Internet of Things: Security Issues with Smart TVs, Who is Responsible between users and Manufacturers?

Submitted by: Prominence Support
Saturday, 29 February 2020

The common Smart TV operates under the Internet of Things (IoT) ecosystem, a rapidly and conspicuous technological advancement in the contemporary world. Although Smart TV's have become pervasive, this success does not go unnoticed in regards to the attacks and threats on this ecosystem. IoT continues to be intertwined into humanity's life and even a defining aspect of the future society. Recent research carried out by an Appliance Insurance Company Prominence Support (https://www.prominencesupport.co.uk/) showed that just less than 6% of all Smart TV owners in the UK have any anti-virus on their smart TV despite major TV manufacturers like Samsung recommending (https://www.cnet.com/news/samsung-recommends-scanning-qled-tvs-for-viruses/) its TV owners to regularly run anti-Virus. This leaves over 10 Million households at risk.

But again, cyber-attacks are not a new phenomenon with internet-enabled devices. Therefore, to secure our Smart TV's everyone has to step up and consider cyber-defense and protection for these gadgets seriously. In this case, there is a real need for securing Smart TVs and any electronics or gadgets that have been connected to the Internet interface.

Security issues with smart devices span around unauthorized access internally and externally. Hence, any security measure should be directed to protecting the hardware resources, data, and information, both in transit and storage. Data confidentiality is a major issue with Smart TVs. Hence, the security mechanism for avoiding such threats would involve focusing on access control and mechanism of authorization as well as authentication and identity management mechanisms. Privacy with IoT is a serious case because the IoT environment is ubiquitous. This is because there are many entities connected; the data is transferred and communicated. Hence, the user's privacy becomes susceptible and vulnerable to attack. The risks with IoT also emerge because of trust issues. The trust comes about because of the engagement between entities as well as the trust from the user's perception. Trust of IoT, therefore, should involve an individual assessing a Smart TV based on its hardware, processors, sensors, memory, software resources, operating system, power source and applications, and drivers.

An emerging cyber-security issue with Smart TV, as raised by the FBI (https://www.businessinsider.com/smart-tv-security-fbi-warning-2019-12?r=US&IR=T), is that hackers could use them as a conduit for cyber-security and gain virtual access into their homes. Another issue of concern for smart TV's that require security measures is that app developers and TV manufacturers may be listening to watching users. Hence, the TV can easily become a platform for hackers to access your home. This can lead to the most annoying suspicious activities like cyber-stalking the homeowners, or even changing the programs to show violent and explicit content to children.

However, to solve and prevent the security issues, it is upon shoppers to ensure that they have understood the features that come with their smart TVs as well as how these can be controlled before making decisions to purchase the devices. Solely relying on the default security settings of the devices cannot fully and adequately protect the family. It is recommended that one should change passwords, whenever possible and must have the knowledge of turning off the microphones, personal information collected and cameras. If these cannot be turned off, then consideration should be made on whether the

risk is worth it to use the device or service. For example, when unable to turn off the camera, it is advisable to put a black tape on the camera. Other suggestions include checking on the TV manufacturer's privacy policy or the streaming service being used. It also calls for the confirmation of the data collected, how the same is being stored and what they are doing with the data. However, one thing remains; the manufacturer must keep the devices secure and patched. Consumers should not be burdened with the need to be tech-savvy enough to check on permissions, settings and apply patches.

The survey carried out by www.prominencesupport.co.uk was of 2,000 British male & female individuals ages 18 – 55 who own at least one household appliance.
Consider referencing and linking to www.prominencesupport.co.uk when using this research. Prominence Support is not interested in any PR Services.