Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Diecinueve

Septiembre: Uso de VPNS y Seguridad en redes Wi-Fi: Cómo proteger tu conexión y evitar el acceso no autorizado

VIEM Vicerrectoría de Innovación y Emprendimiento

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Diecinueve
Septiembre de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

Responsable de la Edición
Ing. Yenny Stella Núñez Álvarez

Revisó
Ing. Fernando Zambrano Hernandez
Director CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 19

Septiembre 2023

Uso de VPN y Seguridad en redes Wi-Fi: Cómo proteger tu conexión y evitar el acceso no autorizado

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

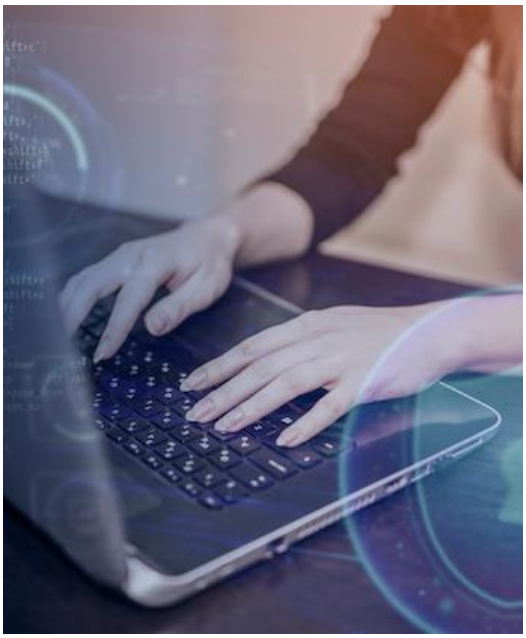
Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Yenny Stella Nuñez Álvarez
ORCID: https://orcid.org/0000-0003-0128-1214

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

Una red wifi (red inalámbrica) permite la conexión a la red de distintos dispositivos desde cualquier lugar o ubicación según los puntos de acceso que amplifican las señales en los hogares y en diferentes organizaciones proporcionando comodidad y movilidad para hacer uso de los recursos y aplicaciones asociadas al internet[1]. Sin embargo, es importante tener precaución al conectarse a redes públicas o abiertas; esto debido a que pueden ser redes no seguras, expuestas a riesgos cibernéticos aprovechados por personas malintencionadas que pueden interceptar cualquier dato que se envíe o se reciba, obtener acceso a los archivos compartidos, secuestrar la conexión a Internet, obtener datos confidenciales entre otras acciones maliciosas. El uso de una VPN (red privada virtual), en este caso, puede ayudar a proteger su conexión a Internet cuando se conecta desde una red Wi-Fi pública creando un túnel cifrado entre su dispositivo y un servidor remoto, lo que hace que los datos sean difíciles de interpretar para los demás usuarios de la red[2].



Fuente: https://www.freepik.es/

[1] https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html#~beneficios
[2] https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

Desarrollo

Con la pandemia se incrementó el uso de las VPN en las organizaciones para el trabajo remoto de sus empleados, esta operación consiste en habilitar una red privada virtual para crear una conexión de red privada entre dispositivos a través de Internet. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas. Su funcionamiento consiste en ocultar las direcciones IP de los usuarios y cifrar los datos para que nadie que no esté autorizado a recibirlos pueda leerlos[3].

Dado que una conexión WIFI y una VPN usan Internet para comunicar, compartir recursos, acceder a aplicaciones y transferir información, ambas conexiones pueden articularse de modo tal que se logre los mecanismos de protección necesarios al momento de acceder a una red pública.

Técnicas de Acceso no autorizado en las conexiones Wifi publicas

Los ciberdelincuentes aprovechan el internet como una superficie de ataque dotada de oportunidades para utilizar una variedad de técnicas enfocadas a vulnerar VPN y redes Wi-Fi públicas entre ellas encontramos:

Ataques de intermediario (man-in-the-middle attack – hombre en medio)

En un ataque de intermediario, el ciberdelincuente se coloca entre el dispositivo del usuario y el servidor al que se está conectando. Esto le permite al ciberdelincuente interceptar el tráfico de datos, incluyendo contraseñas, números de tarjetas de crédito y otra información confidencial[4].

