HOW IS YOUR SMART DEVICE LISTENING TO YOU?

OCTOBER 2020 **ITSAP.70.013**

Smart devices have become increasingly popular at work and at home. They can connect to other devices, creating a network called the Internet of Things (IoT). Certain devices can control all the other smart devices in the IoT by using voice command services. These devices are called digital assistants. Digital assistants connect to other devices and the Internet to accomplish a variety of tasks (e.g. check the weather, change the thermostat temperature, play music). Your organization should consider the cyber security risks involved with using digital assistants before implementing them on your network.

"HEY…, HOW DO DIGITAL ASSISTANTS WORK?"

Digital assistants come in many different device forms, such as smart speakers, smartwatches, and smartphone applications. Digital assistants respond to human commands through voice recognition. These devices are always listening for a command term (e.g. "Hey, device name..."). Once commanded, the device records your request message and browses for the appropriate response. Over time and use, digital assistants create profiles to identify different individuals who make commands. Digital assistants not only save voice recognition data (e.g. speech patterns and natural language), but they also store data about the resources and the smart devices that they use to fulfill your requests (e.g. the websites visited, the washing machine used, the thermostat temperature regularly set).

ARE THERE RISKS?

Digital assistants are high-value targets for cyber threat actors who are looking to steal sensitive information. Cyber threat actors can take advantage of digital assistant vulnerabilities in the following ways:

- Access personal information and conversation history.
- Eavesdrop on sensitive conversations.
- Monitor and store voice recognition recordings.
- Access other IoT devices on your network.
- Tamper with other connected smart device controls (e.g. temperature, security).

WHAT ARE SOME ATTACK METHODS?

Your digital assistant could be targeted by threat actors through attack methods such as the "dolphin" attack and malware.

"DOLPHIN" ATTACK

The "dolphin" attack broadcasts ultrasonic frequency range noises that trigger the recording feature in digital assistants. These noises can not be heard with the human ear and can be embedded into videos, websites, and other sources to target digital assistants in range. Threat actors use "dolphin" attacks to transfer files, make purchases, and steal sensitive data.

MALWARE

Malware (malicious software) infects digital assistants through downloaded attachments and links (e.g. disguised as an application for additional features), allowing threat actors to access your sensitive information. Malware is very hard to detect and diagnose on digital assistants. Threat actors can use malware to record your voice and use that recording for other malicious activities, such as cracking voice recognition authentication on your devices.

Although digital assistants can create profiles to recognize individual voice commands, they will respond and record any voice command they can interpret.

AWARENESS SERIES

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

WHAT SHOULD I CONSIDER WHEN SELECTING A VENDOR?

It is important to understand and consider the privacy terms and conditions in your vendor's end-user license agreement. Consider the following questions when selecting a vendor:

- Is there an option for a "tap to activate" mode?
- Is there an option to turn off the listening function to safeguard private events and conversations?
- Is there an option to play a tone or turn on a light to notify the user when the device is recording?
- What data is sent to their voice processing service?
- What is returned to request a service or application?
- Who has access to raw voice or parsed text?
- How is retained data used and for how long?
- Is the data generated by the device encrypted?
- Are there opt-out options regarding some features if necessary (e.g. where data is sent, what data is returned and retained, who can access the data)?

Research reviews and security ratings on vendors to make note of any history with their databases having vulnerabilities or their storage facilities being breached.

WHERE CAN I LEARN MORE?

If you want to learn more about cyber security, visit the Cyber Centre website (**cyber.gc.ca**) to find our catalogue of publications and other resources, including:

- *ITSAP.00.057 Protect Your Organizations from Malware*.
- *ITSAP.00.012 Internet of Things Security for Small and Medium Organizations*
- *ITSAP.80.101 Virtual Private Networks*

HOW DO I SECURE MY DEVICE?

When setting up your digital assistant, you should identify what information (e.g. higher sensitivity) your smart devices can access via your network. Depending on your organization's security requirements, you may even want to isolate the digital assistant on a separate network, such as a guest network, to protect your main network should a compromise occur. You should also consider some of the following best practices to secure your device:

- Use a password on your digital assistant that is different from any other device or account you own.
- Set a PIN on your digital assistant to prevent unauthorized use of the voice assistant.
- Turn off your digital assistant if personal or sensitive information needs to be discussed in its vicinity.
- Disable the access features for digital assistants to perform security sensitive operations (e.g. unlocking doors or camera controls).
- Disconnect remote access functions on devices if you don't need it (e.g. smart cameras).
- Update and patch software and firmware frequently.
- Use a virtual private network on the network your digital assistant is connected to.

Be cautious about the type of information you are sharing with digital assistants and within listening range of them.

WHAT IF I'VE BEEN HACKED?

If you suspect malicious activity on your digital assistant and smart devices, you should take the following steps:

1. Disconnect the IoT device immediately from your network.
2. Contact your service provider to locate the point of intrusion and determine what data has been compromised.
3. Perform a factory reset and immediately update your device with the latest available version.
4. Scan your network and IoT devices with anti-virus software.
5. Report activity to the Cyber Centre: **contact@cyber.gc.ca**

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**