Use Caution With Smart Devices

Almost all home appliances now include some kind of smart feature. Smart cameras that warn you about snoopers, smart locks that keep them away. You can remotely change your room temperature and lighting, start toasting or cooking, check your fridge contents, or vacuum the floor. Meanwhile, Alexa, Google, or Apple will control all Internet of Things (IoT) devices.

However, IoT devices often have firmware that is outdated or contains an unpatched vulnerability. It's not unusual for patching or updating to fall to the bottom of the average homeowner's priority list. Each new smart device creates a new vulnerability at home by providing a fresh attack vector for attackers. And some devices could cause actual physical harm. Many IoT devices are very hackable, and manufacturers aren't making serious efforts to secure their devices against attacks," said Roger Grimes, a data-driven defense evangelist at security awareness training company KnowBe4.

Here are 5 devices could cause the most harm if left connected and unchecked.

1. **Home safe – do you want hackers to know you have one?**
   Some home safes for storing valuables can be locked and unlocked with your phone and even notify you if they detect false access attempts. And they even come cheap. But is this a bargain worth chasing? Because for cybercriminals, it can act as a beacon, signaling where they can find treasure. "The main item I would never want to be connected to the internet is a home safe. If a hacker knows the basic fact that you own a safe, it could create a potential threat to you and your family," said Kobi Kalif, CEO and Co-Founder of cybersecurity developer ReasonLabs. While it is possible to have a relatively safe system connected to the internet, many users won't have it configured correctly. "We must choose carefully what we enable these smart devices to do," Kalif warned.

2. **Smart ovens or stoves can burn your savings and your entire house**
   Almost all cyber pros mentioned microwaves and traditional ovens, stoves, and toasters as devices to keep offline. "I think any device that has the potential for causing serious harm should be avoided. For example, I'm fine with my refrigerator being connected, although I suspect a hacker might be able to maliciously play with food sensors to let my food spoil. But I definitely don't want my oven connected until I know for sure that there's no way for a hacker to turn my oven on, heat it to a high temperature, and leave it on. Same with a toaster," said Grimes. He warns that such devices in the remote hands of malicious actors can "These devices can create a ton of heat. If accessed by a bad actor, that ability could create a physical risk to the home and the people inside. Or such devices could be used by a cyberbully to annoy someone or raise their utility bills," Ribeiro said. Matthew Carr, Co-founder and CTO at cybersecurity risk assessment company Atumcell Group, also agrees and sees only minimal practical benefits the smart oven offers, but they increase the attack surface. physically harm the family. And the oven companies aren't exactly proven to have the best security measures.

3. **Smart security, baby cameras and smart doorbells**
   While all internet-connected devices have vulnerabilities, cameras have a terrible reputation for leaking private sensitive information, and, even worse, they can be entry points for hackers. "For example, in 2020, over 50,000 home cameras

were hacked, leading the footage to be posted online," Kalif shared. Homeowners appreciate the option to review recordings and provide the footage to law enforcement if something happens. However, according to Ribeiro, this functionality often requires device providers to keep footage on the cloud, giving bad actors direct and often live information about what happens in the home.mEven camera vendors cannot be trusted with private information that could be easily sold to marketing data brokers. Smart baby monitors are even worse. "Strangers have been known to interact with children via cloud-based baby monitors. As a parent in cybersecurity and privacy, this is not a risk I take or would recommend anyone else take," Ribeiro said. Cybernews already reported that many IP camera owners have their devices exposed online and accessible to anyone.

4. **Door locks and garage doors can break digitally**
   Smart locks and garage doors are both risky and useful to cyber pros. Physical vulnerabilities apply to all locks, but only smart locks are vulnerable to cyber threats. Smart locks are "vulnerable to hacking and can compromise physical security," warned Anurag Gurtu, CPO at StrikeReady. Carr agrees: "These can be a risk if their security isn't robust, as they control physical access to your property." However, not everyone thinks that smart locks should be avoided. "Smart locks provide real benefits. Being able to lock or unlock doors remotely can be very beneficial, especially with small children at home. Consider setting up a VPN to access these devices remotely. This way, you can easily add additional security measures, requiring MFA, to access what may otherwise be a very insecure IoT device," argues Josh Amishav, Founder and CEO at Breachsense.

5. **Devices with access to water, heating, electricity**
   Intelligent water systems, smart washing machines or dryers, and smart thermostats offer convenience and sometimes can significantly improve energy efficiency and comfort. There were some disagreements among cyber experts on whether it is best to use them. "Smart thermostats can help homeowners save money on energy bills, and smart lights can be controlled remotely," said Damir J. Brescic, CISO at Inversion6. If properly protected, intelligent air conditioning and heating systems have shown their value in predicting when users want the temperatures to go up or down during the day and night. However, Carr warned that those could also be exploited to infer when a house is empty, leading to significant losses or damages. He would keep washing machines and dryers offline as they offer limited benefits compared to the risks. For users to decide before installing smart systems for water, energy, and even fire/gas detectors, Grimes offered an analogy with cars: car manufacturers make significant efforts to ensure that hackers cannot manipulate critical systems like brakes, speed, and the engine. However, any potential harm would be less severe if a hacker were to disrupt non-critical systems, such as the radio station. "The same thing is needed for any device in your house that has the possibility of harming it," he said.

Do what the cyber pros do – avoid smart devices altogether if there is really no need for them, and disable the features you don't use.