Fuente: https://www.freepik.es/vector-gratis/concepto-actividad-hacker_8269019.htm#query=atauge%20cibernetico&position=6&from_view=search&track=ais

Los ciberdelincuentes pueden realizar ataques de intermediario en redes Wi-Fi públicas utilizando un dispositivo llamado "fake AP" (punto de acceso falso). Un fake AP es un punto de acceso Wi-Fi que se configura para parecerse a un punto de acceso legítimo. Cuando un usuario se conecta a un fake AP, el ciberdelincuente puede interceptar todo el tráfico de datos del usuario.

Uno de los objetivos de este tipo de ataque es el secuestro de correos electrónicos para espiar las conversaciones de su víctima. Una vez que se infiltran en este sistema cerrado, pueden enviar correos suplantándola para pedir transferencias de dinero, información financiera y contraseñas, entre otros.

[3] https://aws.amazon.com/es/what-is/vpn/

[4] https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

El ciberdelincuente tiene la posibilidad igualmente de secuestrar la sesión, donde obtiene el control de las cookies del navegador, que son datos que se almacenan en el navegador y se utilizan para recordar las preferencias, idioma, ubicación, actividad en línea, entre otros. A raíz de este acceso, puede extraer una variedad de datos, desde credenciales de inicio de sesión hasta información personal de formularios web llenados previamente. Otra forma de realizar este tipo de ataque es cuando el ciberdelincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router[5]. Éste es el método más complejo de los dos, pero también el más efectivo; ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.

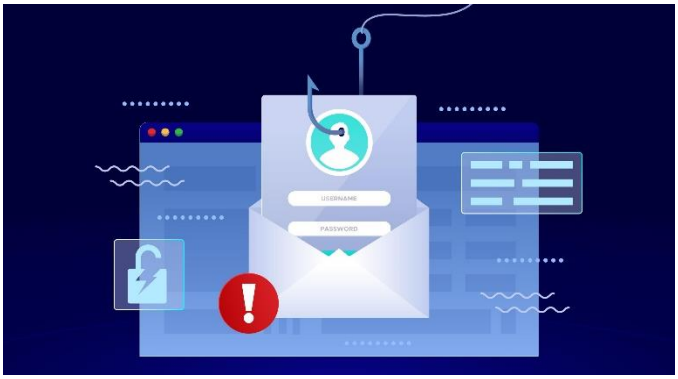
Malware

Los ciberdelincuentes pueden distribuir malware a través de redes Wi-Fi públicas. Este malware puede robar datos personales, infectar dispositivos con virus o ransomware, o incluso tomar el control de dispositivos[6]. Así mismo, los ciberdelincuentes pueden distribuir malware en redes Wi-Fi públicas a través de una variedad de métodos, incluyendo:

- **Enlaces maliciosos:** Los ciberdelincuentes pueden enviar correos electrónicos o mensajes de texto con enlaces maliciosos que, si se hacen clic, pueden instalar malware en el dispositivo del usuario.
- **Archivos adjuntos maliciosos:** Los ciberdelincuentes pueden enviar correos electrónicos o mensajes de texto con archivos adjuntos maliciosos que, si se abren, pueden instalar malware en el dispositivo del usuario.
- **Inyecciones de malware:** Los ciberdelincuentes pueden inyectar malware en el tráfico de datos de un usuario mientras se conecta a una red Wi-Fi pública.

Phishing

El phishing es un tipo de ataque cibernético en el que el ciberdelincuente se hace pasar por una persona o empresa legítima para engañar a la víctima para que revele información confidencial.



Fuente: https://www.freepik.es/vector-gratis/cuenta-phishing_8088576.htm#query=phishing&position=9&from_view=search&track=sph

En este orden de ideas, los ciberdelincuentes pueden utilizar redes Wi-Fi públicas para enviar correos electrónicos de phishing a los usuarios. Estos correos electrónicos suelen contener enlaces o archivos adjuntos maliciosos que, si se abren, pueden instalar malware en el dispositivo del usuario[7].

