TACKLING THE CYBERSECURITY IMPACTS OF THE CORONAVIRUS OUTBREAK AS A CHALLENGE TO INTERNET SAFETY

Kenneth Okereafor
Olajide Adebola

https://www.researchgate.net/publication/339727143

Engl.

The authors describe the influence of coronavirus outbreak on digital behavior.

This part of article outline an importance of using communications for international medical trade, help and worldwide coronavirus statistics.

There is information about the ways China used digital resources to find potentially infected citizens, more precisely creating publicly available data base of infected people and using special ID`s so everyone can check if they had a recent contact with a person considered infected. In case that happened citizens can take a coronavirus test and receive medical care before sickness reaches its peak.

Authors outline possibilities of data alteration and Integrity based attacks as a result of coronavirus breach, also authors are focused on social engineering attacks based on anxiety and despair of people caused by possibility of being infected. Fear of coronavirus gives criminals a variety of methods for making their unhealthy gain. People are anxious to learn how to avoid infection so any message about coronavirus receives easy attention opening new possibilities for scam and internet fraudsters, fake coronavirus websites and malware attacks.

The article provides recommendations for maintaining online safety which include: checking for identity of entities while making online payments, checking for spelling mistakes while accessing websites, paying attention to anything trying to impact your sense of urgency especially referring to coronavirus, being alert about suspicious phone numbers and links, untraceable physical addresses and many other details.

In conclusion authors outline that the panic and anxiety associated with the coronavirus have increased online vulnerabilities and ignited a wave of cyberattacks using social engineering as a tool, whereby cybercriminals are taking advantage of human fear and apprehension to steal confidential information.

Укр.

Стаття Кеннета Окреафорда(Deputy General Manager – Database Security Department of Information and Communications Technology National Health Insurance Scheme(NHIS) Abuja, Nigeria) та Олаїда Адеболи(Chief Technology Officer, Home Plus Services Ltd. Abuja, Nigeria)

Автори описують вплив корона вірусу на цифрові зміни.

Надається інформація про способи, використані Китаєм для попередження інфікування громадян, а зокрема створення єдиної публічної бази даних інфікованих на коронавірус. Завдяки використанню унікальних ідентифікаторів кожен громадянин може перевірити чи не контактував він з інфікованим упродовж останнього часу, що дає можливість пройти перевірку на коронавірус та отримати необхідну медичну допомогу ще до того, як почнуть проявлятися симптоми.

Автори підкреслюють можливість атак на цілісність даних як результат спалаху коронавірусу, також автори звертають увагу на атаки, що використовують соціальну інженерію і направлені на використання стурбованості та відчаю, що викликані можливістю інфікування. Страх перед коронавірусом дає злочинцям велику кількість методів для отримання неправомірної вигоди. Люди стривожені і хочуть дізнатися як уникнути інфекції, тому будь-яке повідомлення у якому йдеться про коронавірус отримує багато уваги тим самим відкриваючи можливості для аферистів і шахраїв, фальшивих веб-сайтів про коронавірус та атак шкідливим програмним забезпеченням.

У статті приведені рекомендації щодо підтримання своєї безпеки в інтернеті, вони включають: перевірку справжності суб’єктів перед здійсненням інтернет платежів, перевірка на наявність граматичних помилок під час відкриття сайтів, уважність до всього, що намагається викликати відчуття невідкладності, особливо по відношенню до корона вірусу, необхідність бути уважним до підозрілих номерів, посилань, фізичних адрес які не вдається відслідкувати та багато інших деталей.

Як висновок автори підкреслюють, що паніка та тривожність викликані коронавірусом посилюють онлайн вразливості та провокують хвилю кібератак з використанням соціальної інженерії як інструменту, завдяки якому кіберзлочинці отримують перевагу на людському страху та користуються нею для викрадення конфіденційної інформації.

Автор анотацій: Самко Владислав, група УБД-31