WORKING FROM HOME DURING THE CORONAVIRUS PANDEMIC CREATES NEW CYBERSECURITY THREATS

Aaron Mauro

https://theconversation.com/working-from-home-during-the-coronavirus-pandemic-creates-new-cybersecurity-threats-134954

Engl.

The article by Aaron Mauro goes about new cybersecurity threats during the coronavirus pandemic. The author claims that people now working from home will soon become a target for hackers.

According to the author, in the coming months, many of us will be subject to a range of cybersecurity threats, such as all-too-common phishing attacks. Phishing campaigns use email to coerce a user into inadvertently helping an attacker by clicking a misdirected link, downloading a malicious file or entering log-in credentials. The article gives an accurate description of how to protect yourself from this type of cyberattack.

The author focuses on increasing number of ransomware attacks on hospitals and labs working on coronavirus. Thus, all institutions, including hospitals and public health organizations, should have recent back-ups that would allow them to rapidly restore services in the event of a ransomware attack.

The main idea of article is that the people who work from home, medical workers and customary user should pay more attention to network security.

The author concludes that COVID-19 represents an opportunity to build better digital infrastructure .

Укр.

У статті Аарона Мауро розповідається про нові загрози кібербезпеці, які виникають під час пандемії коронавірусу. Автор стверджує, що люди, які зараз працюють вдома, незабаром стануть мішенню для хакерів.

За словами автора, у найближчі місяці багатьом з нас буде загрожувати цілий ряд загроз кібербезпеки, таких як поширені фішинг-атаки. Фішинг-кампанії використовують електронну пошту, для того щоб примусити користувача ненавмисно допомогти зловмиснику, натиснувши на неправильне посилання, завантаживши шкідливий файл або ввівши власні облікові дані для входу. У статті подано детальний опис того, як захистити себе від подібного типу кібератаки.

Автор акцентує увагу на збільшенні кількості нападів програм-вимагачів на лікарні та лабораторії, що працюють над коронавірусом. Таким чином, усі установи, включаючи лікарні та громадські організації охорони здоров'я,

повинні мати резервні копії, які дозволять їм швидко відновити обслуговування у разі нападу програми-вимагача.

Основна ідея статті полягає в тому, щоб люди, які працюють з дому, медичні працівники і звичайні користувачі приділяли більше уваги власній безпеці в мережі.

Автор робить висновок, що COVID-19 надає можливість створити кращу цифрову інфраструктуру.

Автор анотацій: Вовк Надія, група УБД-31