COVE PROVIDES PUBLIC WiFi SECURITY

New COVE device uses blockchain tech to create a distributed certificate management system. With no connection to external servers, users surf anonymously.

blockchain wifi security

NEW YORK, NEW YORK, USA, May 14, 2019 /EINPresswire.com/ -- A former Homeland Security Cyber Director Michael Echols and Blockchain developer / Media owner Teemu Airamo, announced the launch of COVE Security — COVE stands for Cyber-Open View Encryption. It is a zero knowledge virtual network security device. When plugged into a power source, COVE hides the data flowing to dangerously unsecure public WiFi networks.

In recent years, the number of data security breaches has soared and cybersecurity experts concede that use of public WiFi is a contributor. Connection in malls, co-working spaces, airports and coffee shops give hackers unauthorized wireless access to the data of unsuspecting WiFi users.

> COVE uses blockchain technology to create a distributed certificate management system."
>
> *Michael A. Echols - Partner at Cove Security*

Although VPNs are typically used to protect private web traffic, technology experts have also identified several issues with using VPN products. Among the concerns, VPNs keep logs of their users and reduce network speed by as much as 90%.

COVE provides the protection of traditional VPNs, but has new bleeding edge features.

COVE uses blockchain technology to create a distributed certificate management system.

This means it has no single point of failure. Additionally, COVE never connects to external servers like VPNs do, that gives users the ability to surf anonymously. These features help users to securely access available WiFi networks.

"A company in the same co-working location where we have offices were exposing medical records while using public WiFi. This type of exposure leads to greater intrusion opportunities for hackers, says Teemu Airamo, Partner at COVE Security.

However, it's not just hackers that web surfers should be worried about — a large number of companies are taking advantage of the new more lenient regulations. There are few consumer protections dissuading their selling of internet user data and browsing history. These business entities are racing to package and deliver information to buyers that may include nation-states.

"We developed COVE to minimize digital risk for all WiFi users. This device will provide security for millions of people across the world," says COVE Security Partner Michael Echols.

"Our goal is to provide an effective all-in-one solution to guard privacy during those times when a person has to use public WiFi as well as when it is the only option at work. COVE Security devices allow users to surf the web anonymously from any location without leaving any traces of browsing history." This is a major security advancement," Airamo concludes.

COVE is being launched as a private beta via its token offering and blockchain authentication services. The company is currently negotiating with government, industry and academic partners.

About Michael Echols:

Michael Echols spent ten years at the Department of Homeland Security. In 2015, Mr. Echols became the White House point person for the rollout of Presidential Executive Order 13691 – Promoting Private Sector Cyber Information Sharing. Most recently Mr. Echols authored five Forbes articles and was featured on a PBS cybersecurity special. Mr. Echols has also led two organizations to CSO50 Award honors for information sharing in the last three years. He is currently on the Health and Human Services CISA Cyber Awareness Task Force.

Mr. Echols also chaired the Communications Sector and the International Network Security Information Exchange (NSIE). Additionally, he managed the President's National Security Telecommunications Advisory Committee (NSTAC), 30 Chief Executive Officer level NSTAC members who represent IT, Defense and Communications companies producing communications policy recommendation for the President of the United States.

Media Contact:

info@covesecurity.io

Aleksandra Pelszynska
Max Cybersecurity LLC
+1 202-499-6855
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/485085061

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2020 IPD Group, Inc. All Right Reserved.