

**Smart Thermostat Technology Vulnerable to Hacking and Security Breaches**

In recent years, many consumers have adopted “smart” home technologies, which utilize the modern ubiquity of Internet connectivity to provide users with greater control over, among other things, home security and energy usage. In particular, smart thermostats have provided consumers with far greater control over their home energy usage, enabling users to adjust home heating and cooling systems with greater ease and specificity. For example, smart thermostats may be remotely adjusted to reflect changes in weather conditions while a homeowner is away on vacation or at work. Like any other Internet-enabled technology, however, smart thermostats and home security systems are vulnerable to malicious cyber activity than can wrest control of such technology from the actual user.

A string of recent media reports concerning the popular Nest thermostat and related Nest products have raised public concern about the vulnerability of smart home technologies currently available on the market. Several users have reported that their systems were remotely hacked, resulting in smart thermostats that were turned up to [dangerously high levels](https://www.nbcchicago.com/investigations/My-Blood-Ran-Cold-as-Smart-Cameras-Thermostat-Hacked-Homeowner-Says-505113061.html), home security devices broadcasting [false warnings](https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/) about impending missile strikes, and a hackers using a smart baby monitor to issue obscene expletives and threaten to [kidnap a user’s infant child](https://abc7news.com/baby-cam-monitor-hack-and-kidnapping-threat-serve-as-warning-for-tech-security/4940379/). Nest—which is owned by Google’s parent company Alphabet—has denied that its systems were compromised and placed blame for such incidents on poor security practices by users.

Consumers with smart thermostats and other smart home devices should take precautions to minimize the possibility of their technology being hacked or otherwise compromised. The best way to prevent unauthorized access to a smart home device is to choose a password for the device that is entirely unique and not in use—either past or present—for any other online account or WiFi enabled device. Personal email addresses and user passwords gleaned from data breaches are sold to hackers for low cost on the Dark Web and the repeated use of the same or similar passwords by a consumer increases the chances that a hacker may gain illicit access to that consumer’s smart technology. Likewise, consumers should ensure that two-factor authentication (2FA) settings are enabled on smart home devices to ensure that only authorized users can access the device. Furthermore, physical access and passwords to smart devices should only be shared by consumers with trusted individuals.

The smart home technology industry is still in its early stages and it is likely that as time goes on and smart devices gain more traction among consumers, greater security features will be developed to address the vulnerabilities that are only now emerging. Nonetheless, consumers should always be proactive about home cyber security in order to protect themselves and their property, as well as to make full use of the benefits of smart home devices.

Please visit [OCC’s website](http://www.ct.gov/occ/site/default.asp).