La seguridad informática es un derecho de todos

¿Por qué hacemos esto?

Buscamos informar a las personas usuarias de la web de los posibles peligros a la hora de navegar por internet.

¿Porqué es importante que dediques atención a este material?

No queremos que pases por una estafa informática, por eso sugerimos que, si usted es usuaria/o de la web, tengas presente algunas de las recomendaciones detalladas a continuación.

¿Para qué me va a servir?

Los contenidos abordados a continuación le servirá para saber qué hacer si alguna vez usted fuera víctima de un ciberdelito.

Les estaremos compartiendo información y algunas sugerencias a la hora de utilizar la internet y la tecnología en general.

A continuación hablaremos de:
Fake Access Points y ***Watering Hole Attack***

Fake Access Points

(puntos de acceso falsos)

¿De qué se trata?

Se trata de una amenaza que aprovecha la necesidad más básica de los seres humanos: la conexión a internet.

¿Cómo se indentifican?

Se indentifican como puntos de acceso de conexión a internet mediante una red de Wi-Fi libre, es decir, sin contraseña.

¿Qué riesgos me puede ocasionar?

Conectarse a esas redes pueden ocasionar un riesgo altisimo, el atacante puede obtener detalles del dispositivo que está conectado y así seleccionar el método de ataque ideal para ingresar a él y hackearlo. Tambien así puede capturar todo el tráfico de la víctima e incluso obtener sus credenciales de acceso a sitios privados, como correos, redes sociales, etc.

¿Cómo evitar ser víctima de este problema se seguridad?

sugerimos fuertemente que no te conectes a redes desprotegidas, o a redes cuya procedencia desconozcas. Expertos sugieren incluso, en lugares en que realmente necesites de internet, como en el aeropuerto, preguntar por la oficialidad de la red a la que te quieras conectar.

Watering Hole Attack

(Ataque de abrevadero)

¿De qué se trata?

Este tipo de ataques están enfocados a compañías, en las que los usuarios visitan constantemente sitios web de confianza relacionados con el contenido de la organización.

¿Cómo se indentifican?

Estas webs generalmente se encuentran incluidas, incluso en listas blancas de navegación por los equipos de seguridad informáticos de la empresa.

¿Qué riesgos puede ocasionar?

Una vez el empleado de la compañía objetivo visite el sitio web alterado, infectará su equipo con un malware que permitirá a los atacantes tomar el control del equipo del empleado y poder así espiar y robar información de la compañía. Los ciberdelincuentes, centran sus esfuerzos en observar el tráfico de la compañía a atacar, haciendo hincapié en aquellos sitios visitados y recogiendo la mayor información posible para crear un perfil concreto de la víctima.

¿Cómo evitar ser víctima de este problema de seguridad?

Los usuarios de dichos sitios web deben prestar atención a la seguridad implementada en los distintos tipos de navegadores empleados y en las continuas actualizaciones del software de sus equipos, no deben olvidar bloquear la ejecución automática de lenguajes de scripting en los navegadores y revisar las listas blancas de vez en cuando para comprobar que apunten a los sitios adecuados.