Cybercriminals Are Coming For Your "Medical Identity"

February 28, 2014 By: Sydney Brownstone Co-Exist

http://www.fastcoexist.com/3026990/cybercriminals-are-coming-for-your-medical-identity

With a growing number of medical devices connected online, our health data is more vulnerable and valuable than ever. And that means people are trying to steal it.

Identity theft is painful. And massive, recent breaches--like when hackers stole millions of Target customers' credit card information--destroy trust. But there's another type of information that cybercriminals may be even more eager to get their hands on: Our medical records, made vulnerable by the "Internet of things."

Barbara Filkins, a senior analyst with the Internet security company SANS, says in a new report, that "medical identity" can actually be far more lucrative than the financial details on a credit card. "A fully compromised identity--meaning I could walk in with credentials and get someone else's insurance to pay for my condition--is worth a couple thousand dollars, versus pennies on the dollar for credit cards. The end game can be a lot more rewarding," she says.

Hacking attempts from the last year prove Filkins's point. Looking at a sample of health care sector data from a global network of sensors, from the threat intelligence firm Norse, SANS registered nearly 50,000 "unique malicious events" or hacking attempts between September 2012 and October 2013. A whopping 375 U.S. health care organizations that had been compromised. An earlier report from 2013 estimated that some 94% of U.S. hospitals had experienced data breaches.

According to the SANS report, many of the recent hacking attempts have been enabled by Internet-connected medical machines. Filkins highlights different biomedical devices, radiology machines, and pharmacy dispensary robots that hold health data and are vulnerable to being compromised. As more of our health records go digital, that vulnerability is only expected to get worse--the Ponemon Institute, for example, estimates that 2 million Americans will pay some $12 billion to deal with medical or insurance theft this year alone.

But what does this mean for the individual? "You can compromise financial records. That can be devastating," Filkins said. "But not life-threatening."

As an example, Filkins cites the story of Anndorie Sacks, whose custody of her children was put in jeopardy when her medical identity had been stolen by a meth user. Filkins, who has dealt with similar cases, also points out the danger of a stolen identity to someone who unexpectedly lands in the hospital--it might be too late, she says, if your records show the wrong blood type.

The report shows that health providers, insurers, pharmaceutical companies, and other organizations simply aren't doing enough when it comes to taking the proper precautions to protect patient data. "It's hard enough trying to recover from identity theft on the financial side, but when it also includes a wrongful diagnosis, that's really bad," she says.