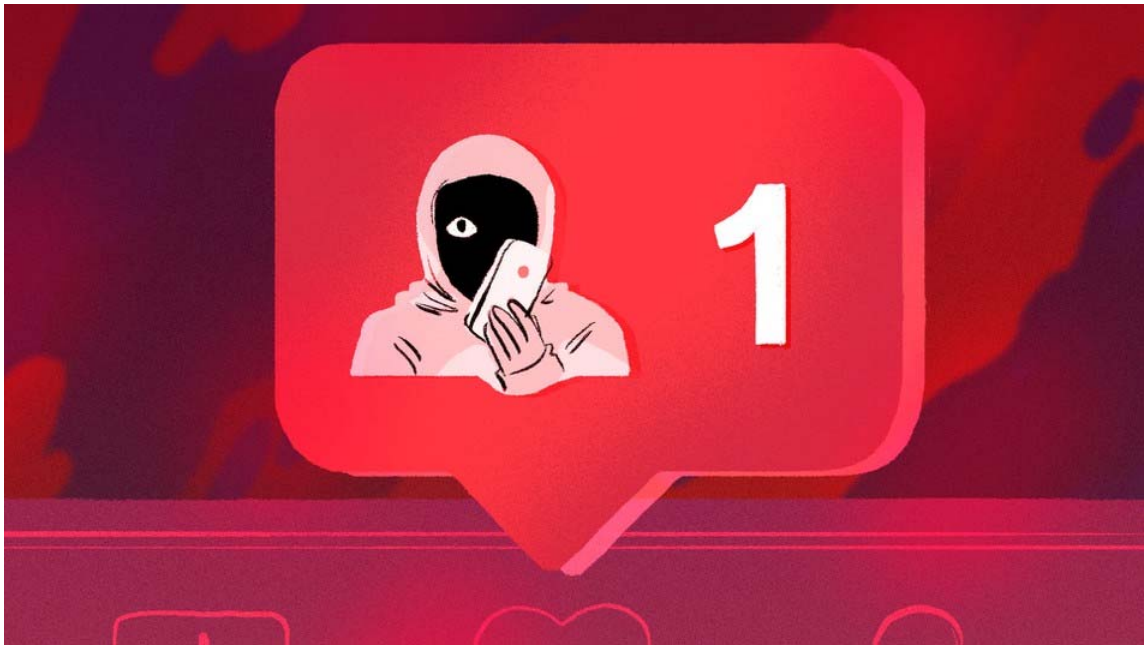
Tech

Instagram hacks raise questions about its 2FA security

Share on Facebook Share Tweet on Twitter Share Share



Instagram's security settings may not be tough enough to keep you safe. IMAGE: VICKY LETA/MASHABLE

BY KARISSA BELL
AUG 22, 2018

Even Instagram's strongest security settings may not be enough to protect your account from determined hackers.

As the company scrambles to manage a wave of hacks that have hit hundreds of users since the beginning of August, many of these users have described a troubling pattern that raises serious questions about the app's security settings.

SEE ALSO: Instagram users are reporting the same bizarre hack

Instagram lets users secure their accounts with two-factor authentication (PSA: here's how to turn on 2FA if you haven't already), but it currently relies on text messages, which aren't as secure as app-based authentication methods.

The company said in a statement last week in response to Mashable's reporting on the growing number of Instagram hacks that it's working to improve its 2FA security, but it didn't specify how. (Developer Jane Manchun Wong previously found evidence the company is testing a feature that would let people use a dedicated authenticator app, such as Google Authenticator.)

But until that update becomes available, the only option for users is the SMS-based method. And while SMS-based 2FA is better than none at all, it may not be enough to protect your Instagram account from determined cyber criminals.

Weak 2FA Security

Of the more than 275 people who have contacted Mashable about hacked Instagram accounts in the last week, most of the people we've heard from have said they were not using 2FA at the time.

But Mashable has confirmed that at least four people were hacked despite having 2FA enabled. At least six others who contacted Mashable have made similar claims, but were unable to provide evidence they had 2FA enabled on their accounts when they were hacked.

In some of these cases, there was no sign that someone was trying to hack their account — until the users were suddenly locked out with no warning. In other cases, they were aware hackers were targeting them, but Instagram's tightest security settings weren't able to protect their accounts.

> "It's not an exaggeration to say that Instagram is my number one security problem that I deal with as an IT professional"

One IT professional who spoke with Mashable on the condition of anonymity because he was not authorized to speak on behalf of his organization, said the Instagram account he manages for his company has been hacked three times in the span of a month, despite strict security settings. The account has two-factor authentication enabled, uses a 20-character password, and the email address linked to the account is a jumble of random characters, He has even given special instructions to his carrier to prevent unauthorized ports of his SIM.

Yet despite all this, the account, which has become a frequent hacking target, has been broken into three times in the last month. He often receives dozens of unauthorized 2FA prompts a day. (Mashable has seen screenshots confirming these attempts.) But oddly, he says that by the time he receives the prompt, the hackers have already managed to gain access to the account.

"Everything that Instagram has available is being done on our account and yet, every single time I get that SMS [the 2FA prompt], they have already changed the password," he told Mashable. "I cannot as an IT professional tell you how they are doing this. They must have some sort of flaw in Instagram fundamentally that they are exploiting to do this."

