Jan 25, 2020, 06:19pm EST | 437,497 views

WhatsApp Users Beware: This Stupidly Simple New Hack Puts You At Risk—Here's What You Do

Zak Doffman Contributor ⓘ ⊕

Cybersecurity

I write about security and surveillance.

LIGHTROCKET VIA GETTY IMAGES

Whether or not Jeff Bezos was hacked over WhatsApp, and whether or not the culprit was Saudi Crown Prince Mohammed bin Salman, the Facebook-owned messaging platform *has* been compromised by security issues this year. And now there is another WhatsApp attack doing the rounds. But this one has nothing to do with nation state cyberattacks or the platform's integrity, and everything to do with our susceptibility to social engineering and our complacency when it comes to securing our devices.

This new social-engineering hack is stupidly simple to execute and just as easy to prevent. There's a basic security setting in WhatsApp that you have likely not set up, but which you should—it takes less than a minute. As soon as you finish reading this article, please check your app's settings and make the fix if required.

When it comes to the hacking of WhatsApp or other messaging platforms, it is important to separate out the various types of risks. Last year we saw nation-state attacks infecting targeted users with spyware, we saw the potential risk from crafted media files sent over the platform, and we saw a backdoor where bad actors could lock targeted individuals out of the messaging app.

All of these issues were fixed by WhatsApp—software patches plugged security gaps and ensured users were kept safe. The latest issue, though, was fixed before it even hit. But that fix requires users to take action, which means it's almost certain that many if not most of you have not yet done so.

This weekend, a friend in a group chat warned the rest of us not to open a message from her—she had been hacked, she said, and we should not "give away any six-digit numbers." Attackers, it seems, had gained access to her WhatsApp account and captured the phone numbers of members of the group. They were then able to send WhatsApps to the other group members, telling them they were about to receive an SMS message and could they please send it back to her. Social engineering at its best. Who would question the simple request of a trusted friend?

MORE FOR YOU

New WhatsApp Warning As This Malicious Hack Strikes Again: Here's What You Do

Is Your WhatsApp At Risk From This Dangerous Hack?

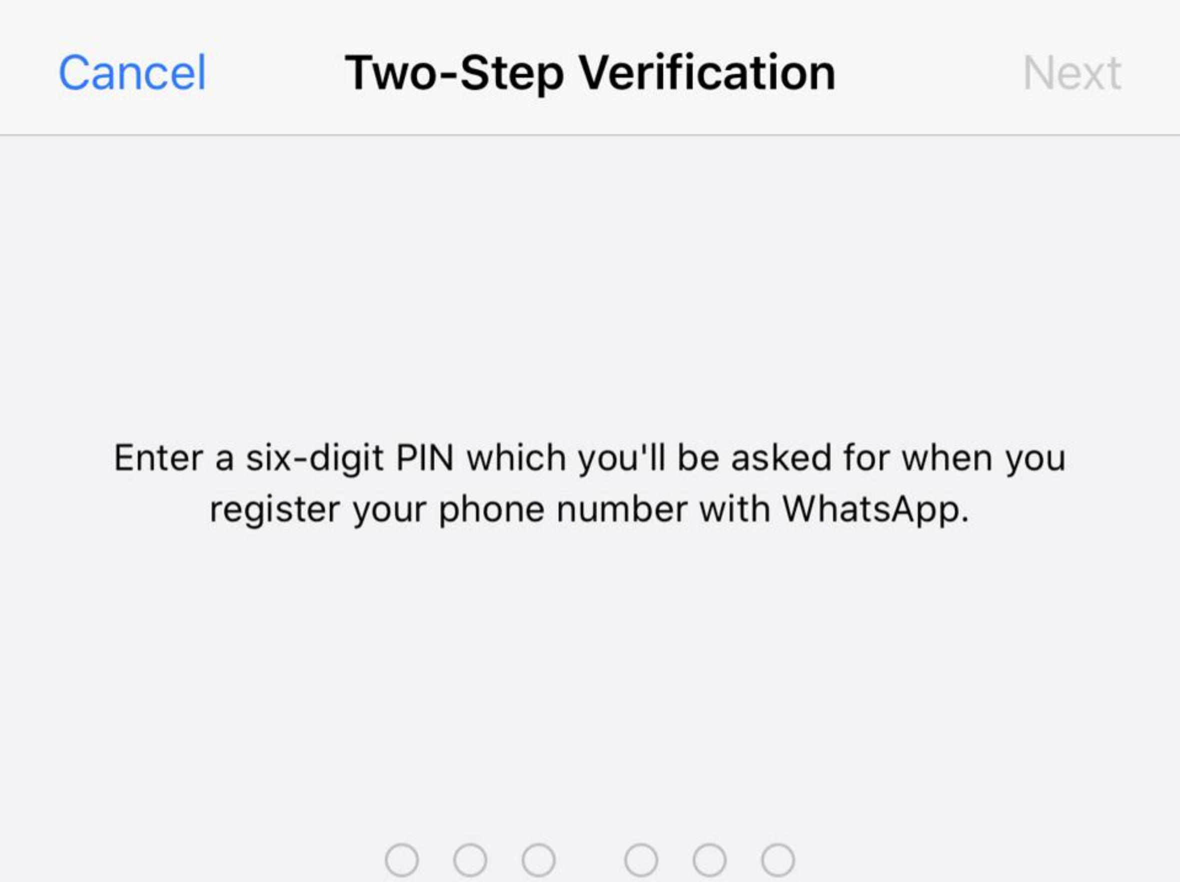
Why You Should Change These 3 Critical WhatsApp Settings

