TEXAS COUNCIL ON FAMILY VIOLENCE

JANUARY 2022
VERSION 1.0

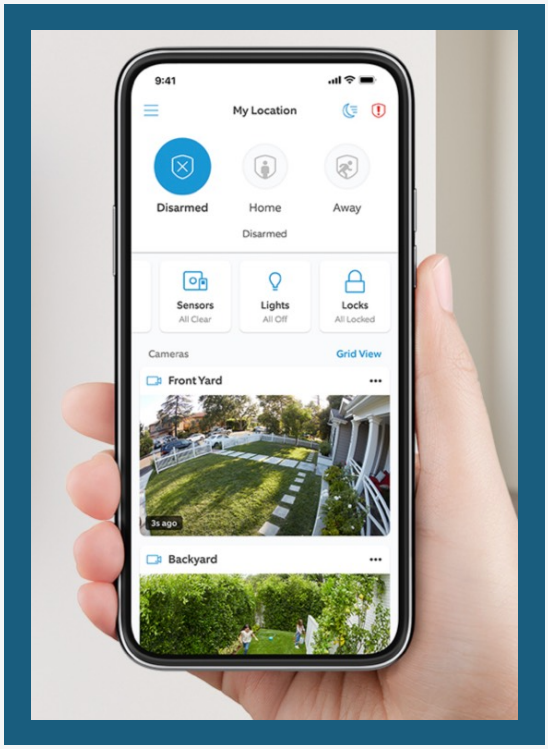
RING SECURITY DEVICES

a survivor safety guide

GUIDE OVERVIEW

Ring devices are available to you as an addition to your safety plan if you choose. This guide, in partnership with a discussion with an advocate, is meant to provide information about the risks, benefits, and steps you can take to maximize your safety. This guide will highlight these steps, explain best practices and empower anyone to make choices to use their Ring device as safely as possible.

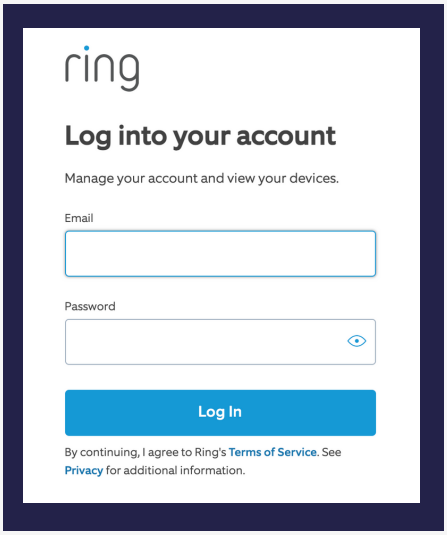
RING DOORBELL



ABOUT RING DEVICES

Ring devices, such as their Video Doorbells and Stick Up Cams, connect to the Ring app (pictured to the left) on your phone, tablet or your account on your computer and allow you to see an HD video stream of a person at your door (or other location) and speak to them using two-way audio communication. These devices connect to your home Wi-Fi network and can send alerts when motion is detected or when someone presses the button on the doorbell. To learn more, visit Ring.com

1 PASSWORD SET UP & SAFETY



Your password is the key to accessing your Ring account from any device. We suggest using a new unique password that no one else knows or can guess.

INSTEAD OF reusing a password or using something personal like your or a loved one's birth date, social security, phone number, favorite sports team, etc.

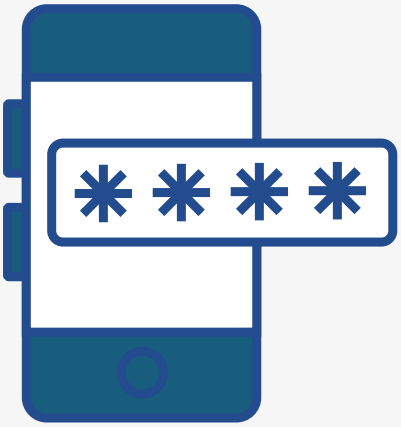
TRY USING a longer phrase or sentence (a line from a movie, book, song, joke, etc.) or use a password manager app that will help you create and remember different passwords for multiple accounts. Learn more about password managers and get suggestions here.

Ring also has specific password requirements and suggestions that you can read about here.

CAN ANYONE LOG INTO MY ACCOUNT IF THEY KNOW MY PASSWORD?

During the account setup process, it is mandatory that all Ring users have **'Two-Step Verification'** enabled - which **helps** prevents logins to your account even if someone knows your username and password. With every **new** login to your Ring account, you'll receive a one-time, six-digit code via email or text message to verify your login attempt. A person needs to enter that code before they will be allowed to access your Ring account. Learn more here.

When using two-step verification, it is only safe if no one else has access to your email account or devices where text messages are received. It may be helpful to update your email password and add a PIN or passcode to your wireless carrier account to help prevent unauthorized changes. Each carrier is different, so log into your wireless carrier account or call your wireless carrier for assistance.



