Why Should You Worry?

The consequences of harboring rogue devices can range from mildly annoying to downright disastrous:

Security Breaches:

Rogue devices can be used to steal your sensitive information like passwords, bank details, or personal files. Think credit card fraud, identity theft, and a whole lot of privacy nightmares.

Malware Outbreaks:

A single infected device can act as a gateway for mal-ware, spreading like wildfire within your network, infecting other devices and wreaking havoc.

Network Disruptions:

Imagine your internet grinding to a halt, buffering videos, and dropped calls. Rogue devices can hog bandwidth, slow down your network, and make your online experience a frustrating crawl.

The Reconnaissance Mission takes approximately 7 days to complete. When the mission is over, simply return the Rogue Device Detection Kit for a refund of your deposit (there is a deposit on the equipment) and a printed report of our findings along with a Checklist of Actions to help secure your network.

MORE INFORMATION

573.693.7279
Visit our site for more information regarding our reconnaissance kit, visit the above site or scan the QR code

2935 BAGNELL DAM BLVD.
Suite 213
Lake Ozark, MO 65049

www.ozarkcomputerclinic.com
Visit our site for more information regarding our reconnaissance kit, visit the above site or scan the QR code

At Ozark Computer Clinic we value your privacy and we do not monitor or intercept any data from any devices on your network. We use a non invasive process to detect any intruders or potential intruders on/around your network. For a complete list of our Privacy Policies, please visit:
https://www.ozarkcomputerclinic.com/privacy-policy/

ROGUE DEVICE DETECTION

OZARK COMPUTER CLINIC

WWW.OZARKCOMPUTERCLINIC.COM

2935 BAGNELL DAM BLVD. SUITE 213
LAKE OZARK, MO 65049
573.693.PCRX

ROGUE DEVICE DETECTION

Beware the Network Infiltrators: A Closer Look at Rogue Devices

Imagine your home Wi-Fi, a cozy haven for online browsing and streaming. Now, picture an unwanted guest lurking amongst your connected devices, silently snooping on your data or disrupting your internet like a mischievous gremlin. These digital intruders are known as rogue devices.

So, What Exactly Are Rogue Devices?

In simple terms, they're any unauthorized devices connected to your network without your knowledge or permission. They can be anything from a forgotten laptop to a cleverly disguised malware-ridden gadget. Here are some common types:.

Rogue wireless access points (Aps)

Compromised devices

Unidentified gadgets

Deploy Our Rogue Device Reconnaissance System

We have a specialized tool that can scan your network for any unauthorized devices, identifying potential threats and giving you a comprehensive overview of your network's security status. Below are what is included with the Rogue Device Reconnaissance Mission;

Advanced Rogue Device Detection Tool

Our powerful system scans your network and surrounding areas, not just detecting rogue devices, but also providing valuable insights about their presence, and potential risks. It's like having a cyber-security bloodhound sniffing out any unwelcome & invisible intruders.

Threat Reports & Personalized Security Advice

We believe in empowering you to become an active guardian of your network. After providing you with a list of possible rogue devices, our technicians will provide clear, actionable advice on how to improve your network security posture. Think of it as a training manual, equipping you with the knowledge and advice to maintain a safe and secure digital environment..

CompTIA SECURITY TRUSTMARK+

Microsoft CERTIFIED SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS

HIPAA compliant

Network Security CERTIFIED PARTNER cbts