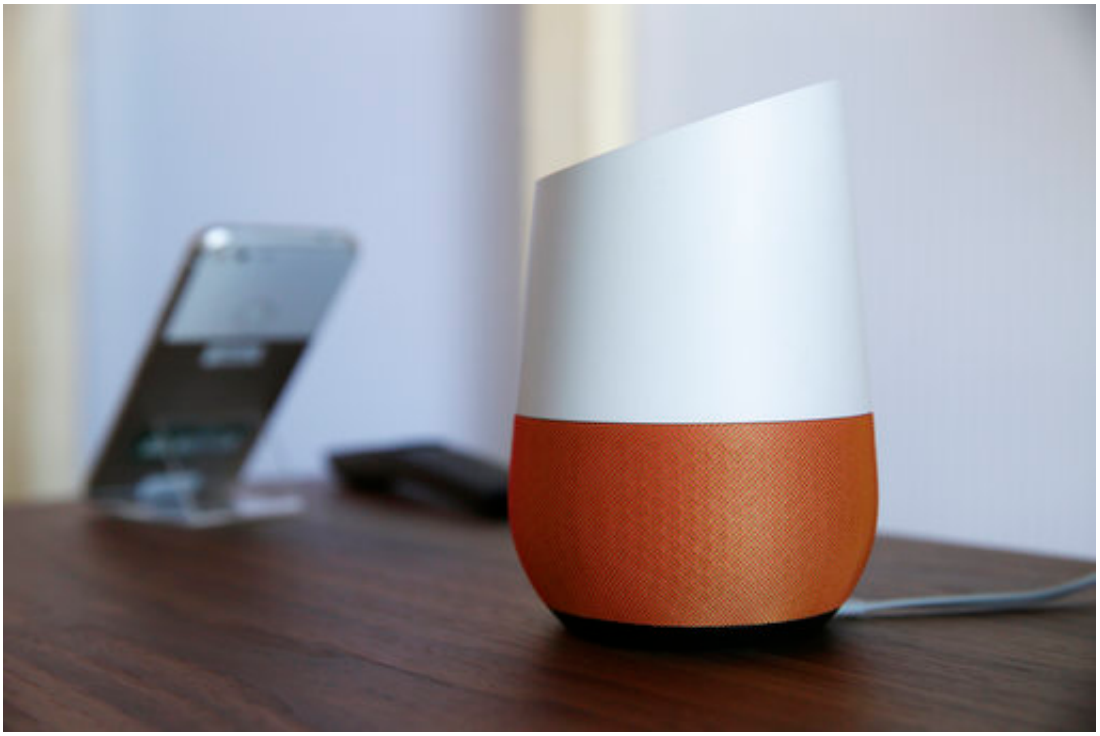
How Burger King revealed the hackability of voice assistants

May 5 2017, by Mae Anderson



In this Tuesday, Oct. 4, 2016, file photo, Google Home, right, sits on display near a Pixel phone following a product event, in San Francisco. Voice assistants such as Google Home, Apple's Siri and Amazon Alexa have always been susceptible to accidental hijack. Burger King's manipulation of Google Home illustrates the vulnerabilities intrinsic to voice assistants that can be targeted by brands, or worse, hackers. But the stunt might help speed up the next developments for home voice assistants: individual voice recognition and even image recognition. (AP Photo/Eric Risberg, File)

Burger King pulled a pretty juicy marketing stunt last month that drew plenty of attention—not just to the Whopper, but also to the intrinsic vulnerabilities of a new type of voice-activated gadget.

The fast food chain's 15-second television ad targeted Google Home, a speaker that can answer questions and control other smart appliances. When an actor in the ad said "OK, Google" and asked a question about the Whopper, Google Home obediently began reading the burger's ingredients in homes around the country—effectively extending the commercial for however long it took someone to shout "OK, Google, stop!"

Google and Wikipedia quickly made fixes to shut it down. Though annoying, the stunt may have done some good by highlighting how easy it is to hijack such devices. (Just imagine a burglar spying a voice assistant and asking it to unlock all the doors.) It could also speed the development of home voice assistants with better security.

"It's a wakeup call," said Earl Perkins, a digital security analyst at the research firm Gartner. "It's a harbinger of things to come."

TRIGGER WARNING

Voice assistants such as Google Home, Apple's Siri and Amazon's Echo devices have always been susceptible to accidental hijack. A Google ad during the Super Bowl that used the phrase "OK, Google" reportedly set off people's devices. And in a January story that briefly turned a family into media celebrities, a woman's 6-year old daughter ordered a dollhouse and sugar cookies simply by asking Amazon's voice assistant Alexa for them.

