

# Can strangers unlock your phone with Face ID? How to prevent this?

If you use facial recognition on your smartphone, the face of a sibling or someone like you can also be unlocked.

Although many smartphone manufacturers try to create their own unique algorithms, security with facial recognition is sometimes problematic. Why is that? We will find the answer below.

## How does facial recognition on phones work?

Many facial recognition systems work with infrared scanning instead of the visible spectrum, which is controversial because it cannot scan your face in the dark.

In general, face unlock works by using the front camera to assess the unique patterns and contours of your face. After scanning, it saves your facial details into memory and converts them into some mathematical expressions. The smartphone then compares that information with your face to authenticate secure access the next time you try to unlock it with your face.

However, most facial recognition technologies today combine infrared emission spectra with actual algorithms. And they collect facial images as 2D arrays. The idea behind this is to prevent image hacking to unlock.

Finally, infrared radiation allows the phone to accurately scan your face, even in the dark.

## Why can facial recognition be problematic?

Of course, conventional visible-spectrum camera scanning has some flaws. It can even scan and allow access with the face of a loved one or a stranger. Plus, it has a higher chance of failure and you can fool around with a photo of yourself.

But that technology is no longer used in modern smartphones. However, even the technology that is in vogue today sometimes has flaws.

So while it's not possible to detail how and why the facial recognition feature of every smartphone out there sometimes crashes, let's look at the possible causes over a few. For example.

### **Samsung's Iris technology is accurate but can be fooled**



Samsung's iris scanning technology, starting with the Galaxy S8 and S8+, has chosen a point on the face to improve the security of the phone. This technology works by scanning for unique patterns in your iris.

Since each individual's iris pattern is unique, Samsung has claimed this to be an anti-deception technology. Unfortunately, there is some potential error with this scanning method as you can still fool it by wearing contact lenses.

And despite combining 2D imaging with iris scanning in more recent versions like the S21 series, Samsung warns that using facial recognition isn't as secure as using a PIN or fingerprinting.

The company also recommends against using this feature with online payment and money transfer platforms.

### **Why is Huawei 2D Live Detection not completely secure?**

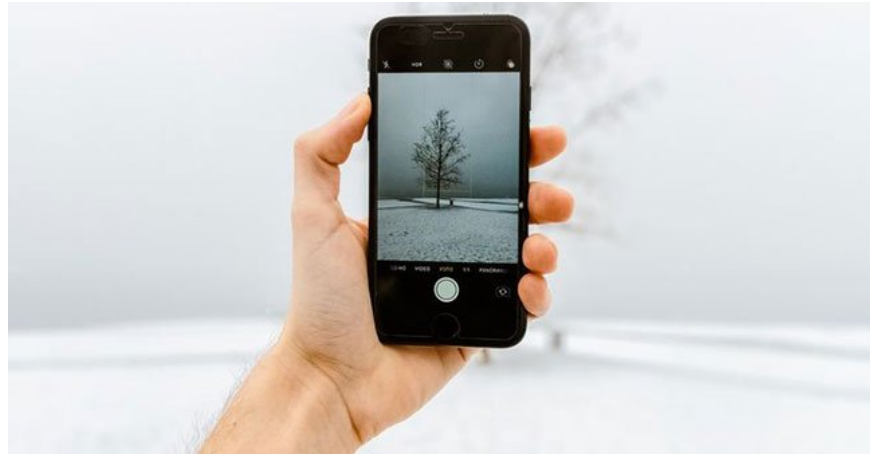
Huawei, which uses open source Android cores, is another popular example of facial recognition. The company first introduced its facial recognition security feature in the P20 series and has since added the feature to other products such as the 2018 Mate 10 and Y series.

Huawei uses 2D live recognition technology, similar to how facial recognition works on other Android phones.

That technology makes it hard for anyone to unlock their smartphone with a photo, as it doesn't work without some facial action like blinking. Therefore, your phone may not open if you do not follow the rules, even with the correct face scan.

In addition, this feature depends on the current status of the front camera on the smartphone. So sometimes someone who looks like you can still open a smartphone. Of course, a poor camera can further undermine the accuracy of the setup.

### **Why can the trusted Apple Face ID be in trouble?**



Apple's Face ID, which debuted with the iPhone X in 2017, remains the most advanced smartphone facial recognition system available today.

In contrast to the 2D infrared iris scanning technology of Huawei and Samsung, Apple takes a 3D image of your face using the TrueDepth camera system instead of a front camera.

Apple's TrueDepth technology combines infrared capture with sensors and scanning components. It then uses these to analyze more than 30,000 dotted areas of the face during the scan to create facial depth.

Your iPhone learns, remembers, and recognizes these patterns, so a mere photo or anyone's face can't fool it.

Apple's Face ID works by adapting to changes in your facial expression and appearance over time. That contrasts with the one-time iris facial recognition and helps it work more accurately.

Surprisingly, Apple's Face ID sometimes successfully unlocks the phone after scanning someone with a strong resemblance to the original owner. But how?

Apple claims that there is only a one in a million chance of someone else's face opening your iPhone. But it also warns that the chances are higher with identical twins, siblings and children whose facial structures are not fully developed.

That's because Face ID learns more about your face each time you enter your Apple passcode: It can pick up different facial patterns to authenticate and unlock your iPhone the next time someone else holds it. . Revealing your passcode to someone could result in a security breach, and they may not need the passcode to unlock your iPhone in the future.

## **How to prevent strange faces from unlocking your device**

While the facial recognition error on your smartphone isn't your fault, there are ways to prevent it if you use the feature.

Errors on iPhones could be the result of algorithms learning other people's facial patterns. To prevent this, you should not share your Apple ID with others. And be careful not to open your iPhone with your Apple ID when someone looks like you, like a sibling.

If your Face ID feature has failed, go ahead and delete that Face ID data by going to Settings > Face ID & Passcode > Reset Face ID. This will remove your face from memory, including all the stored math algorithms

that set up your face patterns. You can create a new one if you want.

Also make sure that you have Require Attention turned on. This means that anyone using Face ID has to be actively looking at the device: no one can open it with your face while you're sleeping or looking away. Go to Settings > Face ID & Passcode and make sure that Require Attention for Face ID is turned on.

While you can lock some apps with Face ID, some smartphone manufacturers have warned that facial authentication can pose some security issues, especially with transactions. online translation. Fingerprints and PINs are still the most secure means of keeping your phone safe.

So, if face unlock is having problems on your smartphone, you should deactivate it to prevent unauthorized access to your device.

You finished reading the article "**Can strangers unlock your phone with Face ID? How to prevent this?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.