3,000 Ring Doorbell and Camera Accounts May Be Vulnerable to Hackers

Ring users should change their passwords and enable two-factor authentication

By Daniel Wroclawski

December 19, 2019

PHOTO: RING

Ring is urging more than 3,000 users to change their passwords and use two-factor authentication after reports surfaced that Ring login information may have been exposed online.

Having these usernames and passwords could allow bad actors to access someone's Ring smartphone app and see live camera feeds and recordings, phone numbers, and home addresses.

A Ring spokesperson told Consumer Reports that the data exposure didn't involve the company's own system. There is "no evidence of an unauthorized

Instead, the account information appears to have come from other data breaches. In a practice called “credential stuffing,” hackers take usernames and passwords from data breaches elsewhere and attempt to break into other accounts. That’s possible because many people use the same usernames and passwords with numerous online accounts.

Besides changing passwords, the company is encouraging customers to enable two-factor authentication, which adds an additional step of making anyone trying to access an account enter a security code that is sent to the account holder via text message.

Ring doesn’t require users to do so, however. Ring’s head of communications, Yassi Shahmiri, declined to comment on why Ring doesn’t require the use of two-factor authentication.

MORE ON SECURITY CAMERAS AND PRIVACY

CR's Home Security Camera Ratings & Buying Guide

How to Prevent Security Cameras From Being Hacked

Tips for Better Passwords

Password Manager FAQ

Best Wireless Home Security Cameras of 2019

The set of stolen login information also came with other account information, such as the names of cameras and users’ timezones. “All that information is accessible if you have someone’s credentials,” Shahmiri said.

“If the bad actor that created the data set obtained credentials through credential stuffing, they could access that data easily, and they could have done so to verify the credentials work,” says Cody Feng, CR’s test engineer for privacy and security. “While we don’t know for certain, I would not call this a data leak based on the evidence we have.”

That’s why it’s important to use two-factor authentication.

"No matter how the data was exposed it is clear that Ring has not used reasonable security measures to protect their consumers' data,” says Katie McInnis, policy counsel for privacy and technology at CR Advocacy. “Even if consumers’ data."

Consumer Reports urges Ring users to change their passwords and enable two-factor authentication. Make sure you use a long, complex password, and if you’re worried about remembering the password, store it in a password manager. All of these steps will help protect you from a future hack or leak.

Consumer Reports tests wireless security cameras for data privacy and data security, and we recently tested the Ring Stickup Cam (2nd gen.) and gave it a Very Good rating for data security. One of the many reasons it received that score was the availability of two-factor authentication. However, at the time, we did find that Ring did not have a mechanism in place to prevent individuals with unusual IP addresses from logging into accounts by default.

The exposure of these account credentials is just the latest in a series of hacks and vulnerabilities that have affected Ring security cameras and video doorbells. Earlier this week, reports surfaced of multiple Ring accounts being hacked through credential stuffing. Back in November, it was revealed that Ring video doorbells contained a vulnerability that exposed WiFi network names and passwords. And last May, The Information reported a vulnerability that let individuals stay logged into Ring accounts even after a password change.

These issues don’t just plague Ring devices either. Last January, there were reports of Nest cameras being hacked, again through credential stuffing.

“Connected devices are only as strong as the security practices companies use to protect them,” said McInnis. “Consumers may be making their privacy and their homes vulnerable by using insecure products.”