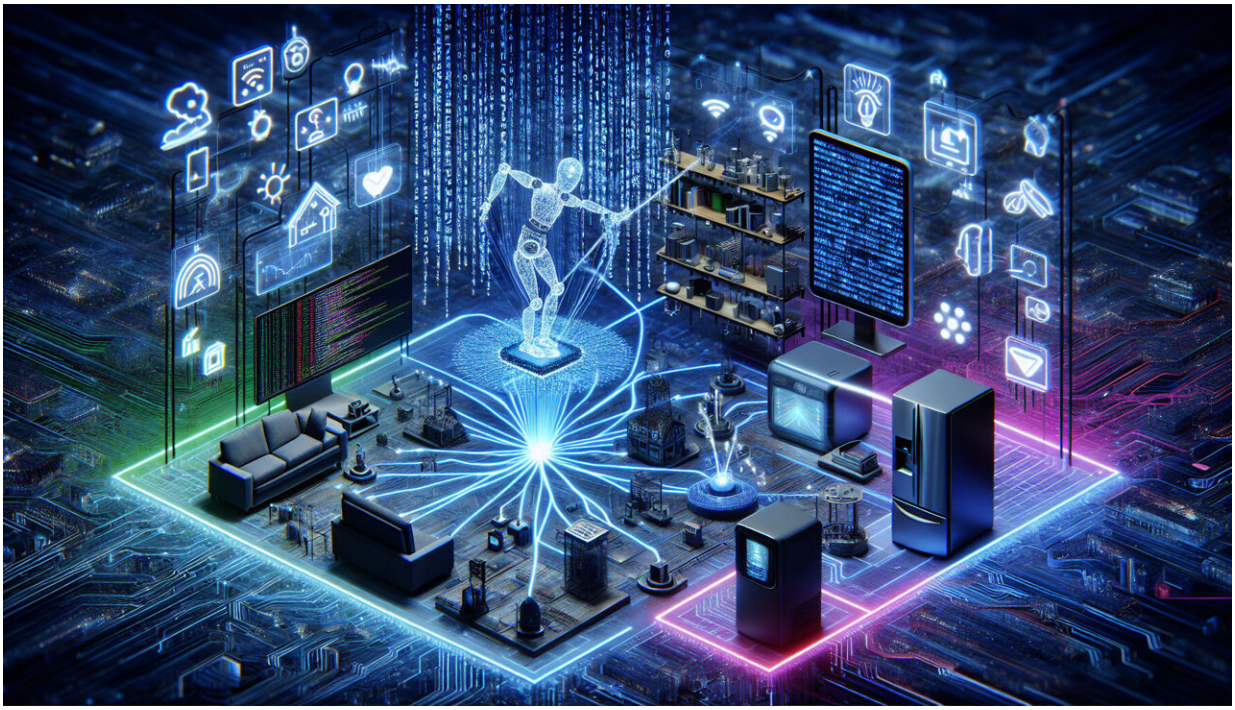
AI is making smart devices easier to hack—here's how to stay safe

April 17 2024, by Chao Chen, Kok-Leong Ong and Lin Li



Credit: AI-generated image

From asking our smart speakers for the weather to receiving personalized advice from smartwatches, devices powered by artificial intelligence (AI) are increasingly streamlining our routines and decision making. The technology is seeping into our lives in subtle ways.

Manufacturers gather vast amounts of user data to ensure these smart devices are responsive and personalized. But this can put users at risk of exploitation by malicious agents, such as hackers looking to steal your data.

As AI becomes more ubiquitous, consumers will also need to become savvier. If you want to enjoy the benefits of a smart everyday device, you should be aware of the safeguards needed to protect you from cyberattacks.

A smarter internet of things

Once we started connecting physical everyday devices like fridges, vacuum cleaners and doorbell cameras to the internet, the Internet of Things (IoT) was born. It is now estimated there are some 17 billion IoT devices worldwide.

IoT devices that existed before AI generally have simpler, more static functionalities, resulting in lower data privacy and security risks. These devices could connect to the internet and perform specific tasks they were programmed to do, such as remotely turning off lights or setting a thermostat.

However, they couldn't learn from user interactions or adapt their functionalities over time. Manufacturers integrate AI into IoT devices to help them "understand" and better cater to user needs and behaviors.

For example, a smart speaker might gather behavioral information by listening to conversations in its environment. This helps it to better understand user preferences and commands, adapt its responses and offer more relevant content or suggestions. Ultimately, this enhances the experience—it makes the device more useful to you.

However, it also makes it less secure. With AI now embedded into such devices, it actually opens a new collection of pathways (known as an "attack surface") for cybercriminals. For example, hackers can use inputs that deliberately cause the AI in the device to malfunction. They can also "poison" the training data of AI models to make them behave in specific ways.

In addition, a malicious attacker can obtain the AI training data through a model inversion attack. If an AI model has been trained on private or sensitive data, replicating this model could potentially expose information that should remain confidential.

Manufacturers should do more

IoT devices have long been vulnerable to hackers due to lack of passwords, lack of encryption or outdated software. With this in mind, smart device manufacturers that prioritize security will implement strong encryption, provide regular software updates and ensure secure data management and transport.

However, users often aren't aware of just how vulnerable their devices might be, or what kind of data they gather and where it goes.

There is a pressing need for industry standards that ensure all devices meet a minimum-security threshold before they come to market.

Manufacturers should provide detailed guidelines on how the collected data is processed, stored and protected. They should also explain any measures to prevent unauthorized access or data breaches.

Governments and industry have recognized the risks and invisible threats posed by AI. We have already seen the significant negative consequences when this is exploited. That is why laws on AI regulation

are being drafted and implemented in Australia and around the world.

In the meantime, consumers must remain vigilant and take proactive measures—to ensure their digital lives bring about more benefit than harm.

How can I protect my devices from cyberattacks?

For a start, review all the devices in your home that connect to the internet. Try to identify AI-powered features, such as learning user behaviors or processing large datasets. These are common in smart speakers, home security systems and advanced wearable technology.

Secondly, explore the functionality of your devices and disable irrelevant or unnecessary AI features. This simple step could prevent AI from gathering personal information and its possible exposure.

Thirdly, when you purchase a device, examine the manufacturer's security disclosure, often found on their website under titles like "Privacy", "Security" or "Product Support". It can also be found in user manuals and, sometimes, directly on the product packaging.

Make sure you understand what sort of AI technology the device uses and how data is collected, processed, stored and protected. What are the safeguards? Did the manufacturer use industry standards or subscribe to strong security guidelines like the European Union's data protection regulation, GDPR?

Security disclosures can vary greatly in terms of clarity. Technical details can be difficult to understand, but information from the Australian government's Consumer Data Right guidelines can help guide your decision.

Asking these questions will help with the selection of devices. Sometimes it is best to pick a manufacturer with a strong track record on security, rather than be swayed by price point alone.

Finally, always keep your IoT devices up to date: when your device requests to install an update, do this promptly. This ensures any security loopholes identified by the manufacturer are properly implemented, closing the opportunity for cyberattacks.

These good habits will go a long way to ensuring your privacy is safeguarded.

Provided by The Conversation

Citation: AI is making smart devices easier to hack—here's how to stay safe (2024, April 17) retrieved 2 May 2024 from https://techxplore.com/news/2024-04-ai-smart-devices-easier-hack.html