AUTHENTICATOR APPS

If you would rather the six-digit code was not sent by email or text message, you can use an 'Authenticator App' that generates the code for you. Even if someone has access to your email account or is able to view your text messages, they cannot get the code. This process is explained here.

WHAT IF SOMEONE DOES MANAGE TO SUCCESSFULLY LOG IN WITHOUT MY CONSENT?

Ring will email you every time a new device successfully logs into your Ring account. If you believe someone knows your password or has logged in without your consent, you should open the Ring app and:

Step One → Tap the 3 horizontal lines in the upper left corner > Tap the Control Center > Tap 'Authorized Client Devices' to view all the devices currently logged in > Take a screenshot (in case need it for evidence later) and > Remove any unauthorized devices by tapping the red garbage can icon next to the device (instructions are here),

Step Two → Update your password (instructions are here).

2 YOUR EMAIL ADDRESS

Ring uses your email address to send security alerts, password reset links and other important information. If someone has access to your email account or mobile device, they can reset passwords and delete important notifications sent by Ring.

INSTEAD OF using an email address that other people may know (or may have or had access to).

TRY CREATING and using a new email address (with a new unique password) to set up your Ring account.

3 SAFEGUARDING YOUR DEVICE(S)

What can someone - such as a current or former partner who uses violence - do if they gain physical access to your smartphone, tablet or computer and open the Ring app?

They Can:

1) Add themselves as a 'Shared User' (Explained on the next page)

2) View your security feed

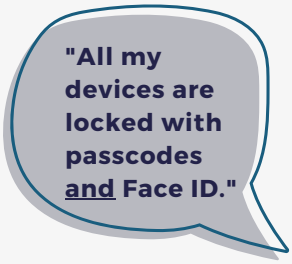
3) See your address in the top left corner

4) Change security settings

They Cannot:

1) Learn or change your password

2) Change your email address or phone number without entering your password



STEPS YOU CAN TAKE TO HELP PREVENT ACCESS

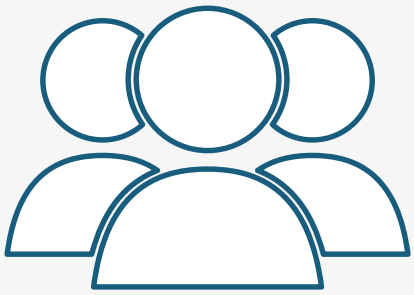
1) View your phone's lock screen setting and ensure you use strong pass-codes and turn on fingerprint or face ID.

2) Refrain from allowing anyone to physically access your device unless absolutely necessary. If you do give someone your device, be present when they use it.

3) Periodically check the following account settings to make sure everything is correct:

- Shared Users
- Authorized Client Devices
- Phone Number

4 SHARED USERS



What is a Shared User?

A Shared User is a person who has permission to watch your live video feed, view video recordings, and receive notifications or alerts for a Ring device that you own. They have their own separate account, and see a similar screen you do as the account holder. You can give a Shared User the ability to view one or more of the devices on your Ring account. **Shared Users cannot turn the alerts on or off.** Adding shared users may be a positive addition to the safety of your children or household members, and below are some risks to be aware of:

Scenario #1:
If someone has physical access to the Ring users smartphone, tablet or computer, they can add themselves as a Shared User and the owner will not be notified.

Safety Recommendations:

1) Set up a passcode and Face/Fingerprint ID on your device to prevent unauthorized access.

2) Check to see if Shared Users have been added: Tap the 3 horizontal lines in the upper righthand corner > tap Settings > tap 'Shared Access' > tap any unknown users and then tap 'Remove User'.

Scenario #2:
Someone you've added as a Shared User has their account accessed by the person who uses violence.

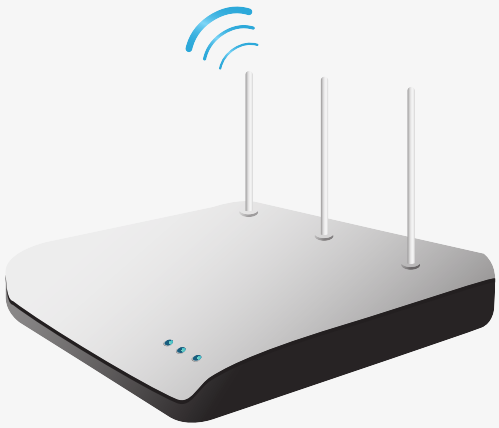
Example: A child who is added as a shared user is visiting the other parent and that parent obtains their login and password. That parent can now log in on their own device using the child's login whenever they want and view the Ring camera feed and recordings - and you will not be notified.

Safety Recommendations:

1) Only add Shared Users who are absolutely necessary as it can be a significant security risk.

