Shutterstock Credit ID: 1227984151

Dec 10, 2019 05:24 GMT

Have yourself a secure and connected Christmas

It's that time of year again...

Parents and family members around the globe are scouring the high streets and the web for the perfect child-friendly gifts.

And as the world becomes more connected, it's no surprise that many of this season's must-have kids' toys are boasting connectivity features such as Wi-Fi and Bluetooth.

But it's important to highlight the potential security risks that this connectivity poses before they become a problem.

This is why our research team came together with leading independent consumer body Which? to identify and test seven of the most popular connected children's toys on the market.

Through in-depth testing of the toys' hardware, associated mobile applications and websites, infrastructure and privacy policies, the team discovered 20 security and privacy issues.

While overall, most of the toys tested presented a minimal direct attack surface, the team did discover that three of the toys tested lacked Bluetooth authentication, which could potentially allow strangers to communicate with a child using the device.

As well as this, issues were also identified in the online applications associated with most of the toys, which included plain text website logins, username or email address enumeration, and weak password and online privacy policies. If compromised, this could put personal data at risk.

These issues are something which the Department for Digital, Culture, Media and Sports (DCMS) hoped to address when the Code of Practice for Consumer IoT Security was introduced in 2018. While positive changes are being made, there is still a way to go to ensure that connected products are secure by design, and that device users stay secure in this digital world.

Guidance for parents and guardians

While the onus should never fully lie with parents or guardians, there are several steps that can be followed to ensure that a child is using connected toys safely and securely. This includes:

Checking the product literature

While it's up to the toy manufacturer to clearly communicate the security and privacy measures that are in place, it's good practice to read the product

literature if available. If in any doubt, it might be worth reconsidering the purchase.

Supervising children when using connected toys

It's important to supervise children when using connected toys, wherever possible. This could also include setting up any online accounts with secure passwords, or supervising children when they're using any chat forums associated with the toys.

Powering-down devices when not in use

To mitigate the risk of security issues such as unauthorised Bluetooth authentication, children should be encouraged to turn off devices when not in use, as powered-down devices cannot be exploited. If the child is too young to remember or perform this, parents should try to ensure that toys are powered down when they're not being played with.

So, this Christmas, we're asking for just two things...

1.We want manufacturers to implement important security measures from the outset and commit to the DCMS Code of Practice for Consumer IoT Security.

2.We want parents to be better educated so they can choose the best and most secure toys for their children.

If you'd like to find out more about this research and our key recommendations, head over to our technical blog.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750