[5] Dispositivo que proporciona Wi-Fi y que generalmente está conectado a un módem.
[6] https://es.malwarebytes.com/malware/
[7] https://www.trendmicro.com/es_es/what-is/phishing/types-of-phishing.html

Otras técnicas

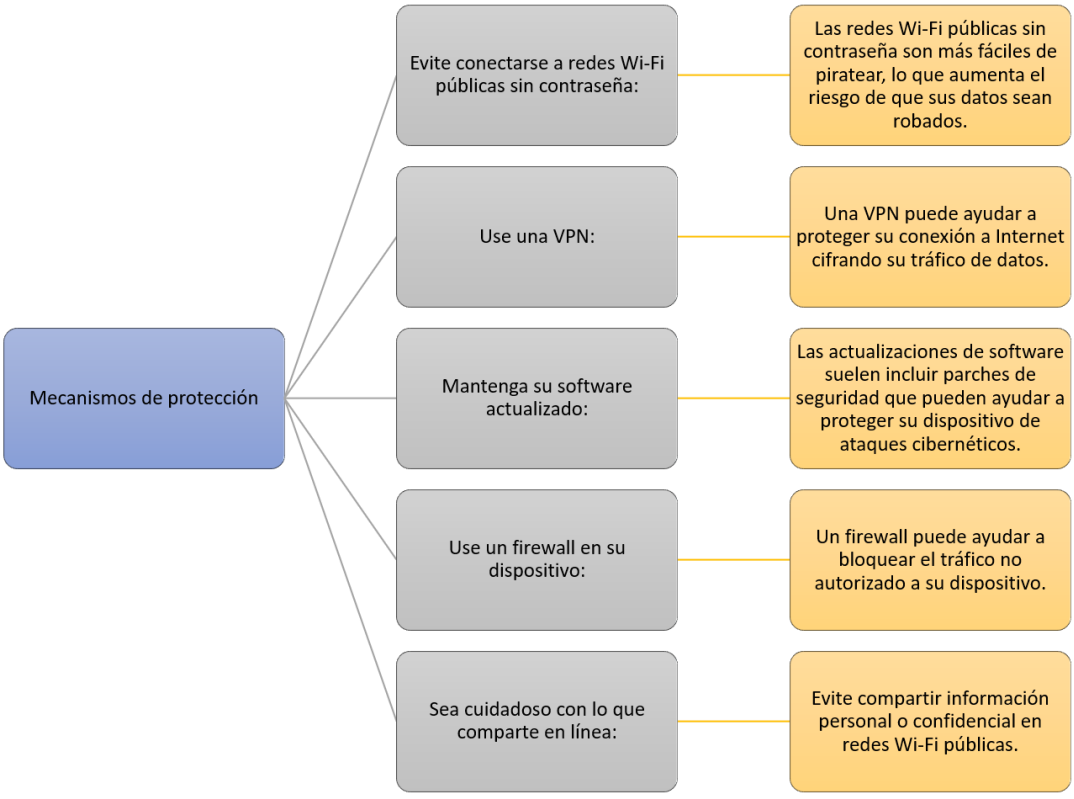
Además de las técnicas mencionadas anteriormente, los ciberdelincuentes también pueden utilizar otras técnicas para vulnerar VPN y redes Wi-Fi públicas. Estas técnicas incluyen:

- **Explotación de vulnerabilidades:** Los ciberdelincuentes pueden explotar vulnerabilidades en el software o el hardware de un dispositivo para obtener acceso al dispositivo.
- **Ataques de fuerza bruta:** Los ciberdelincuentes pueden utilizar ataques de fuerza bruta para adivinar las contraseñas de los usuarios.
- **Ataques de diccionario:** Los ciberdelincuentes pueden utilizar ataques de diccionario para adivinar las contraseñas de los usuarios utilizando una lista de palabras comunes[8].

