Tips on protecting devices from hackers

November 15 2016, by Tami Abdollah

Robert Silvers, Assistant Secretary for Cyber Policy with the Department of Homeland Security, speaks to members of the Coalition for Cybersecurity Policy and Law in San Francisco, Tuesday, Nov. 15, 2016. The Homeland Security Department urged the technology industry to begin immediately securing millions of internet-connected devices that increasingly permeate daily life, including fitness trackers, medical implants, surveillance cameras, home appliances, digital video recorders, thermostats, baby monitors and computers in automobiles. It proposed no penalties for manufacturers that do not comply. (AP Photo/Jeff Chiu)

Billions of fitness trackers, medical implants, surveillance cameras, home appliances, thermostats, baby monitors and computers in automobiles now are connected as part of a rapidly expanding "internet of things."

But many such devices were developed without security considerations. As a result, they are prime targets for hackers.

Read: In world of internet-enabled things, US says security needed

Here are tips to protect your devices:

HOW DO I KNOW IF I HAVE AN "INTERNET OF THINGS" DEVICE?

If you have a device that is capable of connecting to the internet or shares information over a wireless network in your home, it is potentially insecure and can be leveraged for a cyberattack.

Last month, hackers harnessed an army of 100,000 internet-connected devices around the world, such as DVRs and security cameras, to attack Dyn Co., which helps route internet traffic to its destination. It caused temporary internet outages to sites that included Twitter, PayPal, Pinterest, Reddit and Spotify.

WHY SHOULD I CARE?

Hackers can penetrate devices to directly harm someone or to target critical infrastructure.

They can remotely disable a car, raise the thermostat on refrigerated foods, and toy with internet-enabled medical devices.

In the Dyn attack, hackers used the devices to flood the internet infrastructure company with data and knock it offline.

Such tactics also could be used against electrical and water systems, which are increasingly being put online to allow for remote operation.

WHAT CAN I DO?

Make sure you are aware of what you are connecting to the internet, and think about what is necessary.

That feature on your new bathroom scale that syncs with your phone is handy, but can you password protect it from getting hacked?

Any device that has the capabilities of remotely sending information elsewhere is vulnerable. Therefore, the software on that device and the network in connects to must be secured.

If a device comes with a default password, make sure you change it. You should also change the password on your wireless network at home. Use complex passphrases to ensure your device is not easily hacked.

The Dyn attack was made possible by devices with default passwords that were never changed.

WHOM DO I CONTACT IF I AM WORRIED ABOUT A DEVICE?

Contacting the manufacturer or vendor of the device may not always help.

This is especially true because innovation has frequently outpaced cybersecurity education.

The Homeland Security Department sends out public alerts about vulnerabilities through its US-CERT program that you can sign up for on its website .

You can also contact the department directly.