How to Use Ring's Control Center for Better Privacy and Security

Consumer Reports explains how to use the Control Center settings, including the new two-factor authentication requirement

By Daniel Wroclawski

Last updated: February 18, 2020

The security device maker Ring has updated its privacy and security policies and is now requiring all users to employ two-factor authentication, a practice that makes passwords harder to hack.

The two-factor authentication setting, explained in detail below, is now mandatory for all users instead of just new ones, and is the latest security update from the Amazon-owned company.

Late last month, Ring began rolling out its promised privacy and security dashboard, called Ring Control Center, to users of its Android and iOS apps. First reported in early January, the new dashboard allows Ring users to manage new and existing privacy controls more easily. Below, we offer a step-by-step guide for what you should do.

The introduction of the Control Center and this recent update follow a string of instances of hackers gaining access to Ring accounts and spying on unsuspecting users. Before Ring's new Control Center, you had no way to tell if, for example, a hacker had logged on to your account, or even which devices, such as computers, smartphones, or tablets, were logged in to your account.

The changes the company has implemented include: a feature that allows you to view and remove linked accounts for products and services connected to your Ring device (such as digital assistants like Amazon Alexa); allowing you to opt out of receiving requests for video footage from police; and, most recently, requiring two-factor authentication for all users.

"We are glad to see Ring provide their users with more control over the sharing of their personal information and require two-factor authentication for Ring accounts" says Katie McInnis, policy counsel for privacy and technology at CR Advocacy. "We encourage Ring to continue to work to raise the security standards for their products and find additional ways to help consumers manage the use of their data."

As part of Consumer Reports' efforts to protect consumers' privacy and security, McInnis recently sent a letter to 25 connected camera companies urging them to improve their privacy and security standards due to a string of recent hacks and data breaches.

Ring says it has more security features in the works, such as one that will allow you to deny access to a device trying to log on to your account, which should help stop the credential stuffing attacks that affected Ring users back in December.

For now, Consumer Reports advises that you review the security measures provided in the Ring Control Center. It can be a bit confusing to figure out what changes you should make, though, so here's what we recommend. It's a good idea to periodically check these settings just to see if there are any suspicious linked accounts.

To find the Control Center in your Ring app, tap the menu button at the top-left of the screen, then tap on Control Center.

1. Check Two-Factor Authentication Settings

Before the Feb. 18 update, Ring's two-factor authentication was mandatory only for new accounts, meaning that existing users had to manually set up the enhanced security feature by going to the Control Center in the Ring smartphone app.

Now, anytime you attempt to access the Ring app, you'll be prompted to enter a randomly generated secondary password, which can be sent to your phone via an SMS text message or to the email address associated with your Ring account. You'll need to input a new secondary password from your phone or email each time you log on to your account.

2. Review Your Authorized Client Devices

An authorized client device is any smartphone, tablet, or computer that has the Ring app installed and logged in to your account. If, say, you check your Ring cameras on an iPad, work laptop, or smartphone, they will all appear on this list.

If you see any devices on the list that you don't recognize, or even old devices that you no longer use, revoke their access. A device you don't recognize could belong to a hacker, while old devices—which can be stolen or hacked themselves—could be used to access your cameras. You have to revoke all of your devices (tap the red Remove All button) and then log back on to the ones you want to keep.

If a bad actor is using your account, this step, combined with enabling two-factor authentication, will kick them out of your account and ensure they can't log back on. Of course, if you think your account has been hacked, you should also change your password.

3. Review Your Shared Users

A shared user account is an account you create for family members and friends to access your Ring devices. These accounts are a much more secure alternative to handing out your own username and password. This setting lets you see and remove all of your shared users. To see the list of shared users, tap on your home address in the Shared Users menu. If you see people you don't recognize or those who should no longer have access to your devices, revoke their access by tapping on their email address and then the red trash-can icon that appears next to it.

4. Review Your Linked Accounts

Linked accounts are for third-party smart home devices (not smartphones, computers, etc.) and services that connect to Ring products, such as a Schlage Encode smart lock or the Amazon Alexa digital assistant. This setting lets you view the third-party accounts that are linked to your Ring account. If you see any that you don't recognize, or even old accounts that you no longer use, revoke their access by tapping the red trash-can icon. It's a good idea to remove old linked accounts because if they're ever hacked, people could potentially view your live camera feeds without actually breaking into your Ring account.

5. Check Your Video Request Settings

This new setting allows you to opt out of footage requests from local police departments that have partnered with Ring. Before, you could only opt out after you received your first footage request.

"You should strongly consider opting out of video requests from local law enforcement, because neither you nor Ring has any control over how long the police department keeps the video or what they do with your footage once they download it," says CR's McInnis. "In addition, users should be aware that by sending the footage to the police to use as they will, they are also exposing their personal email and physical home addresses to local law enforcement.”

Ring states that local police can’t view live video feeds or control Ring devices. It also says that the only video the police can see is video that consumers either post on the Ring Neighbors network, which is built into the Ring app and is available as a standalone app, or share with law enforcement via footage requests. You can find out more about how Ring works with law enforcement in this FAQ page.

To opt out now, tap the Video Requests button under the Video Requests menu, followed by the Disable button. From this menu, you can also view a map of Ring’s 800+ partner police departments. We've embedded the map below so you can see which departments in your area are working with the company.

Daniel Wroclawski

I'm obsessed with smart home tech and channel my obsession into new stories for Consumer Reports. When I'm not writing about products, I spend time either outside hiking and skiing or up in the air in small airplanes. For my latest obsessions, follow me on Facebook and Twitter (@danwroc).