Maasm

We Broke Into A Bunch Of Android Phones With A 3D-Printed Head

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

Facial recognition is cropping up everywhere. From shopping malls to the workplace, it's likely something is scanning your face every day. But rather than invade your privacy, facial recognition on smartphones is supposed to protect your digital life from snoops.

If you're an Android customer, though, look away from your screen now. We tested four of the hottest handsets running Google's operating systems and Apple's iPhone to see how easy it'd be to break into them. We did it with a 3D-printed head. All of the Androids opened with the fake. Apple's phone, however, was impenetrable.

Two heads are better...

The head was printed at Backface in Birmingham, U.K., where I was ushered into a dome-like studio containing 50 cameras. Together, they combine to take a single shot that makes up a full 3D image. That image is then loaded up in editing software, where any errors can be ironed out. I, for instance, had a missing piece of nose.

Backface then constructs the model with a 3D printer that builds up layers of a British gypsum powder. Some final touch-ups and colourings are added, and the life size head is ready within a few days, all for just over £300. You're then the proud owner of an uncanny, almost-spectral version of your own visage.

A 3D-printed head being made at the Backface studio in Birmingham, U.K. FORBES

For our tests, we used my own real-life head to register for facial recognition across five phones. An iPhone X and four Android devices: an LG G7 ThinQ, a Samsung S9, a Samsung Note 8 and a OnePlus 6. I then held up my fake head to the devices to see if the device would unlock. For all four Android phones, the spoof face was able to open the phone, though with differing degrees of ease. The iPhone X was the only one to never be fooled.

There were some disparities between the Android devices' security against the hack. For instance, when first turning on a brand new G7, LG actually warns the user against turning facial recognition on at all. "Face recognition is a secondary unlock method that results in your phone being less secure," it says, noting that a similar face can unlock your phone. No surprise then that, on initial testing, the 3D-printed head opened it straightaway.

Yet during filming, it appeared the LG had been updated with improved facial recognition, making it considerably more difficult to open. As an LG spokesperson told *Forbes*, "The facial recognition function can be improved on the device through a second recognition step and advanced recognition which LG advises through setup. LG constantly seeks to make improvements to its handsets on a regular basis through updates for device stability and security." They added that facial recognition was seen as "a secondary unlock feature" to others like a PIN or fingerprint.

There's a similar warning on the Samsung S9 on sign up. "Your phone could be unlocked by someone or something that looks like you," it notes. "If you use facial recognition only, this will be less secure than using a pattern, PIN or password." Oddly, though, on setting up the device the first presented option for unlocking was facial and iris recognition. Whilst iris recognition wasn't duped by the fake head's misted-over eyes, facial recognition was tricked, albeit with a need to try a few different angles and lighting first.

The Note 8 has a feature to turn on "faster recognition," which by the manufacturer's own admittance is less secure than the slower option. It didn't matter in this case as the head unlocked on both settings, though it did take a little more effort with lighting and angles with the slower option. The same went for the slower versions on the S9 and the LG, the latter proving trickier to break into. (A Samsung spokesperson told *Forbes*: "Facial recognition is a convenient action to open your phone – similar to the 'swipe to unlock' action. We offer the highest level of biometric authentication – fingerprint and iris – to lock your phone and authenticate access to Samsung Pay or Secure Folder.").

The OnePlus 6 came with neither the warnings of the other Android phones nor the choice of slower but more secure recognition. And, despite some sci-fi style

face scanning graphics when registering a face, the phone instantly opened when presented with the fake head. It was, undoubtedly, the least secure of the devices we tested.

A OnePlus spokesperson said: "We designed Face Unlock around convenience, and while we took corresponding measures to optimize its security we always recommended you use a password/PIN/fingerprint for security. For this reason, Face Unlock is not enabled for any secure apps such as banking or payments. We're constantly working to improve all of our technology, including Face Unlock."

No such luck with the iPhone X, though. Apple's investment in its tech - which saw the company work with a Hollywood studio to create realistic masks to test Face ID - has clearly paid off. It was impossible to break in with the model.

Microsoft appeared to have done a fine job too. It's new Windows Hello facial recognition also didn't accept the fake head as real.

Little surprise the two most valuable companies in the world offer the best security.

Use your head, not your face

Anyone worried about anyone having their device compromised with a fake head, either through our method or others', should perhaps consider not using facial recognition at all. Instead, use a strong alphanumeric passcode, recommended Matt Lewis, research director at cybersecurity contractor NCC Group.

"Focus on the secret aspect, which is the PIN and the password," he added. "The reality with any biometrics is that they can be copied. Anyone with enough time, resource and objective will invest to try and spoof these biometrics."

Got a tip? Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes. Email at TBrewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail.

Thomas Brewster Forbes Staff

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for Th... **Read More**