual de trabajo:

Correo electrónico:



- Al recibir un correo electrónico no esperado de un compañero o de un aliado (proveedores, clientes, socios de negocio, entre otros), verifica su veracidad mediante el remitente porque puede ser un caso de suplantación. En caso de tener archivos adjuntos o enlaces que te lleven a otras páginas, te recomendamos no usar el hipervínculo y ponerte en contacto con el remitente y con el área de Tecnología (seguridad informática) de tu empresa.

- Si te llega información de terceros, como posible información del COVID-19 u otros temas no laborales, te recomendamos eliminar inmediatamente el mensaje y notificar al área de Tecnología (seguridad informática) de la organización para identificar si es un posible ataque cibernético y generar las medidas necesarias para su contención. Es importante notificar, ya que este posible correo malicioso puede llegar a varios compañeros de la organización y entre más rápido se identifique, se pueden tomar medidas preventivas oportunas.

- Si de manera irregular, el sistema de correo (cuando estás navegando en internet en cualquiera de los exploradores) te piden ingresar tu usuario y contraseña, deberás verificar que la dirección del sitio web que solicita esta información corresponde a la empresa, y en caso contrario, no ingresar ningún dato y reportar a las personas de Tecnología (seguridad informática).

Mensajería instantánea (WhatsApp, Messenger, etc):

Al recibir archivos provenientes de cadenas de mensajes o acceder a direcciones de internet que te lleguen con información no verificable por redes sociales o mensajería instantánea, te recomendamos no abrir esta información.

Llamadas telefónicas:

Ante llamadas de supuestas entidades de salud, gobierno, u otras, debes evitar dar información personal como número de póliza de salud, números de tarjetas de crédito, cuentas bancarias, contactos personales cercanos o familiares, entre otras. Cuando termines la llamada, contacta a la línea de atención de esa entidad con el fin de validar su veracidad. Recuerda que esta información puede ser utilizada para responder preguntas de seguridad en las plataformas tecnológicas para robar información.

CONECTIVIDAD

Conectarse a internet fuera de las redes corporativas para realizar tus funciones te expone a un riesgo mayor de ser víctima de un ataque cibernético por las posibles fallas en configuración de las redes que en su mayoría carecen de buenas prácticas de seguridad y la hacen más vulnerables a ataques cibernéticos que buscan capturar la información de las personas que están conectadas en esa red.

Sigue las siguientes recomendaciones para minimizar el riesgo de un ataque cibernético por la conexión a internet:

- Accede a internet solo en lugares de confianza, evitando usar redes públicas de coworkings, centros comerciales, parques, cafés, aeropuertos, clínicas, universidades y otros con acceso a internet compartido con personas desconocidas.

- Si estás ubicado en un lugar donde existan conexiones no seguras, usa el plan de datos de tu celular como módem de acceso a internet compartido y configura una clave segura.

- Cambia la contraseña de la red WiFi de tu casa mensualmente. Si necesitas ayuda para hacerlo, puedes contactarte con tu proveedor de internet.

- Verifica la cantidad de dispositivos conectados a la red de tu hogar y que todos estos sean conocidos. Si necesitas ayuda para esta verificación, puedes contactarte con tu proveedor de internet o usar aplicaciones que lo permiten. Si alguno de los dispositivos conectados a tu red es desconocido, significa que personas externas están utilizando tu conexión.

- Minimiza la cantidad de dispositivos prendidos o conectados a la red de tu hogar para mejorar la velocidad del internet.

DISPOSITIVOS

Los dispositivos como celulares, tabletas, computadores, entre otros, que utilices para la realización de tus funciones laborales, sean personales o asignados por la empresa, deberán tener las protecciones mínimas recomendadas por el área de Tecnología de tu empresa.

Debido a que en el hogar es frecuente que los hijos utilicen los dispositivos de los padres para temas lúdicos o académicos, y en los cuales hay acceso a información de la empresa, se recomienda tener controles de instalación de aplicaciones o software, y de ser posible, tener un usuario exclusivo para los hijos en estos dispositivos. Evita que tus hijos utilicen dispositivos con información personal y corporativa que pueda ser sensible.

En el momento de empezar a hacer uso de los dispositivos compartidos en tu hogar, te recomendamos reiniciarlos para que borren cualquier información contenida en la memoria RAM del dispositivo, minimizando el riesgo de fuga de información por estar ejecutando programas espías.

Otras dos recomendaciones es el uso de VPN (si la empresa la tiene) o una protección adicional que puedas instalar en el equipo en el que estás trabajando con el fin de mejorar tu seguridad y rendimiento. Además, es necesario tener antivirus en el computador, manteniéndolo activado y actualizado.

ACCESO A LA INFORMACIÓN EN LA NUBE

Muchas empresas están migrando el almacenamiento de su información a sistemas basados en la nube para mejorar su disponibilidad. Y por esto, es importante que los accesos a dicha información se hagan desde una conexión a internet segura y desde dispositivos confiables.

Recomendamos tener en cuenta las siguientes características en el momento de ingresar a la información que tu compañía tenga almacenada en la nube:

- Evita descargar información a los dispositivos que estés utilizando y si la tienes que descargar, una vez termines de utilizarla, asegúrate de borrarla de forma segura, tanto en la carpeta como en la papelera de reciclaje.
- Accede solo a la información que necesitas utilizar para el desarrollo de tus funciones.
- No accedas a la información de la nube con conexiones inseguras.
- Asegúrate que no guarde la contraseña de acceso a la nube en el navegador que estés utilizando.