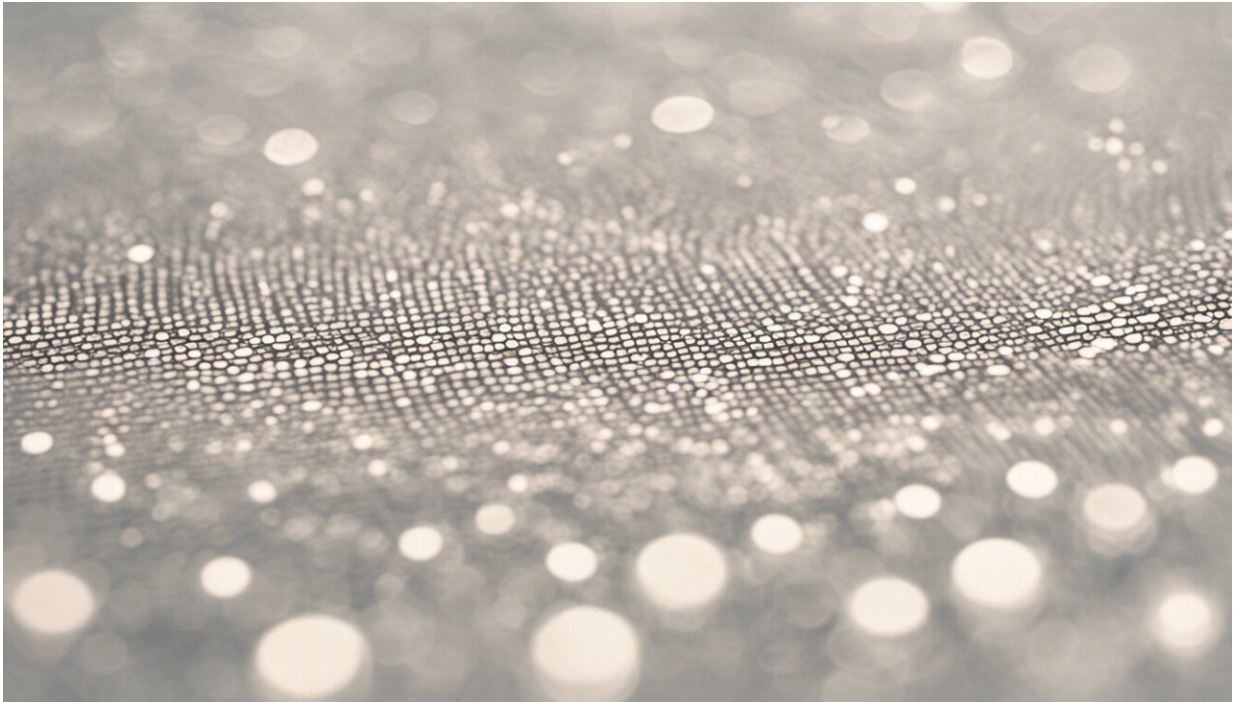# Is your phone safe from hackers?

July 28 2015, by Joe O'connell

Credit: AI-generated image (disclaimer)

A multimedia text could be the vessel that cripples as many as 950 million Android phones around the world, a mobile security expert warned in a Forbes article on Monday.

The security expert, Joshua Drake, discovered that the vulnerability resides in Stagefright, a media playback tool in Android. And he explained how a hacker could launch the devastating cyberattack with

startling ease—needing just the victim's [cell phone number](). With the number in hand, the hacker would send a multimedia message—one that the [phone]()'s user wouldn't even have to open—and immediately gain unrestricted access to personal information as well as the phone's camera and its apps.

Collin Mulliner, a mobile systems [security expert]() and research scientist in the College of Computer and Information Science, recently discussed the major flaw in Android phones with National Public Radio. Here, he offers up some tips for Android users who want to protect themselves against these potential cyberattacks.

How are vulnerabilities such as this one usually addressed?

The issue is really about getting updates and patches—or digital "band-aids"—for your phone. Security vulnerabilities are discovered all the time and the only working security measure is installing an update that fixes a given vulnerability, which is the responsibility of the phone manufacturer.

Oftentimes, the carrier has to sign off on the update before it reaches the end user's phone. This can take a long time; in some cases, it will never happen, due, for example, to a specific phone model no longer being supported by the manufacturer. One easy path to get more timely updates is buying Android devices sold directly by Google. Nexus devices receive very early updates directly form Google.

Are there certain brands of cellphones that are more susceptible to these attacks?

More or less, all Android devices are affected. Only devices that run

Android before version 2.2 are not affected. Further devices that recently got updated are likely patched, but this is hard to tell.

What can people do to limit their chances of being hacked?

They should disable the multimedia message automatic download in the Hangout application on Android. And only open and view multimedia messages from known senders. Users also shouldn't install applications that don't come from the Android Play Store.

Provided by Northeastern University