**Don’t let Smart Devices Hijack your Christmas**

The Internet of Things Alliance Australia (IoTAA) urges consumers to exercise caution when purchasing smart gifts this Christmas.

“Smart devices, be they wearables, toys, TVs or speakers in your home, have been adopted as tools designed to make our lives easier,” said Matt Tett, Chair of the IoTAA’s Cyber Security work-stream.

“Unfortunately, due to the lack of global agreement on how to secure or regulate smart devices, and their ecosystems, many products are easily accessed by those with nefarious intent.”

Christmas isn’t just a busy period for retailers and resorts. It is a peak period for criminals to take advantage of the all too large security gaps in connected devices.

However, in consumers’ rush to buy Internet connected toothbrushes, toys and toasters, there are some straightforward things they can do to protect themselves from potential security threats.

“In the absence of regulations on connected devices, consumers can exercise a great deal of power to protect themselves. The Internet can be your friend. Before purchasing a gift for family or friends, do your due diligence and search for the item online attaching words like – *vulnerable, security, data breach, privacy, and safety.*  You can benefit from the wisdom of crowds that have fallen prey to compromised devices,” said Tett.

Unfortunately, in the current environment, consumers rather unfairly have no-one else to rely on except themselves when it comes to smart devices. They can strengthen their online security by following some simple guidelines.

**Immediately Change the Default Password**

Before connecting any product to the Internet, turn it on, and change the default password to a strong passphrase. Use different passphrases for each device you connect to the Internet. For added protection if the product allows you to change the default administration username, change that also and then connect to the Internet.

While you’re setting passphrases up, activate automatic updates (patching) if it is available. This will ensure that the product is as up to date as possible without having to manually check regularly. Many of us are unaware or forget to update manually, we are after all human.

**Check Features for Privacy Risks before Connecting**

Many devices have inbuilt microphones, cameras and speakers, so you may want to consider where they are positioned within your home. If we were to entertain disaster fantasies, some of these features could enable others on the internet to record, see, hear and speak from the device. Do we really want the device in our bedroom or the children’s room? It is very important to consider *the placement* of the devices in your home.

**Read the Terms and Conditions**

Please don’t let some devices like Amazon Kindle’s 73,000 word and the nine hours it took CHOICE researchers to read out loud Terms and Conditions deter you. Reading and understanding the T&C’s will show you if they on-sell your data to third parties. So, don’t rush through and tick the agree button on the end user licence agreement without reading the fine print.

“By exercising sound judgement and following a few simple steps, with minimal investment of time, consumers can increase their IoT resilience and enjoy their Christmas, without worrying about receiving an unexpected gift of a security, privacy or safety breach with their purchase,” said Tett.

-Ends-

Media inquiries

Valentina Lazarevska

Mobile 0456 433 076

valentina@freshthinking.expert

*IoT Alliance Australia (IoTAA) is the peak industry body representing the Internet of Things (IoT) in Australia.  Over 500 participating organisations and 1000 individual participants are working to accelerate the adoption of IoT across the Australian economy and society.*