Protección de ataques cibernéticos, uso de VPN y la Seguridad en redes Wifi públicas

Existen acciones efectivas que pueden realizarse para protegerse de los ataques cibernéticos en VPN y redes Wi-Fi públicas. Estas medidas se ilustran en la figura 1 incluyen:

Figura 1 Mecanismos de protección para evitar ataques cibernéticos



Fuente: propia

[8] https://www.xataka.com/seguridad/wi-fi-publica-estos-pasos-que-sigo-para-protegerme-cuando-me-conecto-a-red-publica

Las VPN son una herramienta valiosa para proteger la privacidad y la seguridad de los datos al conectarse a Internet o a redes públicas. Sin embargo, incluso las VPN pueden ser vulnerables a los ataques informáticos. Algunos de los mecanismos de protección más comunes para evitar ataques informáticos[9] en las VPN incluyen:

- **Cifrado:** El cifrado es el proceso de convertir datos en un formato ilegible para que no puedan ser leídos por personas no autorizadas. Las VPN utilizan el cifrado para proteger el tráfico de datos entre el dispositivo del usuario y el servidor VPN.
- **Autenticación:** La autenticación es el proceso de verificar la identidad de un usuario o dispositivo. Las VPN utilizan la autenticación para asegurarse de que solo los usuarios autorizados pueden conectarse a la red.
- **Control de acceso:** El control de acceso es el proceso de permitir o denegar el acceso a la red a usuarios o dispositivos específicos. Las VPN utilizan el control de acceso para restringir el acceso a la red a usuarios autorizados.

Otros mecanismos de protección que pueden ayudar a evitar ataques informáticos en las VPN[10] incluyen:

- **Actualizaciones de software:** Las VPN deben mantenerse actualizadas con las últimas correcciones de seguridad para protegerse de las vulnerabilidades conocidas.
- **Seguridad del dispositivo:** Los dispositivos que se conectan a una VPN también deben estar protegidos con las últimas medidas de seguridad, como firewalls y antivirus.
- **Concienciación de la seguridad:** Los usuarios de VPN deben estar conscientes de los riesgos de seguridad y tomar medidas para protegerse.

A continuación, se presentan algunos consejos específicos para ayudar a proteger su VPN[11] de ataques informáticos:

- **Elija una VPN segura:** Al elegir una VPN, busque una que utilice un cifrado fuerte, autenticación y control de acceso.
- **Use una contraseña segura:** Utilice una contraseña segura para su cuenta VPN.
- **No comparta su contraseña:** No comparta su contraseña VPN con nadie.
- **Mantenga su VPN actualizada:** Actualice su VPN con las últimas correcciones de seguridad.
- **Use un firewall:** Use un firewall en su dispositivo para bloquear el tráfico no autorizado.
- **Instale un antivirus:** Instale un antivirus en su dispositivo para protegerlo de malware.

Todo depende de las buenas prácticas y emplear los mecanismos adecuados de forma constante en cuanto a prevención y protección para evitar ataques informáticos en la VPN de la que hagamos uso y de esta forma mantener sus datos seguros.

[9] https://www.avast.com/es-es/c-what-is-a-vpn#:~:text=Una%20VPN%20es%20una%20herramienta,realiza%20operaciones%20bancarias%20en%20l%C3%ADnea.
[10] https://www.brontobytecloud.com/queataques-puede-prevenir-una-vpn
[11] https://forti1.com/es/ssl-vpn-mejores-practicas-7-consejos-de-seguridad/

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:


Correo: csirt@unad.edu.co


Twitter: @csirtunad


Página web: https://csirt.unad.edu.co

Referentes Bibliográficos

[1] https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/wireless-network.html#~beneficios

[2] https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene

[3] https://aws.amazon.com/es/what-is/vpn/

[4] https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

[5] https://www.trendmicro.com/es_es/what-is/phishing/types-of-phishing.html

[6] https://www.xataka.com/seguridad/wi-fi-publica-estos-pasos-que-sigo-para-protegerme-cuando-me-conecto-a-red-publica

[7] https://www.avast.com/es-es/c-what-is-a-vpn#:~:text=Una%20VPN%20es%20una%20herramienta,realiza%20operaciones%20bancarias%20en%20l%C3%ADnea.

[8] https://www.avast.com/es-es/c-what-is-a-vpn#:~:text=Una%20VPN%20es%20una%20herramienta,realiza%20operaciones%20bancarias%20en%20l%C3%ADnea.

[9] https://www.brontobytecloud.com/queataques-puede-prevenir-una-vpn

[10] https://forti1.com/es/ssl-vpn-mejores-practicas-7-consejos-de-seguridad/