HACKERS ARE USING CORONAVIRUS FEARS TO SEND YOU A COMPUTER VIRUS: HOW TO STOP THEM

Dalvin Brown

https://www.usatoday.com/story/tech/2020/02/03/hackers-use-coronavirus-spread-computer-viruses-inject-malware/4644439002/

Engl.

The article by Dalvin Brown (Consumer Tech Reporter in USA TODAY) provides information about hackers that are using coronavirus fears to send you a computer virus and how to stop them.

The author claims that Researchers with IBM X-Force and Kasperky have discovered that hackers are sending spam emails to people in the hopes of infecting smartphones and computers with malicious software. The malware is disguised as legitimate information about coronavirus.

According to the author, the emails sent to people in Japan claim that the respiratory illness has infiltrated the country and urge the receiver to open an email attachment to learn more information. If the receiver opens the file, malicious software harvests personal data and can inject into other software. That means hackers can gain access to personal files and copy them.

As conclusion, the article offers honest advice on things you can do to thwart coronavirus-related attacks and other hacking attempts:

1) Always exercise caution. Don't open suspicious links in email and don't download attachments that you didn't ask for.

2) Be sure to only install official updates.

3) Use secure passwords. Two-factor authentication is always a good idea.

4) Run anti-virus software on your devices.

Ukr.

Стаття Далвіна Брауна (Consumer Tech Reporter із видання «USA TODAY») надає інформацію про хакерів, які використовують страх перед коронавірусом, щоб надіслати вам комп’ютерний вірус та інформацію про те, як їх зупинити.

Автор стверджує, що дослідники IBM X-Force та Kasperky виявили, що хакери розсилають спам-повідомлення людям у надії заразити смартфони та комп’ютери шкідливим програмним забезпеченням. Зловмисне програмне забезпечення маскується під законну інформацію про коронавірус.

За словами автора, електронні листи, надіслані людям в Японії, інформують, що респіраторні захворювання проникли в країну, і закликають одержувача відкрити вкладення електронної пошти, щоб дізнатися більше

інформації. Якщо одержувач відкриває файл, то шкідливе програмне забезпечення збирає його особисті дані та може заражати інше програмне забезпечення. Це означає, що хакери можуть отримати доступ до особистих файлів і скопіювати їх.

Як висновок, стаття пропонує поради щодо того, як ви можете запобігти кібератакам, пов'язаним з коронавірусом, та іншим спробам злому:

1) Завжди будьте обережні. Не відкривайте підозрілі посилання в електронній пошті та не завантажуйте вкладення, про які ви не просили.

2) Обов'язково встановлюйте лише офіційні оновлення.

3) Використовуйте захищені паролі. Двофакторна аутентифікація - це завжди хороша ідея.

4) Запускайте антивірусне програмне забезпечення на своїх пристроях.

Автор анотацій: Ющенко Матвій, група УБД-31