FBI Sees Cybercrime Reports Increase Fourfold During COVID-19 Outbreak

The FBI says hackers have a special interest in COVID-19 research.

April 20, 2020 2 min read

This story originally appeared on Engadget

Instances of cybercrime appear to have jumped by as much as 300 percent since the beginning of the coronavirus pandemic, according to the FBI. The bureau's Internet Crime Complain Center (IC3) said last week that it's now receiving between 3,000 and 4,000 cybersecurity complaints every day, up from the average 1,000 complaints per day the center saw before COVID-19 took hold.

While much of this jump can be attributed to America's daily activities increasingly moving online – newly remote workers unaware of basic security measures or companies struggling to keep externally-accessed systems secure, for example – the FBI says a lot of the increased cybercrime is coming from nation states seeking out COVID-19-related research.

As reported by *The Hill*, deputy assistant director of the FBI's Cyber Division, Tonya Ugoretz, said that "Countries have a very high interest in information on the virus … such as information on a vaccine. We have certainly seen reconnaissance activity and some intrusions into some of those institutions, especially those who have identified themselves as working on COVID research."

Health agencies such as the World Health Organization and Department of Health and Human Services have increasingly found themselves the subject of hacking attacks, Ugoretz said, while IC3 has also seen a rise in the number of malicious emails highlighting COVID-19 to trick users into clicking dangerous links. The German government, for example, may have fallen foul of such a scam, potentially losing millions of euros earmarked for COVID-19 financial aid.

The news comes after a group of federal agencies, including the FBI, put out a joint alert on Wednesday warning of potential cyber threats from North Korea. However, Ugoretz said it’s important “not to read into the timing” of the alert, and instead that it was designed to “shine a light” on some of the fresh cyber risks now facing the US.

https://www.entrepreneur.com/article/349509