Behind the scenes, though, the SMS message was a WhatsApp verification code for the account of the person receiving the text. And in sending it back to the "friend," they were sending it to the attackers. With a fresh WhatsApp install, those attackers could then complete an account take over and progress their scam another turn. This is much simpler than porting the SIM to a new device. The effect, though, is the same. This same scam prompted a raft of police warnings in Singapore last summer.

With the account taken over, the attackers could then message the rest of the group as if from the account holder, as well as any other contacts whose WhatsApp messages were received after the take over. No legacy data is compromised. The target device remains untouched. WhatsApp has simply been ghosted onto an illegitimate device.

This can easily be prevented. In WhatsApp you can set up a PIN of your own choosing, and even an email address to use if you forget that PIN. This is separate to the six-digit code that WhatsApp will send by SMS to verify a new install. It's easy to see the verification code as the two-factor authentication. That can be defeated, as recent headlines on SMS security have shown. Another security layer with your own password is materially harder to beat. So even if you send the code to the attackers, they would still not have your own PIN. Clearly, you should not send the SMS code, but it makes absolute sense to set up this additional security layer anyway.

WhatsApp's "Two-Step Verification" process can be found under the Settings-Account from within the app. It takes less than a minute to set up.



Enter a six-digit PIN which you'll be asked for when you register your phone number with WhatsApp.

○ ○ ○ ○ ○ ○

WHATSAPP / IOS

The direct risk is not to you if you're attacked, but to your contacts. They can expect to receive requests for data or even emergency funds. Again, social engineering at its best. An end-to-end encrypted platform, a message from a trusted friend. We are coded to have our guards down in these circumstances.

If you have been the victim of this scam, you can clearly reactivate your device with a new SMS and transfer everything back. The attackers are banking on it taking time for you to realize what's happened and they may even send you additional SMS codes to confuse you as you look to repair the situation.

It is surprising how many people have not yet enabled the PIN in WhatsApp—almost everyone I have asked has yet to set it up. If you're the same, then please take that minute and set it up now. I know you won't send that verification SMS to a "friend" if asked, but do it just in case.

Follow me on Twitter or LinkedIn.

Zak Doffman

I am the Founder/CEO of Digital Barriers—developing advanced surveillance solutions for defence, national security and counter-terrorism. I write about the intersection... **Read More**

Reprints & Permissions