Smart Toys – A Major Safety Concern

Article by: Bindu Trikha **Published in: IMS Today Sep 2018**

We are moving far ahead in technology but "Are we moving ahead smartly?"

Smart toys for kids are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. We say smart toys are intelligent toys but these toys are actually intelligent in collecting your personal information. These toys contain sensors, microphones, cameras, data storage, and various multimedia capabilities – like speech recognition and GPS options. These hi-tech features could put the privacy and safety of a child at risk due to the large amount of personal information that may be unknowingly disclosed and the data frequently left unencrypted and openly accessible in the cloud and the possibility of hackers exploiting these toys to spy on its users.

Certain toys have microphones that could record and collect conversations through the device. Personal crucial information may be disclosed through normal conversation with the toy or in the surrounding environment. The collection of personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety. Personal information like name, date of birth, pictures, address is generally provided while creating user accounts. In addition, companies may collect additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet usage history, IP address etc. Such toys collect this information, which is further sent and stored by the manufacturer or developer via server or cloud service. The exposure of such information could create a potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos.

The Federal Bureau of Investigation encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their kids hands. Parents should examine toy company user agreement disclosures and privacy practices, and should know where their personal data is sent and stored, including if it's sent to third-party services. In order to make smart toys easily available at competitive prices the security issues are generally not taken into consideration, which may cause harm to child's privacy and physical safety.

Not only internet connected toys pose a great threat to the child's safety and security, the Bluetooth connected devices also poses the same kind of threat. Unprotected Bluetooth-connected toys that do not require PINs or passwords when pairing with a mobile device also pose a significant risk for unauthorized access. Bluetooth connections which lack any authentication protections could be easily used to send voice messages to a child and receive answers. Little technical knowhow is needed to hack into the toys to start sharing messages with a child.

There are certain precautionary measures that can be taken into account while buying Smart Toys - the consumer must know the security issues for any Internet connected toys that they intend to buy, the toy's security measures like Bluetooth authentication and encrypted data transmission, the company behind the toy issues firmware/software updates, in cases where they don't make sure to have it installed and research where data from the toy is stored and whether the company storing it, has a good reputation for security. Before buying smart toys, it is must for every parent to safeguard their kid against possible cyber-attacks. It's time to take the dangers of Smart or Internet-connected Toys seriously and never overlook security safeguards. Safety and security should be the absolute priority with any toy. If that can't be guaranteed, then the products should not be sold and every consumer must also take into consideration these security aspects.

As rightly said prevention is always better than cure. Every consumer must understand the possible negative impacts of the smart toy and make a smarter choice by not letting these hackers harm you and your family. Know the risks. Understand the underlying technology. Be smart and be informed about the new world technologies and their impacts.

Smart Toys - A major safety concern

Bindu Trikha

... The consumer must know the security issues for any Internet connected toys that they intend to buy. These security measures include Bluetooth authentication and encrypted data transmission, the company behind the toy issues firmware/software updates

Smart toys for kids are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. We say smart toys are intelligent toys but these toys are actually intelligent in collecting your personal information. These toys contain sensors, microphones, cameras, data storage, and various multimedia capabilities – like speech recognition and GPS options. These hi-tech features could put the privacy and safety of a child at risk due to the large amount of personal information that may be unknowingly disclosed and the data frequently left unencrypted and openly accessible in the cloud and the possibility of hackers exploiting these toys to spy on its users.

Certain toys have microphones that could record and collect conversations through the device. Personal crucial information may be disclosed through normal conversation with the toy or in the surrounding environment. The collection of personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety. Personal information like name, date of birth, pictures, address is generally provided while creating user accounts. In addition, companies may collect additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet usage history, IP address etc. Such toys collect this information, which is further sent and stored by the manufacturer or developer via server or cloud service. The exposure of such information could create a potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos.

The Federal Bureau of Investigation encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their kids hands. Parents should examine toy company user agreement disclosures and privacy practices, and should know where their personal data is sent and stored, including if it's sent to third-party services. In order to make smart toys easily available at competitive prices the security issues are generally not taken into consideration, which may cause harm to child's privacy and physical safety.

Not only internet connected toys pose a great threat to the child's safety and security, the Bluetooth connected devices also pose the same kind of threat. Unprotected Bluetooth-connected toys that do not require PINs or passwords when pairing with a mobile device also pose a significant risk for unauthorized access. Bluetooth connections which lack any authentication protections could be easily used to send voice messages to a child and receive answers. Little technical knowhow is needed to hack into the toys to start sharing messages with a child. There are certain precautionary measures that can be taken into account while buying Smart Toys. The consumer must know the security issues for any Internet connected toys that they intend to buy. These security measures include Bluetooth authentication and encrypted data transmission, the company behind the toy issues firmware/software updates, in cases where they don't make sure to have it installed and research where data from the toy is stored and whether the company storing it, has a good reputation for security. Before buying smart toys, it is must for every parent to safeguard their kid against possible cyber-attacks. It's time to take the dangers of Smart or Internet-connected Toys seriously and never overlook security safeguards. Safety and security should be the absolute priority with any toy. If that can't be guaranteed, then the products should not be sold and every consumer must also take into consideration these security aspects. As rightly said prevention is always better than cure. Every consumer must understand the possible negative impacts of the smart toy and make a smarter choice by not letting these hackers harm you and your family. Know the risks, understand the underlying technology, be smart and be informed about the new world technologies and their impacts.