Since the devices are so new—the Amazon Echo debuted in 2015, Google Home last year—they're still having growing pains. And they're

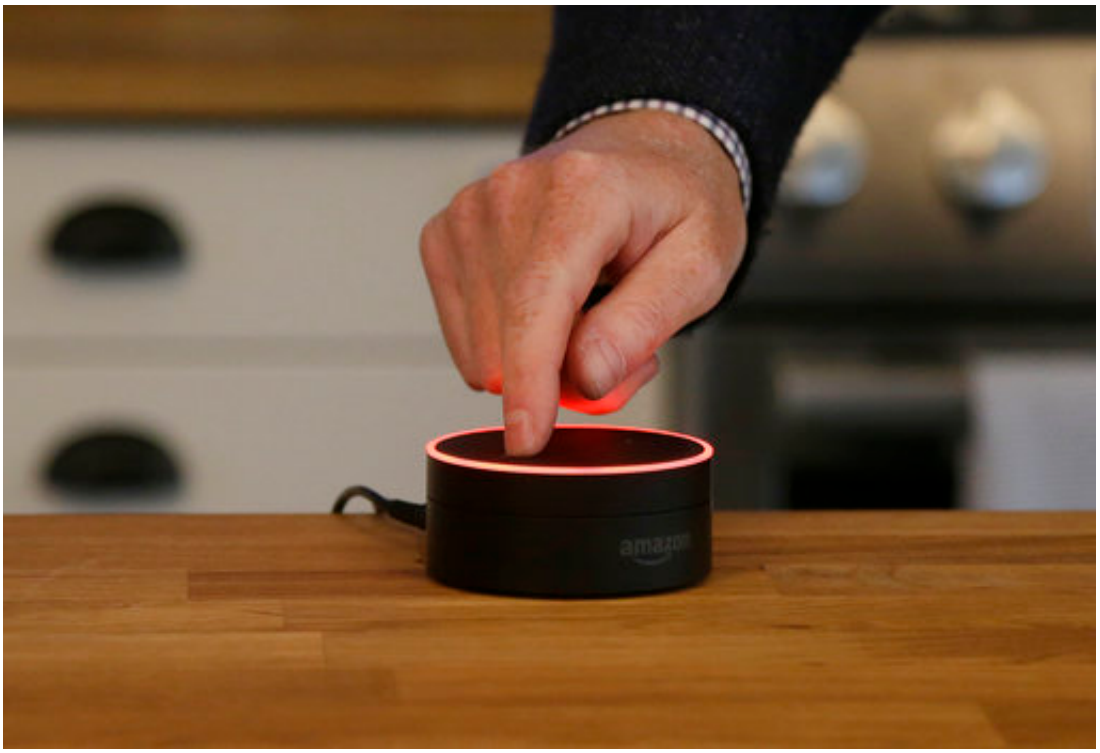
growing in popularity; Consumer Intelligence Research Partners estimates that Amazon sold 3 million Echo devices in the U.S. in the fourth quarter of 2016, bringing the total to more than 8 million. Amazon doesn't release sales figures.

Many experts believe that deliberate attempts to trigger voice assistants will be short-lived. Among other things, brands have to face the consequences of potentially annoying millions of people.

"Burger King was doing what the Burger King brand is known to do, stir controversy and make sure it gets lots of coverage," Forrester principal analyst James McQuivey said. "Very few brands want to do that."

Of course, spammers and other bottom-feeding marketers can still try to implement the technique. But voice assistants already have a few ways to block them.

THREATS AND COUNTERMEASURES



In this March 2, 2016, file photo, David Limp, Amazon Senior Vice President of Devices, pushes down on an Echo Dot in San Francisco. Voice assistants such as Google Home, Apple's Siri and Amazon Alexa have always been susceptible to accidental hijack. In January 2017, a woman's 6-year old daughter ordered a dollhouse and sugar cookies simply by asking Alexa for them through an Echo Dot. Since these devices are still new, they're still having growing pains. But the next generation of voice assistants may come with better security, including individual voice recognition and even image recognition. (AP Photo/Jeff Chiu, File)

Amazon already makes sure its TV commercials and those of its partners can't inadvertently trigger the speaker. Developers that provide Echo with "skills" that let it, for instance, order pizza, are also prohibited from creating Alexa commands that would trigger ads. Google says it also has techniques to block TV ads from activating Google Home. Neither company provided details on those techniques.

Voice assistants are still in their "very early days," Google says; the company plans to "monitor and learn as we go."

Hackers might also be a threat. But because voice assistants are so new and limited in scope, more established connected devices such as webcams, routers and printers pose more of a threat for now.

"It's not that we won't see some creative or unique instance (of hacking), but I don't think this is going to be the next great wave of cybercrime," said Steve Grobman, chief technology officer at the security company McAfee.

MORE SECURITY TO COME

But before long, the devices are going to need better security. "When you move into a world of voice, some of the rules that we're accustomed to, related to security for computers, change," Gartner's Perkins said.

Exactly how that works could depend on exactly what task a voice assistant is performing. Asking about the weather requires less security than say, shopping or accessing a bank account.

Amazon already has options for setting up security codes to shop, make financial transactions or unlock and start cars.

Of course, someone could always overhear you reciting a security phrase. A better solution, and one that companies are hard at work on, would be to identify a person's voice, much the way Google and Facebook identify faces today. Beyond improving security, that technology could help the device personalize recommendations or even ads for the individual, not the whole family.

Apple already lets users voice-train its Siri digital assistant so it's more

likely to activate only when it hears a specific voice. Amazon has a voice training option for Alexa. Google Home can recognize up to six different voices, though it won't prevent unauthorized users from activating the assistant.

Experts suggest that companies will eventually add cameras to voice assistants. Amazon's new Echo Look has a camera, but it's for offering fashion advice. Combining a facial scan with voice recognition would definitely beef up security, although they'll also create new privacy concerns.

"Without any security or minimal security, (voice assistants are) going to be a fat target," Perkins said. "There will be all kinds of innovation associated with compromising these systems."