Security company says a mask fooled Face ID on iPhone X

November 15 2017, by Tim Johnson, Mcclatchy Washington Bureau

Less than a week after the Apple iPhone X went on the market, a cybersecurity firm said it had already defeated the new phone's vaunted face recognition system using a $150 mask made on a 3-D printer.

"Apple Face ID is not an effective security measure," a Vietnam-based cybersecurity firm, Bkav, said in a statement and video on its website.

But U.S. security experts aren't as quick to dismiss the security of the device. The iPhone X, which became available Nov. 3, has numerous other security functions that would make most such methods impractical for all but the most dedicated criminals, and perhaps still unachievable, those experts said.

For most people, according to Terry Ray, chief technology officer at Imperva, a Redwood Shores, Calif., cybersecurity firm, "Face ID is probably just fine."

It's a key debate in the ongoing evolution of biometrics to verify users of computers and other devices and allow them to make purchases and sign into apps with a simple action.

Motorola introduced fingerprint readers on a smartphone in 2011, and Apple followed in 2013 with Touch ID on its iPhones. Most major smartphone makers now use such sensors.

Face recognition is the next iteration of biometric identification. At a presentation announcing iPhone X's face recognition capabilities Sept. 12, nearly two months before its Nov. 3 release, Apple Senior Vice President Phil Schiller said engineering teams developed artificial intelligence to help the product distinguish between real owners and masks.

"They have even gone and worked with professional mask makers and makeup artists in Hollywood to protect against these attempts to beat Face ID," Schiller said.

Apple says the iPhone X uses infrared imaging and a depth map of a

user's face with 30,000 invisible dots to ensure identity. It says chances that a random person could grab the phone and unlock it are one in a million, and that the phone recognizes if its owner is asleep to prevent someone from unlocking the phone without the owner's knowledge.

Face ID allows users to unlock the iPhone X by looking at it, then make purchases from the Apple store or conduct other Apple Pay transactions using stored payment-card data.

The Vietnamese cybersecurity firm said it obtained an iPhone X Nov. 5 and immediately began using a 3-D printer to create a mask of the iPhone's owner. It said in a statement that an artist fashioned the mask's nose by hand and that artificial skin was also made by an artist.

It said the approximate cost of the mask was $150. The firm said it only intended to show a "proof of concept" that Face ID can be skirted and that such techniques would not target regular users but more likely "billionaires (and) leaders of major corporations."

Bkav did not give details of how long it took for its iPhone X to unlock with the mask. The iPhone model requires a six-digit alphanumeric passcode if a user makes five unsuccessful attempts to match a face.

"What they didn't disclose was how many attempts and what level of effort it took to get the mask to work flawlessly," Paul Norris, senior systems engineer at Tripwire, a Portland, Ore. software security company, said in a statement Monday.

"In order to compromise Face ID authentication, the attacker would have to have a detailed map of the face of the user, create a mask that would map the exact details of the victim's face, unlock the phone within five attempts, and do all of this within 48 hours. This seems like an unlikely sequence of events," Norris said.

Face recognition doesn't work if the iPhone X has been locked for two days.

"The attacker has 48 hours to unlock the phone so they can't spend too much time working out fixes for their five tries or else the phone locks with a passcode," Ray said.

Apple declined to comment on the controversy beyond a statement on its website that noted Face ID's security features, which it said involved "some of the most advanced hardware and software that we've ever created."