He has been able to regain access to the account each time because he has a contact at Instagram, but the constant hack attempts still take a toll. Fending them off has become a near-constant struggle — he says he's typically able to reset his password and head them off if he catches them within the first few minutes — which takes time away from other duties.

"It's not an exaggeration to say that Instagram is my number one security problem that I deal with as an IT professional," he says.

Small businesses upended

It's still unclear how these attacks are occurring. In the past, hackers have hijacked Instagram users' SIMs in order to gain entry into 2FA-protected accounts. But that doesn't appear to be what's happening in these cases, in which users describe their 2FA settings being bypassed, changed, or disabled without their knowledge.

> "Two-factor authentication obviously does help, but it's not foolproof"

"Two-factor authentication obviously does help, but it's not foolproof," says Stuart Madnick, an information technology professor at MIT's Sloan School of Management, who notes that clever hackers are often able to find loopholes that allow them to bypass 2FA.

One such loophole is particularly well known. A flaw in a routing protocol used by telecom companies, known as the Signaling System 7 (SS7) protocol, essentially allows hackers to redirect 2FA text messages from their intended recipients. This flaw has been exploited to great effect in the past. In January 2017, a group hackers exploited the SS7 flaw in order to empty their victims' bank accounts, ArsTechnica reported. And researchers at Positive Technologies demonstrated just how easy it can be to exploit this particular flaw when they used it to hack into a Coinbase account last year. Two Democratic Congressmen publicly asked the FCC to work with carriers to address SS7 vulnerabilities last year, but they have not yet been patched.

Whether or not this is what's happening to Instagram is impossible to say for sure without the company weighing in directly. Instagram has declined multiple requests to comment on the record. But the wave of recent hacks, which have caused hundreds to lose access to their accounts, highlight the fact that security is a growing concern for the service, which now has more than one billion users.

SEE ALSO: Instagram is investigating hacked accounts, promises new 2FA features

For small business owners who rely on Instagram for customers, these hacks can be especially devastating.

Robert Jordan who uses Instagram to communicate with clients for his soundtrack design company, reports a similar experience. On the night of Aug. 12, he was unable to log into his Instagram account, which had about 5,000 followers and was protected with 2FA. He soon realized the username had been changed, as well as the password and email for the account. His bio was deleted and his profile image changed to a partial image of a horse, which appeared to be a still from the DreamWorks film *Spirit: Stallion of the Cimarron.*

"For business profiles like mine that deal with multiple clients day to day through Instagram and other social media, it puts a huge dent in customer satisfaction"

He says he never received any indication from Instagram that something was wrong — no 2FA prompts and no emails alerting that his account info had been changed. Like dozens of others who have spoken with Mashable, he's had no luck navigating Instagram's support system.

"It’s extremely disappointing that, with such sensitive information like credit cards, addresses, phone numbers, and private messages linked to accounts, their support is less than subpar," Jordan says. "Since a lot of people are ditching Facebook over the data privacy issues, and LinkedIn isn’t extremely popular, Instagram has been my biggest connection. For business profiles like mine that deal with multiple clients day to day through Instagram and other social media, it puts a huge dent in customer satisfaction."

These types of small business accounts are significant not just to the people who run them. Small businesses are an increasingly important demographic for Facebook. There are 25 million business profiles on Instagram, according to the company's own statistics. And while not all of these businesses pay for advertising, the company is increasingly trying to encourage them to do so — Instagram lets businesses target users with shoppable ads in its feed and recently began experimenting with in-app shopping in Stories, in addition to traditional ads.

But unlike Facebook, which has fairly robust security settings (like the ability to use physical security keys as well as secondary authenticator apps), Instagram's security settings are fairly rudimentary. Businesses and other accounts with large followings have the same limited settings available to them as everyone else.

These settings don't go far enough to protect accounts that have large followings or whose handles are short or unique enough to make them prime hacking targets, users say. For example, though 2FA is offered, users are only prompted for additional codes when logging in from an unrecognized device. Instagram also doesn't require a password or other authentication method in order to change account information or to disable 2FA altogether.

Keeping users informed

Instagram, may also not being doing all it can to educate people about the risk of potential hacks, says Madnick, the MIT professor. "It's not clear to Instagram's best interest to tell people that they're under threat. It's a conflict of interest of sorts." He notes that many people never enable 2FA because they don't know it exists or assume they won't be targeted.

Complicating the hacks is Instagram's support system, which appears to be poorly equipped to handle the influx of requests to recover hacked accounts. Instagram said last week that users' whose accounts are improperly accessed and have account information changed should follow emailed instructions to revert the changes on their accounts. But many report that these links are dead by the time they see them. Others say they never receive any email at all, or that their attempts to reset their passwords are in vain because all of the contact information associated with account has already been changed. Instagram says it has other ways of letting its users recover accounts, but declined to comment on specifics beyond pointing to its previous blog post.

For users who have been hacked, this process adds insult to injury. People who are already desperate to regain control of their accounts — whether it's to support their business, recover photos of loved ones, or protect their privacy — end up feeling they're moving in circles, receiving automated email after automated email, with no resolution.

So while the rest of Instagram's 1 billion users wait for the security update the company promises is in the works, some of its most dedicated users are still waiting on a solution that may never come.

WATCH: Instagram launches their latest video feature called IGTV

TOPICS: BIG-TECH-COMPANIES, FACEBOOK, INSTAGRAM, SOCIAL-MEDIA-COMPANIES, TECH