2) Turn off the child's access when they are with the other parent or out of the house as follows: Tap the 3 horizontal lines in the upper righthand corner > tap Settings > tap 'Shared Access' > tap the name of the shared user and toggle their access to off.

5 HOME WIFI



Ring devices require WiFi to operate. If someone (such as a former partner who uses violence) has or had access to the Internet service account or set up the home WiFi being used for the Ring device, you can take some extra steps to secure the home's WiFi network.

Safety Recommendations:

Internet Service Provider Account: Log into your account on the internet service provider's website and confirm no one else has access. This process will differ depending on your provider. If there is a chance someone else knows your password, you may want to change the password.

Updating Passwords: Updating the WiFi password is not always straightforward. If your Internet service provider provides an app to use with your account, you can likely update the password this way. Or you can call them and ask how to update the password. Alternatively, you can attempt to update the password yourself using the instructions found here.

Also consider changing your router login and password from default settings. Learn more here.

6 VIDEO RECORDINGS

If your device includes a Ring Protect Plan, you can save, review, and share video recordings from your Ring devices to your Ring account. Your Ring device may record an incident that could be relevant to a family law matter, protective order or criminal investigation. You are under no obligation to share video recordings unless you choose to do so.

The video footage can be stored for up to 60 days. This time frame can be shortened within the app's control center. Be sure to store any saved videos in a secure location. One option for storing recordings securely is DocuSafe, created by the National Network to End Domestic Violence. Read about it here, and click here to learn more about sharing and downloading videos.

For support to address what may be useful to document and how to do that safely, contact the law enforcement agency you are working with, or your local family violence center.

7 SAFETY PLANNING CONSIDERATIONS

Safety Planning

A Ring device is not a substitute for your safety plan, but it can be a step you choose to take as a part of your safety plan. Practicing strong safety habits is still recommended: keep doors and windows locked, maintain control over the keys to your home, keep your phone charged, etc. If you have questions about safety planning, contact your local family violence organization or the National Domestic Violence Hotline for support. No matter what steps you choose to take, the violence is never your fault.

Steps During an Incident

In the event you are alerted via the Ring app to an unsafe person at your front door or within view of an external stick-up cam, you can plan in advance what action to take. Below are some options to consider:

Options if You are at Home:

1) Use the devices's two-way speaker to communicate as opposed to answering the door.

2) Use the device's two-way speaker to create the perception you are in the home while safely exiting the home.

Options if You Are Not at Home:

1) Ensure that motion alerts are enabled when you are away from home. The Ring app allows for several customizable settings for motion alerts. For example, you can be can be alerted (while at home or away) whenever a person passes in front of a video doorbell or stick up camera. This is helpful to assess safety before returning home or provide peace of mind while in the home.

2) If a motion alert is received, possible options include:

- Calling law enforcement.
- Speaking to the person remotely through the app, as opposed to answering the door.

8 OTHER SAFETY CONSIDERATIONS

End-to-End Encryption (E2EE)

This feature provides an additional, advanced encryption option to give users even more control over who can view their videos. With E2EE, only your enrolled mobile device has the special key needed to unlock these videos, designed so no one else can view your videos - not even Ring or Amazon. Learn more about this feature here.

When turned on, users lose certain features but may gain enhanced safety. For example, Shared Users will lose access to enrolled devices. The steps to activate this feature can be found here.

Neighbors

There is a news feed in the Ring app called 'Neighbors' that provides real-time crime and safety updates in your area. Other Ring users are able to post recordings from their devices and other notes of happenings in the neighborhood. This is also available as a separate app, and a person does not have to have a Ring device to download the Neighbors app. Ring has community guidelines to what can be posted, and you are able to flag content to request it be taken down. You may find it useful to monitor the Neighbors app to ensure your privacy.

Request for Assistance

The Neighbors news feed and app features 'Requests for Assistance', which enables public safety agencies to ask the public for help with an active investigation. Users are under no obligation to participate in or respond to Requests for Assistance. More information, including on how to turn this feature off, can be found here.

9 SAFETY EXPECTATIONS

Risks

As with all technology platforms and online accounts - there is a risk that a data breach may occur that is outside your control and potentially could expose user information and/or provide unauthorized access to accounts. In the case of home security devices like Ring, this can mean unauthorized access to your video feed and recordings. If you would like to learn more about some past security issues with Ring, and how Ring addressed them in order to make an informed decision about installing and using their products, you can read articles like this one and conduct your own online research on Ring.

Contacting Ring

In the event you have an issue that requires assistance (locked out of your account, security concerns, etc.) you can contact Ring directly here for support via chat or phone. If it is an emergency, call 911.

Resource Links:

- National Network to End Domestic Violence
- Texas Council on Family Violence
- EndTAB
- National Domestic Violence Hotline